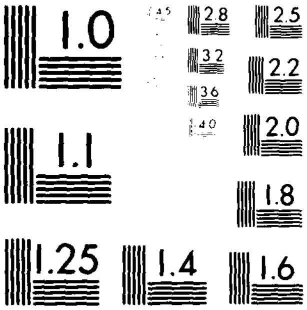
AD-A109 726   R AND D ASSOCIATES   ARLINGTON VA   F/G 15/3
CURRENT METHODS FOR EVALUATION OF PHYSICAL SECURITY SYSTEM EFFE--ETC(U)
MAY 81   R B DAVIDSON, J W ROSENGREN   DNA001-81-C-0109
UNCLASSIFIED   RDA-TR-179200-001   DNA-TR-81-18   NL

1 of 3
AD
A109 726


1.0
4.5
2.8
2.5
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

12

DNA-TR-81-18

CURRENT METHODS FOR EVALUATION OF PHYSICAL SECURITY SYSTEM EFFECTIVENESS

R & D Associates
1401 Wilson Boulevard
Arlington, Virginia 22209

1 May 1981

Technical Report

CONTRACT No. DNA 001-81-C-0109

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

THIS WORK SPONSORED BY THE DEFENSE NUCLEAR AGENCY
UNDER RDT&E RMSS CODE B310081464 B99QAXRB00032 H2590D.

Prepared for
Director
DEFENSE NUCLEAR AGENCY
Washington, D. C. 20305

DNA PRINTING PLANT

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER DNA-TR-81-18	2. GOVT ACCESSION NO. AD-A109 126	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) CURRENT METHODS FOR EVALUATION OF PHYSICAL SECURITY SYSTEM EFFECTIVENESS		5. TYPE OF REPORT & PERIOD COVERED Technical Report
		6. PERFORMING ORG. REPORT NUMBER RDA-TR-179200-001
7. AUTHOR(s) Robert B. Davidson Jack W. Rosengren		8. CONTRACT OR GRANT NUMBER(s) DNA 001-81-C-0109
9. PERFORMING ORGANIZATION NAME AND ADDRESS R & D Associates 1401 Wilson Boulevard Arlington, Virginia 22209	16	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Subtask B99QAXRB000-32
11. CONTROLLING OFFICE NAME AND ADDRESS Director Defense Nuclear Agency Washington, D.C. 20305		12. REPORT DATE 1 May 1981
		13. NUMBER OF PAGES 194
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This work sponsored by the Defense Nuclear Agency under RDT&E RMSS Code B310081464 B99QAXRB00032 H2590D.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Security System Assessment
Security System Modeling
Physical Security
Physical Protection
Safeguards
Nuclear Materials Management

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report provides the Defense Nuclear Agency with information on the availability and capability of techniques applicable to the evaluation of nuclear weapon physical protection systems. It considers older methods still in use, more recently developed methods, and methods which are not yet fully developed. The report examines six assessment schemes which attempt global evaluations of a security system and twelve techniques which →

20. ABSTRACT (Continued)

analyze specified attacks on a protected entity. A series of twelve tables compares the features and capabilities of the models. Observations on the possible utility of individual techniques, on security system modeling, on security system evaluation, and on the uses of security system evaluation techniques conclude the report.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

LIST OF TABLES

I. EXECUTIVE SUMMARY

1. REVIEW ELEMENTS AND TERMINOLOGY

a. Introduction--This study is intended to inform the Defense Nuclear Agency (DNA) about available computer models that can help evaluate physical security systems for nuclear weapons (at fixed sites and in transit). It also assesses the possible utility of the models as an aid to DNA in making security-related decisions. This report updates the findings of previous RDA surveys prepared for the Navy Surface Weapons Center (NAVSWC) (Ref. 1) and for the Nuclear Regulatory Commission (NRC) (Ref. 2). Like the NAVSWC study, the present review concentrates on computer models, but also examines other techniques that might support similar evaluations of physical security systems. We have attempted to consider all information available to us in March, 1981.

b. Nuclear Weapon Physical Security Systems--Present DoD systems for security of nuclear weapons are basically similar to NRC and DoE systems for the security of special nuclear material. They are based on the Department of Defense nuclear weapon security directive (Ref. 3) and

[1] Davidson, R.B., and Rosengren, J.W., An Assessment of Current Physical Security Models, R & D Associates, RDA-TR-111500-001, October 1979.

[2] Gref, L.G. and Rosengren, J.W., An Assessment of Some Safeguards Evaluation Techniques, R & D Associates, NUREG-0141, RDA-TR-5000-002, February 1977.

[3] Department of Defense, Security Criteria and Standards for Protecting Nuclear Weapons, Directive 52140.41, 30 July 1974.

manual (Ref. 4). Both the military and the civilian systems involve the same types of subsystems and components. The main features are:

- Exclusion areas, special access areas, restricted areas.
- Barriers and locking systems.
- Intrusion sensors and alarm systems.
- Surveillance systems (e.g., closed circuit TV).
- Guard forces.
- Duress alarms.
- Security communications.
- Back-up response forces.

Both types of security systems also share common types of rules and procedures. These include:

- Two-man rule for access to nuclear material.
- Personnel reliability program.
- Control of access authority.
- Use of exchange badges for exclusion areas.
- Defined response to hostage situations.

c. Actions to be prevented--A nuclear weapon security system needs to be prepared to prevent a variety of malevolent acts. These include:

- Theft of nuclear weapons.
- Capture of on-site control of a nuclear weapon (which could permit its use for blackmail).
- Disablement or destruction of nuclear weapons (which could be accompanied by dispersal of plutonium).
- Nuclear explosion on site.

[4] Department of Defense, Nuclear Weapons Security Manual, Unpublished.

- Launch of nuclear-weapon-carrying vehicle by direct unauthorized action or by indirect action, e.g., by alteration of control circuits.

d. Adversaries--

(1) Adversary action modes--Several different modes of "attack" can be used by an adversary who seeks to carry out a malevolent act involving nuclear weapons. These can be categorized as employing:

- Force--action that is overt and that involves or threatens physical violence against people or property.
- Stealth--action designed to be covert, to avoid detection.
- Deceit--action designed to deceive, such as the use of false identity or false authorization.

(2) Potential adversaries--Adversaries can be divided into two general categories--insiders and outsiders. Insiders are persons authorized some participation in facility operations, possibly including security operations. An outsider attacker is one who has no legitimate participation in facility activities. Various motives may prompt an attack on nuclear weapons. They include:

- Terrorism.
- Psychological disturbance.
- Paramilitary objectives.
- Criminal greed.

e. Computer models--We here summarize some general categories into which existing codes for modeling security systems can be divided. We also note some features that distinguish the various codes.

(1) Basic types of models--It is useful to distinguish between two basic types of security models--those that examine a security system's performance in a specified threat scenario and those that attempt a global evaluation of the system.

A *scenario-oriented model* simulates the attack specified by the user in more or less detail, tracing its progress and predicting its outcome.

A global model evaluates a security system more systematically. Its operation begins with generation of a set of scenarios which test the security system in a particularly stringent way. It then estimates the probability of attacker success in those optimized scenarios, identifying attacks to which the security system seems particularly vulnerable.

(2) Model components--It is a common and useful practice to divide the security system evaluation process into separate functional tasks, which are often accomplished by relatively independent computer codes--modules or subroutines within the modeling system. These include:

(a) Target identification routines--These perform some sort of fault tree analysis to determine, for example, which facility entity or entities must be attacked to successfully injure a nuclear fuel system installation in a particular way.

(b) Pathfinding routines--These codes consider all members of one or more classes of adversary paths in a facility and identify those paths that are in some sense best.

(c) Path simulation routines--These trace the adversaries' progress along their chosen path through the areas, portals, and barriers of the facility. They may also follow the movements of the guard force. They determine whether or not (or with what probability) the attackers are confronted by the security force or succeed in achieving their goals.

(d) Collusion analysis routines--These codes identify combinations of personnel who can use their insider privileges to carry out unauthorized activities directed against the facility.

(3) Treatment of probability--Many of the processes that physical security system models simulate are of a partly random nature. Typically, the system to be modeled includes several such random elements. These processes receive different statistical treatment in different models.

One approach to this problem, uses mean values in deterministic calculations. Another approach uses Monte Carlo techniques to produce a distribution of outcomes that is properly averaged over the various component distribution functions. A third, less satisfactory, approach utilizes a single random draw (from the appropriate distribution) for each stochastic variable.

(4) Transport models--Security systems to protect nuclear weapons in transit must be mobile and self-contained. Several groups have written or adapted models to deal with this special situation.

2. DESCRIPTIONS OF EVALUATION TECHNIQUES

The report describes each of the physical security evaluation techniques listed in Table 1.

We have generally divided the descriptions of major

TABLE 1. DESIGNATIONS OF SECURITY EVALUATION METHODS

DESIGNATION	TITLE AND ORGANIZATION
"GLOBAL" EVALUATION	
SAFE	Safeguards Automated Facility Evaluation (Sandia National Laboratories)
SSEM	Site Security Evaluation Model (TRW)
PANL	Path Analysis (Sandia National Laboratories)
VISA	Vulnerability of Integrated Safeguards Analysis (Science Applications, Inc.)
ASM	Aggregated Systems Model (Lawrence Livermore Laboratory)
SURE	Safeguards Upgrade Rule Evaluation (Sandia National Laboratories)
MAIT	Matrix Analysis of the Insider Threat (Science Applications, Inc.)
SVAP	Safeguard Vulnerability Analysis Program (Lawrence Livermore Laboratory)
SSNI	Sensor System Nullification by Insiders (Sandia National Laboratories)
SAA	Structured Assessment Analysis (Analytic Information Processing and Lawrence Livermore Laboratory)
SCENARIO EXAMINATION	
SSPAM	Security System Performance Assessment Method (Mission Research Corporation)
FSNM	Fixed Site Neutralization Model (Vector Research, Inc., for Sandia Laboratories, Albuquerque)
PROSE	Protection System Evaluator (John E. Lenz University of Wisconsin at Oshkosh)
SNAP	Safeguards Network Analysis Procedure (Pritsker and Associates for Sandia National Laboratories)
FESEM	Forcible Entry Safeguards Effectiveness Model (Sandia National Laboratories)

TABLE 1. DESIGNATIONS OF SECURITY EVALUATION METHODS (continued)

DESIGNATION	TITLE AND ORGANIZATION
NEWMOD	(Technical Support Organization, Brookhaven National Laboratory)
GPPLT	Generic Physical Protection Logic Trees (Sandia National Laboratories)
SOURCE	(Sandia National Laboratories)
SABRES	(Sandia National Laboratories)
SAS	Stand-Off Attack Simulation (Jaycor)
SAM	Security Analytic Methodology (Los Alamos National Laboratory for Air Force Weapons Laboratory)
ISEM	Insider Safeguards Effectiveness Model (Sandia National Laboratories)
BOARD GAMES	
GTS	Guard Tactics Simulation (Nuclear Regulatory Commission)
NWSSBG	Nuclear Weapon Storage Site Board Game (Booz-Allen and Hamilton)
SKIRMISH/ AMBUSH	(Sandia National Laboratories)

techniques into a few standard sections, typically including:

- Brief introductory overview.
- Situations examined (for scenario methods).
- Pathfinding (for global methods).
- Adversary description.
- Guard force description.
- Facility description.
- Combat engagements.
- Mathematical approach and performance measures.
- Presentation of evaluation results.
- Computational requirements.
- Documentation and applications.
- Assessment.
- Bibliography.

The descriptions appear in the same order as the entries in Table 1 except for the descriptions of board games (the final entries of Table 1),which the reader can find in Appendix B.

3. DISCUSSION OF EVALUATION METHODS

a. Tabular comparison of the methods--A series of tables summarize some of the properties of the evaluation systems.

Table 1 indicates the designations used to identify the methods. Table 3 records the state of development and documentation of the various techniques as of April 1981. Table 4 provides a rough indication of computational requirements.

Table 5 summarizes the range of coverage and capabilities of the evaluation aids. Table 6 and 7 provide more detail, respectively, about the adversary attributes and the adversary activities considered by each method. Table 8 compares the guard force descriptions. Table 9 examines representation of the facility and its security system hardware. Table 10 lists the security system activities each method considers.

Table 11 compares treatments of stochastic elements, and Table 12 characterizes the data base provided in some evaluation systems. Finally, Table 13 indicates the nature of the reports each method provides on security system performance.

b. A physical-security-system evaluation tool kit--No currently available evaluation technique meets all criteria for an ideal assessment aid. Moreover, no single current method provides all of the available capabilities that a security system evaluator or planner could profitably employ in a facility examination. Complementary techniques are separately available that together can provide considerable insight into the adequacy of a physical security system. We suggest some possible choices for a useful mosaic of methods.

(1) Global evaluations--To obtain an overview of the vulnerability of a security system to physical assault, the model of choice at present is probably SAFE. Its recently documented provisions for automated input assistance have made it much easier to use. SAFE's criterion for critical paths is as sound as any now in use. Its preliminary examination of critical paths using EASI and BATLE provides a good starting point for further evaluation.

SSEM is a close competitor for the global evaluation function. It offers some advantages over SAFE in certain applications, particularly those in which unusual circumstances cast tabulated component performance data into doubt. Many required data are built into the code for user selection.

To provide a global examination of the security consequences of insider privileges, we would choose MAIT. It is relatively easy to use, conservative from the point of view of the security system, and thorough within its range of concern.

(2) Scenario examination techniques--If a simple treatment is adequate, as is often the case, the EASI/BATLE combination is as good as anything currently available. It is sound, well documented, and treats--in some way--all the basic processes in the physical protection problem (detection, adversary progress and delay, guard force response, and combat engagement). It is as easy to use as any current evaluation tool.

The more detailed scenario simulation models continue to present difficult choices. SSPAM is not quite complete, and will require more testing and documentation before it can be used with confidence. FSNM has had some limited tests but is not yet entirely debugged. It cannot now be used on most computer systems, and there are no immediate plans for further development. Both SSPAM and FSNM require human factors data that are not now available, and that may prove difficult or impossible to obtain. SABRES II, which shares this problem, *is* complete and documented. Unfortunately, it treats only the combat engagement phase of a scenario.

SNAP is the only currently available, adequately documented modeling system that can carry out general detailed scenario simulations. Because it is uniquely flexible, it almost certainly belongs in the standard security system modeling kit. It is not, however, a convenient substitute for more rigidly defined models like SSPAM and FSNM, which should require less user attention to completeness and validation.

(3) Special purpose models--Two models we have examined attempt to address survivability within the context of security problems--Sandia/Livermore's SOURCE and Jaycor's SAS. They have differing strengths and weaknesses, which makes a choice between them difficult (and perhaps inappropriate). SOURCE deals with the road convoy ambush problem. SAS treats the entire transport problem, but considers some convoy characteristics in a less convenient way than SOURCE. Both could be useful.

(4) Hardware for security system modeling--A tentative consensus in the modeling community favors the use of high performance minicomputers with virtual memory operating systems (especially the Digital Equipment VAX 11). Most modelers now consider a graphic tablet attached to an interactive data entry system (with built-in display capabilities) almost essential for accurate, cost effective preparation of input for the more elaborate models. Most modeling groups prefer TEKTRONIX 4050 series microcomputers, with various compatible tablets, to support this part of the system.

c. Observations on security system modeling--It is impractical (if not impossible) to:

- incorporate *all* relevant features in a security system simulation or;
- *definitively* validate a security system model.

Many of the data required for very detailed scenario simulations are unavailable (and likely to remain so). Greater detail does not necessarily imply either great accuracy or high credibility. Problems of practicality and validation do not excuse the modeler from his responsibility to:

- create practical models that include the *most important* relevant features to produce suggestive, useful and demonstrably plausible results and
- select data and submodels that reflect the realities of the security systems as closely as the state of the art will allow.

Two useful aids in fulfilling the model designer's responsibilities are trial sensitivity studies--in which simulation runs are compared with one another to see if the results reflect changes in parameters and data in a reasonable way--and test examinations of real-world facilities--which allow evaluations based on modeling to be compared with conclusions of security system professionals.

Much has been learned in each attempt to produce a new generation of physical security system evaluation algorithms. An important part of the learning process takes place when model developers make a serious attempt to identify and correct the deficiencies of the previous generation's methodology.

d. Observations on security system evaluation--The comprehensive requirements of an adequate simulation can structure the initial data-gathering phase of a security system evaluation in a particular fruitful way. In fact, a significant fraction of the benefit of such an evaluation is often realized in this phase, as "obvious" weaknesses are uncovered.

Because computer models can be unusually thorough, they may uncover vulnerabilities that would elude a human evaluator. However, because no model or group of models is likely to consider the more imaginative attacks a creative professional might suggest, computerized procedures can constitute only part of a sound evaluation process.

Models can provide a framework within which experts can reach consensus decisions on security system adequacy. It should be much easier to reach agreement on parameters and methodology in the abstract than it would be to blend personal judgements of total systems.

An assessment that compares the performance of two candidate security system designs against unrealistically capable adversaries is likely to find both systems seriously wanting. More might be learned in a comparison that includes a variety of adversaries with varying capabilities (perhaps over a range that *culminates* at human limits).

Examination of a security system for adequacy against insider threats is important, because insiders *are* potential adversaries and because a security system that defeats insiders is likely to perform well against outsiders who use deceit.

Some plausible adversary activities are much more difficult to model than others. The evaluator of a security system has a special responsibility to consider separately, *outside* the context of automated assistance, any activities that are difficult to simulate.

Code originators, who know all the peculiarities of a given model (including the precise meaning of the numbers that go in at the beginning and come out at the end) are important--if not essential--members of teams that use the model in a security system evaluation. Similarly, site personnel should be actively involved in data gathering and analysis.

e. Observations on the uses of physical security system evaluation methods--Policymakers and researchers can use security system evaluation techniques to identify and understand factors that determine the success or failure of security systems. Managers and system designers tend to focus more sharply on specific systems, often within a relatively narrow range of excursions from a base case. Both sets of users will take advantage of whatever capabilities their chosen methods provide to screen many options economically. The evaluation method's basic function in this process (whatever its object) is to rank alternatives in a systematic and consistent way.

II. REVIEW ELEMENTS AND TERMINOLOGY

1. INTRODUCTION

The object of this study is to provide the Defense Nuclear Agency (DNA) with current information on the capability of available computer models to evaluate the performance of physical security systems for nuclear weapons, at fixed sites and in transit. It is also to provide an overall assessment of the models with regard to their possible utility to DNA as an aid in making security related decisions. This report updates the findings of previous RDA surveys prepared for the Navy Surface Weapons Center (NAVSWC) (Ref. 1) and for the Nuclear Regulatory Commission (NRC) (Ref. 2). Like the NAVSWC study, the present review concentrates on computer models, but also examines other techniques that might support similar evaluations of physical security systems.* We have attempted to consider all information available to us in March, 1981.

In the past two years there have been no revolutions in the state of the art of physical security system evaluation. There has, however, been steady evolutionary progress (and some change of emphasis in the major programs). Many of the models examined for the NAVSWC report are now better tested and documented. Several of the models have become easier to use, with automated assistance in input preparation and extensive use of interactive graphics. There is increased

*We do not discuss methods for evaluating materials control and accounting systems in this report. Such techniques were examined in RDA's NRC Survey (Ref. 2) and in two recent assessments prepared for the Department of Energy (Refs. 5, 6).

5. Dowdy, E.J., and Mangan, D.L., A Review of Safeguards and Security Systems Effectiveness Evaluation Methodologies, Office of Safeguards and Security, Department of Energy, January, 1980.

6. Paulus, W.K., Survey of Insider Safeguards Effectiveness Evaluation Models, Sandia National Laboratories, SAND 80-2580, October, 1980.

emphasis on techniques which attempt to accomplish the goals of computer modeling without (necessarily) using either computers or models. There seems to be less emphasis on elaborate high-detail scenario simulation models. This report reflects these trends in its coverage, and in its discussions of the models affected by the trends.

We have revised all of the NAVSWC report's model descriptions--some extensively, some less so. We distinguish old documentation--used in preparation of the NAVSWC review--from new in the bibliographies associated with the models by a nonstandard type style. We include new discussions of techniques not considered in the previous RDA surveys. We concentrate on those tools that seemed most promising as aids to DNA, and generally treat only briefly techniques which would require extensive modifications to be of interest to DNA.

2. NUCLEAR WEAPON PHYSICAL SECURITY SYSTEMS

Present and contemplated arrangements for security of nuclear weapons are generally similar to NRC and DoE systems for the security of special nuclear material. They are based on the Department of Defense nuclear weapon security directive (Ref. 3) and manual (Ref. 4). They share domestic safeguards systems' objective of "deterring potential adversaries from initiating or continuing acts involving the illegal acquisition or malevolent use of nuclear materials, and preventing the completion of such acts by detecting" them "and responding so as either to preclude theft or sabotage or to recover nuclear materials taken (Ref. 5)."

All of the systems--military and civilian--involve the same types of subsystems and components. The main features are:

- Exclusion areas, special access areas, restricted areas.
- Barriers and locking systems.

- Intrusion sensors and alarm systems.
- Surveillance systems (e.g. closed circuit TV).
- Guard forces.
- Duress alarms.
- Security communications.
- Back-up response forces.

DoD security procedures and rules also have much in common with those of other security systems. These include:

- Two-man rule for access to nuclear material.
- Personnel reliability program.
- Control of access authority.
- Use of exchange badges for exclusion areas.
- Defined response to hostage situations.

3. ACTIONS TO BE PREVENTED

A nuclear weapon security system needs to be prepared to prevent a variety of malevolent acts. To be comprehensive, a computer simulation system would need to be able to consider any of them. Possible hostile actions include:

- Theft of nuclear weapons.
- Capture of on-site control of a nuclear weapon (which could permit its use for blackmail).
- Disablement or destruction of nuclear weapons (which could be accompanied by dispersal of plutonium or U-235).
- Nuclear explosion on site.
- Launch of nuclear-weapon-carrying vehicle by direct unauthorized action or by indirect action, e.g., by alteration of control circuits.

4. ADVERSARIES

a. Adversary action modes--Several different modes of "attack" can be used by an adversary who seeks to carry out a malevolent act involving nuclear weapons. These can be categorized as employing:

- Force--action that is overt, which involves or threatens physical violence against people or property.
- Stealth--action designed to be covert, to avoid detection.
- Deceit--action designed to deceive, e.g., the use of false identify or false authorization; the creation of false impressions.

These terms can be used to describe the activity by which an attacker may enter a facility and carry out his plans.

An action may involve a combination of modes. For example, if the action begins as deceit or stealth, it may shift to force if an alarm is sounded. One general mode of action can be a combination of the above modes--for instance, the extortion of assistance from an insider, possibly someone in high authority. This could involve blackmail, the use of hostages, or some threat of violence. For example, a weapon officer's family could be held hostage, under threat of death if the adversary action is not successful.

b. Potential adversaries--Adversaries can be divided into two general categories--insiders and outsiders. Insiders are persons authorized some participation in facility operations, possibly including security operations. The designation "insider" is used for all such persons; their possible access and authority can range from very limited to very great. The insider adversary may be a determined malefactor, or he may be a person whose assistance is extorted or bought.

An outsider attacker is one who has no legitimate participation in facility activities. Attacker groups planning actions against nuclear weapons will probably require some advance inside information, supplied by a past or present insider.

c. Other attributes--Attacker attributes of possible interest in computer modeling efforts include:

- Possible division into component groups.
- Numbers in those groups.
- Knowledge of facility, weapons, and security.
- Weapons.
- Barrier penetration aids.
- Disguise.
- Transport.
- Communications.
- Personal attributes--dedication, intelligence, physical capabilities, etc.

d. Possible attacker motivation--There are various motives that may prompt an attack on nuclear weapons. It is conceivable that differences in motives may lead to differences in attributes that should be taken into account in modeling. In any event, some motives may make certain scenarios interesting that might otherwise appear unlikely. The motives are often implied by the labels that are given to possible attacker groups.

- Terrorist--A central goal is to make a political statement that receives great attention. The theft of a nuclear weapon and the threat of its use or its actual detonation would attract tremendous attention to a political cause.
- Paramilitary--The object may be to acquire nuclear weapons for some military activity, or to acquire intelligence information on U.S. weapons.
- Psychological--The malevolent action is motivated by psychological maladjustment, disaffection, mental aberration, etc.

- Criminal--The main motive is simply a desire to acquire wealth. This might be done by selling a stolen weapon or by extorting money through the threat of a nuclear explosion.

5. COMPUTER MODELS

We here summarize some general categories into which existing codes for modeling security systems can be divided. We also note some features that distinguish the various codes.

a. Basic types of model--It is useful to distinguish between two basic types of security models--those that examine a security system's performance in a specified threat scenario and those that attempt a global evaluation of the system.

A *scenario-oriented model* simulates the attack specified by the user in more or less detail, tracing its progress and predicting its outcome. If the analyst has sufficient skill, experience, and imagination, examination of a relatively modest number of scenarios using such a model may provide an adequately comprehensive and stringent test of security system--but this is in no way guaranteed. Evaluation techniques that do not involve simulation, but consider specific situations freely chosen by the analyst, are discussed in the section of this report which deals with scenario simulation (Section III, 2).

A global model evaluates a security system more systematically. Its operation begins with generation of a set of scenarios which test the security system in a particularly stringent way. It then estimates the probability of attacker success in those optimized scenarios, identifying attacks to which the security system seems particularly vulnerable. Often, a global model will identify particularly weak elements of the security system. The analyst may choose to examine the most interesting scenarios in greater detail, with a more elaborate scenario-oriented model than the one which is embedded in the global model. Evaluation techniques which do not involve simulation, but provide detailed guidance in choosing a set of situations to be considered, are discussed in the section of this report which deals with global simulations (Section III, 1).

b. Model components--It is a common and useful practice to divide the security system evaluation process into separate functional tasks, which are often accomplished by relatively independent computer codes--modules or subroutines within the modeling system. These include:

(1) Target identification routines--These perform some sort of fault tree analysis to determine, for example, which facility entity or entities must be attacked to successfully injure a nuclear fuel system installation in a particular way. These entities are thereby identified as more or less significant targets for the security system's hypothetical adversaries. Such routines may well be of interest to designers of nuclear weapon systems, to help them identify sets of circumstances that could lead to some particular sabotage objective such as unauthorized launch. Any important sabotage of the weapon system is, of course, a concern of the security system. However, the application of this type code to a complex weapons system is more the province of the weapon system designer than it is that of the security system designer or evaluator. These codes are not discussed further in this report.

(2) Pathfinding routines--These codes consider all members of one or more classes of adversary paths in a facility and identify those paths that are in some sense best. They may seek paths that are shortest in distance, shortest in elapsed time (including time required for penetration through barriers), along which intrusion is least

likely to be detected, etc. The path may be optimized all the way to the target (e.g., the nuclear weapons), to the target and out, or to some other position. For example, some codes determine paths that minimize probability of detection up to a distance from the target than can be traversed in less than the minimum response time of the guard force. (This maximizes the probability that the attackers will reach the target before being intercepted by the guard force.)

(3) Path simulation routines--These trace the adversaries' progress along their chosen path through the areas, portals, and barriers of the facility. They may also follow the movements of the guard force, sometimes at a different level of detail from that which is used to characterize the attackers' movements. Factors which may be taken into account by such routines include adversary and guard capability levels and equipment, performance parameters of security system hardware, operational and environmental conditions, mean times required to perform various tasks, etc. They determine whether or not (or with what probability) the attackers are confronted by the security force or succeeded in achieving their goals.

(4) Combat engagement routines--These routines predict the outcome of a confrontation between guards and attackers and estimate its duration. Factors which typically influence those predictions include numbers of combatants, weapons available to each side, level of competence/dedication/training, degree of tactical advantage, etc. Different examples of such routines allow for vastly different levels of tactical complexity. Some routines simulate the engagement in considerable physical and psychological detail; others translate the initial conditions into attrition rates for use in a system of differential equations that describe the development of the engagement.

(5) Collusion analysis routines--These codes identify combinations of personnel who can use their insider privileges to carry out unauthorized activities directed against the facility. Such acts might range from tampering with vital components of the alarm system to actual acts of sabotage or theft.

c. Treatment of probability--Many of the processes which are simulated in physical security system models are of a partly random nature. Stochastic features must therefore be included in those models. For example, times to complete tasks such as penetration of a barrier may be randomly distributed about some mean value according to a certain distribution function; less than perfect intrusion detectors are activated with less than unit probability by adversaries who pass them; etc. Typically, the system to be modeled includes several such random elements. These processes receive different statistical treatment in different models.

One sound approach to this problem, used in some of the simplest models, uses mean values in deterministic calculations. Probabilities and uncertainties introduced by random variations are propagated into well defined uncertainties in the results. Another sound approach, suitable for models of any complexity, repeats the simulation many times while randomly drawing values from appropriate distributions for each of the stochastic variables. If carried out a sufficient number of times, this Monte Carlo procedure produces a distribution of outcomes that is properly averaged over the various component distribution functions.

A less satisfactory (but more economical) approach utilizes a single random draw (from the appropriate distribution) for each stochastic variable. It is difficult to see how this could be valid in any context but that of a simulator to be used for training purposes.

d. Transport models--Security systems which must protect nuclear weapons in transit are somewhat different than fixed site protection systems, and face a somewhat different threat. Most obviously, they must be mobile, which limits them in many ways. (They cannot employ thick reinforced concrete barriers, for example.) They have less control over their surroundings in that they generally cannot effectively exclude either people or equipment from their immediate vicinity. They must be more or less self-contained. (Response forces that do not travel with the convoy are unlikely to be available for assistance on the time scale of a typical ambush scenario.) Because mobility can be a key to security system success, the vulnerability of convoy vehicles is typically much more important than the vulnerability of equipment in a fixed site physical security system. Adversary tactics are likely to be different. (Stand-off attacks may be particularly effective.) Several groups have written or adapted models to deal with this special situation.

III. DESCRIPTIONS OF EVALUATION TECHNIQUES

1. GLOBAL EVALUATION MODELS

a. Safeguards Automated Facility Evaluation (SAFE) (Sandia National Laboratories)--SAFE, Sandia's global evaluation modeling system for fixed site physical security systems, is composed of several relatively independent subsystems. In carrying out its part of the evaluation, each subsystem provides data for the next stage of the analysis. Together, these modules test an installation's ability to prevent access to, acquisition of, or removal of protected assets. This is done in a manner that is comprehensive in the sense of considering all critical attack paths (of the type that can be treated by the model). The tests are as stringent and conservative as the analyst chooses to make them through his specification of security system and adversary force performance measures.

Most of the computer codes which comprise SAFE can be run independently. Sandia has incorporated several of them (with more or less modification) into other models. We will discuss them under subheadings corresponding to the part of the problem which they address. This will facilitate cross-reference elsewhere in this report, and will allow easier access to discussions of codes which may be of interest in their stand-alone versions.

(1) Facility Characterization--The pathfinding procedures of SAFE require an extensive listing of points of interest within the installation (called nodes), accompanied by an exhaustive description of their interconnections (called arcs). Each location or connection must be characterized by type, average (and standard deviation) of the adversary's delay time, and probability of alarm activation. Since the previous survey, Sandia has developed

new sections of SAFE of these data to the computer (and in preparing them for further processing). (They were not included in some early versions of SAFE distributed to other organizations).

(a) <u>Graphical Representation Interactive Digitization (GRID)</u>--GRID helps the user identify and characterize the facility's significant points (nodes), including targets, penetration points, portals and staircases. The analyst also uses it to specify the positions and types of barriers such as walls. Because SAFE's automatic arc generating procedure considers only straight line paths, the user enters special extra points--called pseudo-nodes--to provide routes which go around obstacles rather than through them. GRID runs on a Tektronix 4051 desk-top microcomputer. An attached digitizing tablet provides a convenient means for reading node locations from a facility blueprint. Whenever the user wishes, GRID can display the data which have been entered, presenting a simplified facility drawing on the 4051's screen. This allows the analyst to examine them for accuracy and completeness and to correct them if desired. When he is satisfied, he can send a data file suitable for subsequent SAFE processing (listing node poistions and types) to SAFE's host main frame computer over telephone lines.

(b) <u>Automatic Region Extraction Algorithm (AREA)</u>--For simple facilities, the analyst can identify by inspection the arcs to be considered in further processing. For more complex facilities, SAFE provides an automated procedure to identify and help characterize significant arcs. AREA takes the set of node data provided by GRID and (with some assistance from the user) defines the abstract facility graph (nodes and arcs) that is used in later parts of the evaluation process. To use AREA, the analyst must digitize the facility quite precisely (which should not be difficult with GRID). AREA can identify certain unreasonable or imprecise entries to help eliminate erroneous data early in the analysis. It also helps the user modify a data set before further processing.

(c) Safeguards Engineering and Analysis Data Base (SEAD)--To complete SAFE's system specification, the analyst must specify such data as the delay time and detection probability associated with each barrier penetration node, the security force response time to each target node, the adversary velocity, and the probability that the security force is alerted when an alarm is activated. SAFE's designers suggest that the analyst use data appropriate to the specific security system components in their actual operational environment (a counsel of perfection!).

The modules of the SEAD system will eventually help the analyst prepare SAFE facility descriptions. He will be able to call component performance data from the data base interactively, either one component at a time or by type. The SEAD modules were designed to serve as dynamic, computerized handbooks of data on the performance of physical security hardware. They can produce answers to user inquiries, provide up-to-date hard copy compilations of the handbook data, and could serve as a modeling data base for other codes as well as SAFE. Information from the Sandia barrier data base (Ref. 7) was incorporated in

[7] Intrusion Detection Systems Handbook, SAND76-0554, Sandia National Laboratories, October 1977.
Entry Control Systems Handbook, SAND77-1033, Sandia National Laboratories, September 1977.
Barrier Technology Handbook, SAND77-0777, Sandia National Laboratories, April 1978.

the one completed SEAD module. Sandia is developing interfaces with SAFE and experts to complete them in FY 1981. Sandia has suspended development of additional SEAD modules, at least in part to avoid needless publication of safeguard component vulnerabilities.

(2) Pathfinding routines: KSPTH, MINDPT, PATHS, ADAPTH, POST--Several procedures are (or soon will be) available in SAFE to identify those adversary paths through the facility which most severely test the security system. With one exception (discussed below) they are unidirectional: they optimize paths from one node (exterior or target) to another (target or exterior), but not round trip paths. Identification of one or several critical paths can be requested, and three different measures of system stress can be employed. Most of the procedures discussed here are deterministic: they use a single average value for each facility parameter and identify optimal paths that correspond to those fixed average values.

In older versions of SAFE, KSPTH identified one or more paths which minimized, as desired, either the time required for the adversary to reach each significant location in the facility or the probability that he would be detected along the way. In the current standard version of SAFE, MINDPT, which has replaced KSPTHS, identifies a most critical path that minimizes time, detection probability, or a third figure of merit: the probability that the adversary will de detected while the security force still has time to respond before the adversary reaches his target. Both KSPTH and MINDPT use an efficient search algorithm designed by E.W. Dijkstra (and modified by J.Y. Yen) to identify their optimal paths.

SAFE's second generation PATHfinding Simulation (PATHS) generally uses MINDPT's minimization-of-probability-of-timely-detection scheme (including the Dijkstra-Yen search) but applies it in Monte Carlo fashion to sets of facility parameters chosen in accord with distribution functions specified by the analyst. Like the other pathfinding routines, PATHS ranks the routes it explores and identifies those it considers most critical. It also identifies those adversary activities which occur with highest frequency in the set of paths which are most critical. Such a list could be a valuable aid in improving an installation's security system. It is most often used after MINDPT has already established that there are interesting vulnerabilities to be explored.

Most recently, Sandia has developed a code called ADPATH, which will replace MINDPT in the standard version of SAFE sometime in FY 1981. Like MINDPT, ADPATH is a deterministic algorithm. It differs from other Sandia pathfinding routines in three major respects: it uses an improved search algorithm devised by L.R. Ford, Jr., it handles both the entry and the exit phases of theft paths in a single run, and it allows for different treatment of the two directions of travel along a path or through a barrier. The latter improvement is rather significant, since it allows a somewhat more realistic treatment of escape after theft. (ADPATH cannot account *dynamically* for degradation of security system elements during the entry phase--an extremely difficult mathematical problem!)

For installations in which the adversaries must visit several targets to accomplish their mission, Sandia has developed a pathfinding code called POST to find optimal paths (by repeated application of ADPATH).

(3) Path evaluation: EASI, BATLE--Those paths which have been identified by SAFE as especially likely to defeat the physical security system are examined further to obtain additional measures of the installation's vulnerability to attacks along them. The intent is to provide a conservative global assessment of the system to be used in design tradeoff studies and --perhaps--regulatory certification. Because the number of critical paths to be examined is relatively

small, the path evaluation codes that follow could, in principle, be quite elaborate. To preserve the option of carrying out sensitivity studies at moderate cost, however, Sandia uses fairly simple models to follow adversary progress in the current standard implementation of SAFE. (Sandia is developing an option which would perform more elaborate path examinations using the SNAP simulation system described elsewhere in this report.)

Up to the point at which the adversaries are confronted by the guards (or the hostile act is accomplished without such an encounter), SAFE employs a procedure called Estimate of Adversary Sequence Interruption (EASI). Two versions of EASI essentially similar to the one in SAFE are available for stand-alone use. Sandia has implemented one of them in the instruction sets of several hand-held programmable calculators. The other requires more substantial computational facilities but can accept its input from a time sharing terminal. It can also present part of its output as a useful set of two- or three-dimensional graphs that portray the sensitivity of the results to the performance of elements of the security system. All the versions of EASI treat the adversary path as a sequence of tasks, which might include travel from one point to another, penetration of a barrier, etc. Associated with each task is a mean performance time, its standard deviation, and a probability that the alarm system will detect the adversaries once they have performed the task. EASI also requires estimates of mean guard force response time (which includes alarm assessment time), its standard deviation, and the probability that the existence of an activated alarm will be communicated to the guard force. EASI combines these data to produce a cummulative probability that the guard force will confront the adversaries before they have succeeded in their objective. In Sandia's tests, EASI values for this measure-of-merit were similar to results obtained from more elaborate models such as FESEM, ISEM, and FSNM. EASI carries the scenario to the amount of confrontation of guards and adversaries. In SAFE, a code called Brief Adversary Threat Loss Estimator (BATLE) assesses the likely outcome of the ensuing struggle. BATLE is a small-scale engagement model that uses estimated average attrition rates rather than carrying out a detailed simulation of the events of the encounter. BATLE estimates these attrition rates from user-specified assumptions about combatant characteristics and circumstances, including posture, cover, weaponry and firing proficiency, using empirical relationships based on military weapons effectiveness data. BATLE's attrition rates differ for participants who defend or mount an assualt. Circumstances (and attrition rates) can change--and additional guards or attackers can arrive--at any time during the course of an engagement. The engagement terminates when specified "absorption states" have been reached. (In practice this almost always means that either the number of guards or the number of adversaries has become zero.) BATLE calculates a probability that the security force will win the battle. The product of this probability and EASI's probability of interruption is SAFE's measure of overall security system effectiveness for a given critical path.

(4) Computational requirements--SAFE offers considerable evaluation capability. To provide that capability, SAFE requires substantial (but not extraordinary) computational resources. In the current standard version, a fairly elaborate microcomputer system supports data entry and verification. Such systems have become more common recently, but they are not so universally available now that they can be considered standard equipment. The rest of SAFE runs on a standard large main frame computer, using resident graphic display software in addition to a Fortran compiler, and up to about

35,000 words of storage. For a fairly complex problem, a single run through the SAFE procedure required about two minutes of central processor time on the Sandia CDC 6600.

(5) Documentation and application--Sandia has prepared an extensive collection of documents about SAFE and its components since the previous RDA survey. New entries in the bibliography for this section include a multi-volume SAFE user's manual containing an overview, and extensive methodological discussion, a detailed example and listings of the computer codes. Rather complete current descriptions of BATLE and of several of the pathfinding routines have also been added to the list, as have a set of directions for the application of SAFE to a reactor and a report of parallel applications of SAFE and other Sandia evaluation techniques to a reactor and a fuel cycle facility. SAFE is as well documented as any technique we have examined.

SAFE has been actively applied by Sandia since the last RDA survey. Major recent applications included examination of four nuclear reactors and a generic Navy ship. Typically, such an application considered a large number of sabotage targets (including some which had to be visited in sequence), and included sensitivity studies leading to recommendations for security system upgrades. Various versions of SAFE have been transfered to five non-Sandia users.

(6) Assessment--SAFE, like other global evaluation techniques we have examined, falls somewhat short of providing either a definitive or a truly comprehensive security system evaluation. Certain system elements are treated in a simplified, sometimes artificial way*. Only paths corresponding to

*Some examples: Random guard patrols are treated by averaging guard response time over the entire tour of duty, including time spent in the guard house; insider assistance is considered by arbitrarily degrading performance parameters for each alarm judged to be susceptible to tampering by an insider.

very straightforward adversary tactics are examined as candidates for critical paths, and only a single threat and a single system condition are considered in a given evaluation run.

Nevertheless, SAFE's evaluation of an existing or planned facility can be very helpful to the analyst--quite likely as helpful as any currently available modeling system. SAFE's capabilities, some of which are unique among available evaluation procedures, have been continually refined during the course of its development and are impressive.

BIBLIOGRAPHY

General

Chapman, L.D., Engi, D., Grady, L.M. and Pavlakos, C., SAFE Users Manual. Volume I: Introduction to SAFE,
Volume II: Method Description,
Volume III: Example Application,
Volume IV: Code Descriptions,
NUREG/CR-1246, SAND 79-2247, Sandia National Laboratories, to be published.

Chapman, L.D., Application of SAFE to An Operating Reactor, NUREG/CR-0928, SAND79-1372, Sandia Laboratories, August 1979.

Pavlakos, C.J., Chapman, L.D., Grant, F.H. and Kimpel, C.H., Application of Sandia Physical Protection Methods, NUREG/CR-1893, Sandia National Laboratories, to be published

Engi, D., Chapman, L.D., Grant, F.H., and Polito, J., A Combined SAFE/SNAP Approach to Safeguards Evaluation, NUREG/CR-1591, SAND 80-0529, Sandia National Laboratories, August 1980.

Chapman, L.D., Assessment of Methods for Evaluating Adequacy of Physical Protection Systems, NUREG/CR-1781, SAND 80-2352, Sandia National Laboratories, November 1980

Chapman, L.D., Grady, L.M., Bennett, H.A., Sasser, D.W., Engi, D., Safeguards Automated Facility Evaluation (SAFE) Methodology, NUREG/CR-0296, SAND 78-0378, Sandia Laboratories, August 1978.

Chapman, L.D., Bennett, H.A., Engi, D., Grady, L.M., Hulme, B.L., and Sasser, D.W., Safeguards Methodology Development History, SAND 79-0059, Sandia Laboratories, May 1979.

Chapman, L.D., Briefing on "Evaluation of Physical Protection Systems at Nuclear Facilities", Sandia Laboratories, June 1979.

Bennett, H.A., Boozer, D.D., Chapman, L.D., Daniel, S.L., Engi, D., Hulme, B.L., and Varnado, G.B., Safeguards System Effectiveness Modeling, SAND76-0428, Sandia Laboratories, September 1976

SEAD

Hall, R.C. and Jones, R.D., A Scientific Data Base for Safeguards Components, NUREG/CR-0459, SAND78-1176, Sandia Laboratories, October 1978.

Pathfinding

Engi, D., Shanken, J.S. and Moore, P.W., Pathfinding Simulation (PATHS) User's Guide, NUREG/CR-1589, SAND80-1626, Sandia National Laboratories, to be published.

Hulme, B.L. and Morgan, C.A., ADPATH: An Adversary Path Subroutine, NUREG/CR-0869, SAND79-1205, Sandia Laboratories, July 1979.

Hulme, B.L. and Morgan, C.A., POST: A Subroutine for Path Ordering of Sabotage Targets, NUREG/CR-1226, SAND80-0058, Sandia National Laboratories, February 1980.

Hulme, B.L., Holdridge, D.B., KSPTH: A Subroutine for The k Shortest Paths in a Sabotage Graph, SAND77-1165, Sandia Laboratories, August 1977.

Hulme, B.L., MINDPT: A Code for Minimizing Detection Probability Up to a Given Time Away from a Sabotage Target, SAND77-2039, Sandia Laboratories, December 1977.

Hulme, B.L., Wisniewski, J.A., Codes for Dijkstra's Shortest Path Algorithm, SAND78-0493, Sandia Laboratories, April 1978.

Hulme, B.L., Wisniewski, J.A., A Comparison of Shortest Path Algorithms Applied to Sparse Matrices, NUREG/CR-0293, SAND78-1411, Sandia Laboratories, August 1978.

EASI

Sasser, D.W., EASI Graphics--GCS Version, SAND80-0212, Sandia National Laboratories, March 1980.

Bennett, H.A., User's Guide for Evaluating Physical Security Capabilities of Nuclear Facilities by the EASI Method, SAND77-0082, NUREG-0184, Sandia Laboratories, June 1977.

Bennett, H.A., The "EASI" Approach to Physical Security Evaluation, NUREG760145, SAND76-0500, Sandia Laboratories, January 1977.

Sasser, D.W., EASI on the HP-25, and HP-67, NUREG-0231; SAND76-0597, Sandia Laboratories, May 1977.

Bennett, H.A., Sasser, D.W., EASI Program Improvements for HP-67 and TI-59 Calculators, NUREG/CR-0350, SAND78-0506, Sandia Laboratories, July 1978.

Sasser, D.W., User's Guide for EASI Graphics, SAND78-0112, Sandia Laboratories, March 1978.

BATLE

Engi, D. and Harlan, C.P., Brief Adversary Threat Loss Estimator (BATLE) User's Guide, NUREG/CR-1432, SAND80-0952, Sandia National Laboratories, May 1981.

Engi, C. and Farrell, R.L., Markov and Semi-Markov Modeling of Small Engagements, NUREG/CR-1309, SAND79-2013, Sandia Laboratories, December 1979.

Engi, D. Siegel, A.I. and Wolf, J.J., Human Effects Aspects in Simulating Hostile Attacks Against Nuclear Facilities, NUREG/CR-1310, SAND79-2237, Sandia Laboratories, December 1979.

Engi, D., A Small-Scale Engagement Model with Arrivals: Analytical Solutions, SAND77-0054, NUREG-0238, Sandia Laboratories, April 1977.

b. Site Security Evaluation Model (SSEM) (TRW)--SSEM is TRW's global physical protection system evaluation code. It was developed in the early 1970s, reaching its mature form by the end of 1974. Since then, the only major change in the model has been the development of an improved input system (by TRW and Informatics) in 1978. SSEM was discussed in both of the previous RDA surveys of security system evaluation models. Despite its age, it is quite competitive with more recently developed global models. As a result, it is still in active use.

SSEM considers attacks on a protected facility by a single group of adversaries intent on performing a malevolent act at some target within the facility. The attackers approach the target along an optimized route from the outer perimeter (in the case of outsiders) or from some point of legitimate access (in the case of insider adversaries). So long as deceitful outsiders are judged to have successfully deceived the access control system, they are treated as insiders. SSEM selects routes that minimize the probability that the attack is recognized before the adversaries complete their activities at the target.

(1) Adversary description--SSEM describes attackers in terms of their abilities to defeat or evade each type of impediment which might be placed in their path by the security system. These capabilities include insider privileges, and skills useful in penetrating barriers, defeating alarms, opening locks and entering controlled portals by deceit.

(2) Guard force description--Guards have one main function in SSEM scenarios: they may detect the attackers. (Presumably, they also operate parts of the independently

modeled access control system.) For use in estimating adversary detection probability, the guard force description includes details such as visual and aural acuity, and time schedule, duration, coverage, and composition of any patrols or guard post details. To aid in estimating response times, the input information also specifies guard locations, procedures, and travel speeds.

(3) Facility description--SSEM superposes a rectangular array of grid points on a scale drawing of each floor of the facility, spaced so that each element of the security system which is to be modeled is unambiguously located between two adjacent grid points. Grid points occur at each intersection of a two- or three-dimensional mesh of orthogonal lines. The site is described by specifying what barrier type (if any) and what alarm type (if any) occur between each grid point and each of its neighbors along the grid lines. (Interior points have six neighbors in a three-dimensional facility, four in a facility which has only a single level.) In addition, SSEM defines the lighting level at the grid point, and identified any targets or volume sensors which may be present there. An extensive data base of performance parameters for walls, doors, locks, alarms, and CCTV systems simplifies entry of this information.

The code examines each direction of motion from each point to an adjacent point along a grid line and assigns a probability of successful adversary penetration (passage through any obstacles without detection, as a function of time spent) to each motion. The bulk of the computer time used by SSEM is spent in optimizing these point-to-point journeys. SSEM can save information about the optimized path segments for future use (in sensitivity studies, for example). In examining these path segments, SSEM employs a barrier submodel (to provide raw probability of penetration), an alarm submodel (to provide probability of alarm, given penetration), and the guard submodel (to provide probability of detection, given an activated alarm). An unusual feature of SSEM is its use of detailed physical models for most of the security system's detection processes, mechanical and human. (Any advantage of this approach over use of empirical performance measures may be accompanied by uncertainties introduced by simplified physical descriptions of the detection processes.)

(4) Pathfinding and path evaluation--SSEM simultaneously identifies and evaluates critical paths to each potential target. It does this by applying dynamic programming techniques to the successful penetration probabilities --described above--for each journey from grid point to grid point. SSEM can carry out the optimization so as to maximize a success probability. SSEM's designers' early experience with the method led them to conclude that a total time constraint has little impact on adversary success. This, and the much higher cost of the constrained optimization, led them to remove the time constraint in all recent applications. SSEM's global measure of security system effectiveness is the adversaries' overall success probability, computed as a function of the time available to them for completion of all their activities.

(5) Auxiliary models--Associated with the submodels which carry out the evaluation described above are other, essentially independent, submodels which treat various aspects of security system operations. They include a Key, Combination, and Document Control Model (which keeps records, compiles inventories, and calculates compromise probabilities for those entities), an Access

Control Model (which simulates typical operations of an access control point and estimates probability of evasion by an unauthorized person), a Bomb Damage Model (which estimates the effects of an explosion on people and barriers), a Mob Action Model (which simulates confrontations between a hostile crowd and the security system), a Cost Model (which estimates the annualized cost of a specified physical security system), and an Emergency Destruction Model.

(6) Computational requirements--As expected for a global assessment model, SSEM's demand for computational resources is substantial. Examination of a real fuel cycle facility, described in terms of 605 grid points, required about 4 minutes of central processor time on an IBM 370/195, a reasonable time expenditure for such an examination. Storage requirements, however, were formidable: about 800,000 bytes or 100,000 double precision words. Data collection, entry and verification were rather burdensome in the original version of SSEM. To alleviate that burden Informatics (in collaboration with TRW) wrote a new data input package, which uses a Hewlett-Packard 9800 series desk-top microcomputer to assist in the process. A digitizing tablet helps the analyst locate grid points and security system elements at the correct positions on a facility blueprint. A plotter provides displays of the information entered on digitized maps (for checking and editing). The package produces a tape containing the SSEM input information which used to be produced by hand; it can be edited if desired.

(7) Documentation and applications--Most SSEM documentation is classified Secret. This reflects the original sponsorship of the model rather than the sensitivity of the publications, which are similar to the

unclassified model documents that describe other models. Those with access to the classified SSEM documents can consult a user's guide (with the most complete description of SSEM output), a summary, two volumes of detailed descriptions of the submodels, and at least one document that discusses an application. One unclassified discussion of the model we found particularly useful is contained in a summary dated 31 March 1976. Like other available unclassified SSEM discussions (most of the rest are collections of TRW briefing charts), it is unpublished.

SSEM has been applied to as many real facilities as any global model. These include two facilities belonging to the original client, three State Department office buildings, a nuclear fuel cycle facility, and three nuclear weapon storage sites of interest to the Defense Nuclear Agency (DNA). Most recently, TRW has examined two NASA office facilities and a generic satellite tracking station. One of the State Department evaluations was carried out by personnel of that department. TRW has also transferred the SSEM code to the Nuclear Regulatory Commission and to DNA (which plans to modify it to produce a new model called Security Integration and Technology Evaluation of site-X--SITEX).

(8) Assessment--SSEM's pathfinding scheme is a good one, as are the criteria it can use in selecting critical paths. SSEM's capabilities which compare favorably with that in more recent models. Some of the independent submodels of SSEM are particularly attractive because they treat elements of security systems which are slighted in other evaluation schemes. SSEM's only serious omission is its inability to reevaluate its critical paths (including any combat engagements which may occur along them) once they

have been identified. TRW has plans to remedy this omission by acquiring models developed by other organizations (including SABRES II for combat engagements).

BIBLIOGRAPHY

Site Physical Security Final Report, TRW, Unpublished.

Anon., Planning Study Data Input Package, TR-78-1863-1, Informatics, Inc., May 1978.

Physical Security Model Final Report, Volume I, Summary, TRW, Unpublished.

Physical Security Model Final Report, Volume II, Model Description and Derivation, TRW, Unpublished.

Physical Security Model Final Report, Volume III, Model Description and Derivation (Continued), TRW, Unpublished.

Physical Security Model Users' Guide, TRW, Unpublished.

Demonstration of the TRW Site Security Evaluation Model, TRW, Unpublished.

"TRW Safeguards Assessment Model," Briefing to NRC, 12 March 1976.

Sikonia, R.F., "TRW Site Security Evaluation Model," TRW, February 1979.

TRW Site Security Evaluation Model Summary, 31 March 1976.

c. Path Analysis (PANL) (Sandia National Laboratories)--PANL was developed for Sandia (by TRW) as part of a global evaluation methodology in which the analyst plays a much larger role than he does in the more highly automated procedures described previously. PANL estimates the adversaries' probability of avoiding a confrontation with the security system. Together with a compatible version of another Sandia code called BATLE (described in section III.1.a (3) of this report), PANL can also estimate the adversaries' probability of mission success.

(1) Situation, adversary, and guard force description--PANL considers attacks on the facility by any of fourteen predefined types of groups, characterized as insiders or outsiders, with particular modes of transportation (in and out), possibly carrying metal tools, weapons, or explosives. If the analyst plans to consider combat engagements in evaluating the security system, he must provide BATLE information about numbers of adversaries, number of members and response time for each guard group, illumination level, and weapons type, level of training, and cover factor for each side. The adversaries may attempt sabotage (in which reaching the target to perform a malevolent act is the main concern) or theft (in which removal of protected material is as important as gaining access to it.)

(2) Pathfinding and performance measures--PANL shares the pathfinding task with the analyst, who may well bear the heavier part of this burden. First, the analyst prepares an Adversary Sequence Diagram (ASD): a schematic chart of generic path segments within the facility, for example outer fence to inner fence, or inner fence to building portal. Next, the analyst constructs a set of fault trees corresponding to the path segments of the ASD. Each fault tree is a description

of what must happen for the adversary to traverse the corresponding path segment. Finally, the anlayst uses the fault trees to derive expressions for minimal detection probabilities and minimal adversary delay times for each segment. (For attempted theft, the adversary delay for a given segment can be different on paths *to* the target, on paths *from* the target where the adversaries traversed the segment on their way in, and on paths *from* the target where the adversaries *did not* traverse the segment on the way in.) If he chooses, the analyst can provide sets of delays corresponding to several alternative security system configurations, for comparison later in the analysis.

PANL uses the detection probabilities and delay times to find optimal paths through the ASD. It considers paths for which the adversary has chosen to minimize detection probability up to each stage of the ASD (in turn), and to minimize time to the objective thereafter. The PANL/BATLE combination calculates the probability that the adversary completes his mission (even if one or more guard groups confront him) via each such path through the ASD, and identifies and ranks those paths for which the completion probability is unacceptably high. Alternatively, PANL alone (without BATLE) can identify and rank paths through the ASD with unacceptably low probability of timely detection (early enough for a security force to confront the adversaries within some prespecified response time).

(3) Documentation and Application--A classified TRW report on nuclear weapon storage site security systems contains the best published description we have encountered of PANL and the evaluation scheme in which it is used. Sandia has published a PANL user's guide with detailed instructions for use of the code on Sandia's computers. Sandia has used

PANL in examinations of several DcE facilities.

(4) Assessment--The PANL or (combined PANL/BATLE) codes are probably easier to use than either of the global evaluation codes discussed earlier in this report. Because an analysis using PANL depends critically on the quality of the Adversary Sequence Diagram and the evaluated fault trees produced by the analyst, however, a PANL facility examination comparable to a SAFE or SSEM examination may require more analyst skill and could require a comparable amount of analyst effort.

BIBLIOGRAPHY

Site Physical Security Final Report, TRW, Unpublished.

Cravens, N.M., Gallegos, M.H., Winblad, A.E., Clark, C.M., Gauthier, J.H., and Trujillo, D.A., Path Analysis (PANL) User's Guide, SAND80-1888, Sandia National Laboratories, September 1980.

d. Vulnerability of Integrated Safeguards Analysis (VISA) (Science Applications, Inc.)--SAI's VISA methodology has evolved considerably since it was described in the previous RDA survey. To distinguish the more recent version of this technique from its predecessor, SAI calls it VISA-2. Compared to the original VISA, VISA-2 places less emphasis on simulation (as opposed to judgement) as an evaluation tool. It also considers societal risk (as defined by NRC and DoE: attempt frequency times success probability times consequence) rather than just security system effectiveness when possible.

(1) Overview--VISA-2 evaluates a small number of key scenarios--involving a few key threats--to reach a quantitative estimate of security system effectiveness. First, the analyst chooses a few plausible "primary" threats (from a longer list of possibilities) on the basis of their higher risk. Next, for each primary threat he chooses one or more scenarios that are plausible and that present a high probability of adversary success. For each such scenario, the analyst determines some quantitative measure of security system effectiveness (MOE). He then aggregates the MOEs for all the scenarios associated with each primary threat. Finally, he combines aggregate measures of effectiveness for the various primary threats to produce a single global figure of merit for the security system.

Depending on the nature of the application and the resources available to him, the analyst can use a variety of techniques for each of the analytic and synthetic parts of the procedure. In analysis, he can use either estimation (simple or detailed) or simulation (again at various levels of detail, employing either available computer codes or field tests). In synthesis, he can choose worst case measures of effectiveness, or any of several weighted averages.

(2) Threat screening--VISA-2 establishes a collection of threats for screening by considering each of the malevolent acts to be prevented and each type of adversary likely to attempt such an act. The analyst identifies the most plausible combinations of adversary type and act, and screens those threats according to the risk they pose. When he can estimate each factor to his satisfaction, the analyst considers all of the three quantities whose product defines risk: probability of attempt; probability of success, given an attempt; and consequence, given a successful attempt.

(3) Scenario screening--For each of a set of primary threats chosen for their high score in the risk screening, the VISA-2 analyst constructs a number of scenarios. He does this by considering a range of possible target characteristics; adversary capabilities and tactics; and threatened system conditions. From these, the analyst selects those combinations which would be most attractive to the potential adversary. SAI suggests the use of several possible techniques for this screening, including gaming exercises, field tests and "global" modeling.

(4) Scenario evaluation--VISA-2 asks the analyst to assign a quantitative measure of security system effectiveness in each of the primary scenarios selected in the screening process. The MOE, defined as the probability that the adversary fails, ranges from a value of one for a perfect security system to zero for a system which is non-existent or totally ineffective. SAI suggests a correspondence between adjudged levels of security system effectiveness (e.g., "very high," "moderate," "low") and quantitative probability values which they feel is neutral as between defense- and offense-conservatism. The analyst

is to divide the scenario into segments (e.g., entry for theft, weapon acquisition, weapon removal); separately estimate the adversary success probability for each segment--considering both covert and overt attempts; and combine these success probabilities with detection probabilities to obtain an overall security system MOE for the scenario. Alternatively, SAI suggests that he might use gaming, a field test, or a scenario evaluation model to determine an MOE. In the near future, SAI plans to extend the scenario evaluation to consider security system actions to mitigate the consequences of the malevolent acts.

(5) Scenario and threat synthesis--The VISA-2 analyst combines the primary scenario MOEs in a systematic way to deduce a global measure of effectiveness for the security system. First, he aggregates all scenario measures associated with a given primary threat. He can choose the lowest MOE or an average (possibly weighted by plausibility) of MOEs for the various scenarios. Then he averages the figures of merit for the various primary threats, possibly weighting the figures according to consequence or risk involved.

(6) Documentation and applications--VISA-2 was only recently developed, and is still somewhat fluid. Its only published documentation is an abstract of a paper to be presented at a meeting. We found somewhat more detail in unpublished collections of SAI briefing charts. VISA-2 has had two applications, both concerned with nuclear weapon site security. They were carried out by a team consisting of VISA-2's developer, a site expert and a former member of the Special Forces.

(7) Assessment--VISA-2 is more accurately described as a framework for evaluation than as a model. The large measure of flexibility that VISA-2 provides may allow a team of experienced analysts to carry out useful facility evaluations very economically. The analysts should carefully record their assumptions and judgements during such evaluations (SAI did this in the example we examined), and the ultimate user should carefully examine them. Less experienced or less knowledgeable evaluation teams may find other, less flexible tools better adapted to their needs. (Such analysts could use these tools *within* the analytical segments of VISA-2 if they desire.)

BIBLIOGRAPHY

Harris, L., and Owel, W.R., "VISA-2 A General Procedure for Assessing the Safeguards Risk of Nuclear Facilities," Abstract, 1981 INMM Annual Meeting, Science Applications, Inc., April 1981.

Kull, L., Harris, Jr., L., and Glancy, J., "VISA--A Method for Evaluating the Performance of a Facility Safeguards System," Nuclear Materials Management, Fall 1977, pp. 292-301.

Donnelly, H., et. al., VISA: A Method for Evaluating the Performance of Integrated Safeguards Systems at Nuclear Facilities (2 Volumes), SAI-77-590-LJ, Science Applications, Inc., 30 June 1977.

e. Aggregated Systems Model (ASM) (Lawrence Livermore National Laboratory and Applied Decision Analysis)--LLNL developed ASM to help the Nuclear Regulatory Commission evaluate and choose among alternative systems to protect against possible diversion attempts in facilities that handle SNM. ASM combines information about safeguards component effectiveness, adversary characteristics, diversion consequences and safeguard costs. The ASM analyst collects performance data from facility personnel. The data can be subjective, for use in preliminary assessments, or they can be results from detailed subsystem analyses, for use in more elaborate studies. ASM attempts to provide a global evaluation of a candidate safeguards system by considering several analyst-specified diversion strategies, and choosing and examining the one that most seriously threatens the facility. ASM considers adversary deterrence more explicitly than any of the other evaluation techniques we surveyed for this report.

ASM consists of several components. The ones that deal with security system effectiveness treat possible adversary activities leading to theft of SNM; they treat safeguard system provisions for detecting these activities and identifying their perpetrators; and they treat interactions between adversaries and the safeguards system. (As was noted by a previous reviewer in reference 6, an additional planned code section that would provide specific component cost and performance information for consideration in designing safeguard system improvements is not yet documented.)

The ASM analyst considers standard classes of potential adversaries, who may be insiders or outsiders and may have major or minor equipment. The adversaries may include persons who exercise authority over elements of the safeguards system, and the adversaries may enjoy assistance from colluding insiders. They may seek enough SNM for a weapon or less than that. They may carry out their mission all at once or over a period of time. ASM adversaries have analyst-specified probabilities (per unit time) of attempting a diversion. After carrying out a preliminary ranking based on some of these data, the ASM analyst considers only a few (most threatening) types of adversary in subsequent evaluations. For each adversary considered, he chooses several generic diversion paths expressed as lists of safeguard system elements that might detect the adversary. ASM uses a set of parameters for each type of adversary to describe the adversary's level of aversion to detection and capture, and his eagerness to carry out the diversion.

ASM derives a measure of performance for each diversion path by considering up to six detection events. The detection events can involve single detectors or can reflect aggregate performance measures for several components. Events may include electronic detection (by quantity estimators, process monitors, personnel monitors, procedure monitors), visual detection (by stationary guards, roving guards, two-person rules), or detection by means of records (the accounting system, physical inventories). Performance measures (at any level of aggregation) can reflect experimental data or judgement. ASM often groups detection processes to simplify subsequent analysis.

The ASM analyst examines interactions between adversaries and the system's detection elements by considering decision trees that include facility design choices, adversary stategic and tactical choices (within a limited range of options), and stochastic events associated with adversary detection, identification and capture. ASM pays particular attention to adversary tactical decisions, in which, at the outset of each action, the adversary decides if he should continue or be deterred. In making these decisions, the adversary balances his desire to carry out diversion against the probability that he will be identified. The end events of the decision trees can include successful diversion, partially successful diversion, partially successful diversion, deterrence, or capture. ASM uses these trees (carrying out a Markov "lottery" over the stochastic events) to identify the adversary's preferred choices and to evaluate the safeguard system's expected performance given those choices.

LLNL has published several documents describing evolving versions of ASM, each adapted to a particular application. These publications use non-standard definitions for some safeguards terms, which is an unfortunate distraction. None of the publications we examined would provide an analyst who had not participated in ASM's development with sufficient information to use the technique in a facility evaluation. (One particular area of ambiguity is the exact role of the ASM computer codes vis-a-vis that of the analyst.) LLNL has applied ASM in examinations of two nuclear material fabrication facilities, and has used the results to advise NRC on more general regulatory matters.

The capabilities ASM provides, particularly with respect to treatment of adversary deterrence, may well be useful in some facility examinations. LLNL plans to publish an ASM user's manual shortly. This should make assessment and exploitation of ASM's potential easier.

BIBLIOGRAPHY

Wissenberger, S., Aggregated Systems Model of Nuclear Safeguards, Volumes I and II, NUREG/CR-1140, UCRL-52712, Lawrence Livermore National Laboratory, February 1980.

Value-Impact Analysis of Material Control and Accounting at Vallecitos Nuclear Center, Lawrence Livermore National Laboratory, Unpublished.

Value-Impact Analysis of Material Control and Accounting Upgrade Alternatives, Lawrence Livermore National Laboratory, Unpublished.

e. Safeguards Upgrade Rule Evaluation (SURE) (Sandia National La'oratories--Sandia developed SURE to help the Nuclear Regulatory Commission implement a proposed set of performance-oriented regulations (10 CFR 73.45) for licensing of fuel cycle facilities. SURE consists of an elaborate series of questionnaires concerned with performance of individual security system components, together with a set of rules for aggregation of the responses based on a decomposition of the performance requirements. SURE evaluates predicted overall system performance relative to required performance. SURE uses a computer for scoring of the questionnaires, and for aggregation of the responses in accord with SURE's rules. SURE does not utilize modeling techniques. It treats adversary capabilities and strategy only implicity.

The current version of SURE consists of 97 component effectiveness questionnaires to evaluate specific detectors, barriers, portals, guards, guard procedures, pieces of guard ·uipment, and design features. It also includes four system evaluation questionnaires to examine combinations of components acting together to perform a given task, or systems that operate in ways that makes simple formulas for aggregation of component data inappropriate. In particular, the system questionnaires examine alarm assessment, alarm reporting, security system communications, and penetration sensing, making reference to appropriate component questionnaires when necessary.

Each component questionnaire consists of about ten to fifteen questions concerned with equipment operation and design factors such as environmental conditions, reliability, vulnerabilities, and maintenance activities. Procedure questionnaires are similar in length, and inquire about conditions of performance (including site conditions), training and proficiency levels of performers, and vulnerability considerations.

SURE aggegates responses to the questions in a five-level hierarchy: to component performance measures, then low-level task performance measures, then sub-function measures, then system function measures and finally to the performance capability measures required by 10 CFR 73.45. (If several areas are to be protected at an installation, the analyst must carry out a further aggregation of performance measures for the separate areas.) Sandia states that the questions should be weighted (in aggregating responses) on the basis of contribution of the condition represented by the worst possible response to component failure; that the questions within a questionnaire should be grouped to consider separately distinct modes of failure; and that aggregation rules within a questionnaire should reflect a fault tree for component failure. Because such an aggregation scheme would have been expensive to develop, the published version of SURE gives all responses a uniform weight (0.5), except those judged trivial or "nonperformance oriented," which get a weight of 0.0. It treats each questionnaire as a single undifferentiated group of questions, and it uses a uniform aggregation rule for all questions. At the higher levels of aggregation, above that of the individual questionnaire, SURE uses rules that its developers selected as most reasonable. In some cases their choices fall short of stringent defense conservatism. Other choices can be made using the interactive computer program if desired.

SURE is described in a Sandia/NRC overview document, and in a two-volume design and evaluation guidebook that includes a complete description of the computer program. SURE has had a limited test, in which Sandia evaluated a candidate security system (for a material access area with a plutonium vault) designed by Allied General Nuclear Services using the NRC design guidance that accompanies SURE. The security system, considered "good" by AGNS, received an overall score of 0.3 on a scale of 0 (poor to non-existent) to 1 ("excellent"). NRC has not yet established an acceptance level that would assign regulatory significance to this score, or to the (similar) subscores related to specific performance requirements.

The current version of SURE is tied so closely to 10 CFR 73.24 that its direct utility to non-NRC users is limited. We examined it to determine if adaptations of SURE's approach might be useful to DNA. Many of SURE's component and system questionnaires treat factors which are important to performance at either nuclear fuel cycle facilities or weapon storage sites. An evaluation tool for use in certification (like the current version of SURE) is generally somewhat lenient, so that good non-ideal systems can be certified. Changes in SURE's aggregation rules could produce a more defense-conservative methodology designed to highlight important vulnerabilities for further examination.

BIBLIOGRAPHY

Bennett, H.A., and Olascoaga, M.T., Evaluation Methodology for Fixed-Site Physical Protection Systems, NUREG/CR-1590, SAND80-0505, Sandia National Laboratories, September 1980.

Bennett, H.A., and Olascoaga, M.T., Design Guidance and Evaluation Methodology for Fixed-Site Physical Protection Systems

Volume I : Description, Implementation, and Testing of Design Guidance and Evaluation Methodology.

Volume II: Component Selection Matrices and Effectiveness Test Questionnaires.

NUREG/CR-1198, SAND79-2378/1,2, Sandia National Laboratories, July 1980.

g. Matrix Analysis of the Insider Threat (MAIT) (Science Applications, Incorporated)--The MAIT method is concerned with threats that arise from access and control privileges granted to facility employees. MAIT makes no distinction between disloyal employees, loyal employees coerced to cooperate with adversaries, and external adversaries who manage to exercise privileges normally reserved to employees. MAIT makes no attempt to examine threats which involve other possible modes of adversary behavior (such as the use of force) that might be used to achieve malevolent goals. Within the limits set for it, the analysis is intended to be conservative and thorough.

At the heart of the MAIT procedure is a systematic enumeration of certain characteristics of the facility and its security system--including key administrative procedures. The analyst makes this enumeration during the preparation of a series of checklists (binary matrices) which constitute the main input to MAIT's computer code. (A convenient command language facilitates entry of the matrices.) Contents of the checklists are summarized in Table 2. The MAIT code combines the information in the checklists to identify persons and combinations of persons who can use insider privileges to seriously threaten specified assets.

(1) Facility description--MAIT's description of the physical layout of the facility is contained in two of its six major checklists. The first of these, Matrix 1, specifies movements from one location in the facility to another that are possible for the adversaries. Generally, the matrix that represents this information is sparse. Because Matrix 1 can be asymmetric, one way portals (and portals that monitor motion in only one direction) can

TABLE 2. MAIT CHECKLISTS (BINARY MATRICES)

FACILITY DESCRIPTION

1. ALLOWED MOVEMENTS FROM LOCATION TO LOCATION
2. LOCATION OF SECURITY SYSTEM ELEMENTS

SITUATION SPECIFICATION

3. SECURITY SYSTEM ELEMENT APPLICABILITY TO SPECIFIC THREAT TYPES
4. SECURITY SYSTEM ELEMENT OPERATION UNDER SPECIFIC FACILITY CONDITIONS

INSIDER PRIVILEGES

5. ACCESS (PAST SECURITY SYSTEM ELEMENTS) BY AN INSIDER OR INSIDER PAIR
6. CONTROL OF SECURITY SYSTEM ELEMENTS BY AN INSIDER OR INSIDER PAIR

be easily represented. Execution of MAIT begins with generation of a path--based on the information contained in the allowed-movements matrix--from a specific starting point to a specific target location, and (in the case of theft) to a specific terminal location. Other paths will be similarly generated until all such paths have been examined.

The MAIT analyst completes the facility description by assigning each element of the security system which is to be considered to one of the locations. Portals are often listed as separate locations in the first (allowed-movements) matrix so that protective devices associated with the portals can be precisely placed in this assignment. The security system device location matrix which results, Matrix 2, is used to transform each of the generated paths (through a series of locations) into a list of devices encountered along the path.

The security elements list representing the path is modified by information in checklists 3 and 4. One of these, Matrix 3, embodies MAIT's recognition that all security system devices may not provide protection in each of the threat situations to be considered. Two obvious examples are the inapplicability of explosive detectors to scenarios for theft of SNM in which explosives are not used to penetrate barriers, and the inapplicability of SNM detectors to sabotage situations in which SNM is not removed from the facility. In theft analyses, MAIT maintains separate versions of this list for the path in and the path out, to reflect such factors as a detector to sense stolen material, or a standard practice of search upon exit.

Checklist 4 reflects the fact that different sets of security system devices generally operate during different facility situations. For instance, certain procedures and alarms may be ignored during emergencies, extra guards may be assigned to oversee transfer operations, etc. SAI is developing modifications which will allow MAIT to treat changes of condition during a scenario (at a point most advantageous to the adversary). Limiting the list of protective devices to only those applicable to the given threat and facility condition is more conservative (and more realistic) than mechanically applying all devices to every situation.

(2) Treatment of access and control privilege--The two remaining checklists, 5 and 6 determine how close the adversaries with certain employee privileges can come to defeating the security system by exercise of those privileges along the path under examination. Matrix 5 records the access privileges of each potential adversary or pair of adversaries. It lists the protective devices which, though active, will not alert the security system when encountered along that particular adversary's (or adversary pair's) path. One typical example is a controlled portal that might be entered by an outsider adversary with a counterfeit identification badge. Another is a guard post which could be passed with impunity by a disloyal employee who normally passes the post in the course of his work.

For each hypothesized adversary and adversary pair in turn, protective devices which could be defeated by exercise of access privileges are removed from the list of active security system elements. The path is then further examined using MAIT's last checklist, Matrix 6. That list (the second matrix in this group) records control privileges: the ability or inability of each employee or employee pair to prevent each of the protective devices from alerting the security system when it otherwise would do so. Examples of such control privileges include a potentially disloyal guard's ability to ignore an alarm it is his duty to monitor or a coerced maintenance worker's ability to disable a sensor he is sent to check. By comparing the list of remaining active safeguards with this matrix, MAIT can determine how many protective devices remain functional when each hypothetical adversary or pair of adversaries use their access privileges along the path, and they are assisted by each employee or employee pair who might collude with them by exercising control privileges. Very short or non-existent lists of remaining functional system elements indicate potential deficiencies in the system.

(3) Presentation of evaluation results--MAIT's computer code can provide output at two levels of detail. The first--a summary--is always produced. It presents statistical performance measures. The second--more detailed--is produced only on request (by a post-processor of several MAIT working files). It presents the details of the entire analysis. MAIT's single most important measure of performance is a table listing the frequencies with which paths with zero, one, two, etc., protective devices remaining active (after exercise of privileges) occurred in the total set of paths. MAIT identifies security elements which occur *and are defeated* frequently along paths for which few protective devices remain. These elements represent high-leverage opportunities for security system improvements. The devices which most frequently *remained functional* in these short-list paths are also identified, to allow the analyst to examine their adequacy. Finally, MAIT identifies the most threatening persons and pairs of persons.

(4) Computational requirements--The MAIT computer codes were developed on SAI's DEC System 10 computer system. MAIT is written in FORTRAN. Its memory requirements (about 42,000 32-bit words) fall within the range available at many central computing facilities. MAIT has also been implemented on the Naval Surface Weapon Center's Interdata 7/32 minicomputer, and on SAI's secure VAX 11-780. SAI reports that simple benchmark examples require one to a few minutes of execution time and that an elaborate treatment of a real facility required 45 minutes on the relatively slow System 10.

(5) Documentation and application--SAI has published a user's manual containing a description of the method, detailed instructions for input preparation, a list and discussion of the computer codes, and sample input and output. The Naval Surface Weapons Center has prepared a technical note which discusses its (cleaner) version of the computer codes in exhaustive detail. SAI has helped DoE apply MAIT in a storage site evaluation (in parallel with other evaluation techniques).

(6) Assessment--The MAIT methodology addresses only a limited part of the security system evaluation problem. It does so simply, systematically, economically, and relatively thoroughly. An analyst with a background in security systems rather than modeling should be able to use it with only a modest amount of training. Within its range of concern, it is a valuable security system evaluation aid.

BIBLIOGRAPHY

Monroe, R.W., NSWC-TN-80-521, Naval Surface Weapons Center, unpublished.

Six, D.E., and Nichols, D.H., "DoE Contractor Vulnerability Analysis: DPA or MAIT?", Journal of Nuclear Material Management, IX, 427-433 (1980).

McDaniel, T.L. and Huszar, L., Safeguards Against Insider Collusion; The MAIT (Matrix Analysis of the Insider Threat) Method for the Analysis of Facility Safeguards Against Insider Collusion--User's Manual, NUREG/CR-0532, SAI-78-996-LJ, Volume 2, Science Applications, Inc., December 1978.

NiCastro, J.R., Woolson, B., and Glancy, J., Internal Threat Analysis, SAI-77-947-LJ, Science Applications, Inc., 30 November 1977.

h. Safeguard Vulnerability Analysis Program (SVAP) (Lawrence Livermore National Laboratory)--LLNL designed SVAP to reveal vulnerabilities of nuclear facilities to diversions (thefts) by non-violent insiders. SVAP examines physical security, material control, and material accounting (the latter--not discussed further in this review--over four different time intervals). At the start of a SVAP analysis, the analyst gathers a very detailed description of the facility and its procedures using a data collection workbook. He restructures the data and then enters them into a microcomputer that produces an input tape for the SVAP main program. Because SVAP analyses are structured to support NRC licencing reviews, the anlayst and the program generate an unusually complete documentary record in the course of a facility examination.

(1) Facility, adversary, and guard force description--SVAP describes the facility in terms of locations through which the adversaries can pass during a diversion, monitors that can detect people or materials at a location, a transmission system that carries monitor messages to the guard force, and a utility system that provides power, etc., to support the operation of the safeguards system. SVAP describes potential adversaries (facility employees) solely in terms of their access or control privileges. SVAP guards are described explicitly only to specify the location(s) to which they respond when a given alarm sounds. Guards may also be included among the security system's various monitors.

(2) Analysis and performance measures--The physical security and material control section of SVAP first separately examines five potential sources of vulnerability: inadequate monitoring, inappropriate guard response, failures of the transmission system, failures of the utility system, and vulnerability of the material-control-documentation system to

forgeries. First, in the monitor analysis, SVAP identifies diversion routes with exit paths covered by three or fewer detectors. Then, in the response analysis, it finds paths for which guards go to locations other than ones on the exit route in response to an alarm. Next, in the transmission system analysis, SVAP searches for theft attempts in which receipt of an alarm depends on two or fewer independent transmission paths. In the utility system analysis, SVAP looks for situations in which failure of two or fewer elements of the utility system could allow an undetected diversion. Finally, in the material-control-document analysis, SVAP identifies sets of documents required to move protected material out of the facility legitimately along various paths (there will always be at least one such set).

After SVAP has examined each of these separate sources of vulnerability, it performs a more stringent analysis to identify combinations of circumstances and acts--possibly including monitor, transmission system or utility system failure, inappropriate guard response, or document falsification--that could allow diversion that would not alert the security system. The failures considered can arise from "normal" outages or from adversary action (in which case SVAP identifies the potentially dangerous adversaries).

For each target examined (up to ten in a single run) SVAP output includes a summary that lists the numbers of: paths covered by three or fewer monitors; paths for which guard response is inappropriate; situations in which transmission of an alarm depends on two or fewer paths; situations in which failure of two or fewer elements of the utility system would thwart detection; and sets of colluding insiders who (with "assistance" from random security system failures could carry out undetected diversion. SVAP summary output also includes graphs of probability of adversary success versus number of colluding insiders. In another output section, SVAP presents more details of both the separate and combined vulnerability analyses. It identifies specific sets of security system elements involved in each vulnerable situation. These lists culminate in one that identifies combinations of colluding insiders who can divert material without generating an alarm (possibly with "assistance" from one or more random failures).

(3) Computational requirements--The input phase of the SVAP code uses a Tektronix 4050 series microcomputer, which can also be used to receive output at a remote location. The main vulnerability analyses are carried out on a large main frame computer (a CDC 7600 at LLNL). The most demanding section of the program is a Sandia code called SETS, which manipulates boolean equations. SETS has variable storage and computer time requirements. From time to time, for sufficiently large or ill-structured problems, SETS's needs exceed the practical capacity of the 7600. (LLNL is seeking a replacement for SETS that will allow SVAP to avoid these difficulties and run on a smaller machine.)

(4) Documentation and applications--SVAP documentation does a good job of telling the user what should go in and what will come out, but it says very little about what happens in between. SVAP has been applied to two storage vaults and three fabrication facilities.

(5) Assessment--within its range of concern, SVAP supports a detailed and exhaustive examination of a facility. We expect that a thorough SVAP evaluation will be somewhat demanding of analytic resources, partly because SVAP considers a lot of information and partly because the data collection handbook currently requires more human handling of data than it should. Investment in a SVAP analysis may well be justified for a complex installation like a nuclear fuel cycle facility. SVAP may be less cost-effective when applied to simpler systems.

BIBLOGRAPHY

Gilman, F.M., Dittmore, M.H., Orvis, W.J., and Wahler, P.S., Safeguard Vulnerability Analysis Program (SVAP) Executive Summary, NUREG/CR-1169,ES, UCRL-52724, Lawrence Livermore Laboratory, April 1980.

Wahler, P.S., Safeguard Vulnerability Analysis Program (SVAP) Data Gathering Handbook, Volumes I and II, NUREG/CR-1169, UCRL-52731, Lawrence Livermore Laboratory, April 1980.

Orvis, W.J., Safeguard Vulnerability Analysis Program (SVAP) User's Manual, NUREG/CR-1169, Volume III, UCRL-52730, Lawrence Livermore Laboratory, May 1980.

i. Sensor System Nullification by Insiders (SSNI) (Sandia Laboratories, Albuquerque)--Another approach to examining the vulnerability of a protection system to insider adversaries who tamper with its parts was proposed by Sandia Laboratories in a report published in early 1978. It uses boolean equations to represent certain features of the security system and manipulates those equations (using a computer code called SETS) to identify security system deficiencies. The product is a list of combinations of insiders who, by exercise of their otherwise legitimate privileges, can clear a path for removal of a protected assets from the facility.

So far as we know, automated assistance for construction of the required boolean equations has not been developed (but see the description of LLNL's SVAP in the section that preceeds this one). The Sandia modeling group has continuing plans to extend its capability to evaluate threats posed by insider adversaries.

BIBLIOGRAPHY

Boozer, D.D., and Worrell, R.G., A Method for Determining the Susceptibility of a Facility to Sensor System Nullification by Insiders, SAND77-1916C, Sandia Laboratories, Albuquerque, February 1978.

Worrell, R.B., and Stack, D.W., Common Cause Analysis Using SETS, SAND77-1832, Sandia Laboratories, Albuquerque, December 1977.

Worrell, R.B., Set Equation Transformation System (SETS), SLA-73-0028A, Sandia Laboratories, Albuquerque, May 1974.

j. Structured Assessment Analysis (SAA) (Analytic Information Processing and Lawrence Livermore National Laboratory)--The SAA approach calls for a discrete series of successively more stringent evaluations of a security system, to uncover first its most serious omissions and then its more subtle shortcomings. SAA was developed by LLNL to assess the capability of material control and accounting systems to prevent or detect diversions (theft) at facilities which handle special nuclear materials. We included SAA in this survey of physical-security-system evaluation techniques because material control systems include physical security elements, and because SAA examines adversary attempts to tamper with a security system in more detail than other techniques that treat possible malevolent activities by insiders.

SAA uses sets of boolean equations to represent the relevant features of the protected system, and manipulates the equations to accomplish its analyses. In SAA's first evaluation, its object is to determine if the adversaries can accomplish their mission undetected, i.e., if all potential diversion paths are "covered." In addition, at this stage SAA identifies the sets of protective measures that prevent diversion from each of the target sets (potential diversion paths specified by the analyst at the outset of the analysis) that are found to be protected. This allows the analyst to identify individuals or sets of individuals who might "uncover" a target set.

At stage two, SAA examines the adequacy of coverage by determining if (at normal levels of component performance) the probability of detecting an adversary who tries to carry out a diversion is acceptably high. SAA does so by deriving and evaluating boolean equations for probability of detection by the entire set of measures that provide protection along each diversion route. Stage two considers the average effects of routine common-cause failures that might affect several detectors (such as power interruptions), but assumes that the adversaries have neither knowledge of nor control over the status of any component of the security system.

In its third stage, SAA assumes that potential adversaries are aware of component status, and calculates the frequency with which potential diversion routes become uncovered (allowing riskless diversion by a knowledgeable insider) during "normal" interruptions of component operation.

In stage four, SAA considers adversaries who are both knowledgeable and aggressive. These adversaries actively tamper with the security system, possibly in quite sophisticated ways including interference with auxiliary support systems and with systems that monitor for tampering. SAA's stage four adversary's strategy is to expand adversary influence over components and locations as far as possible (starting from what was originally authorized) without being detected. Simulation of this process in a complex facility is a formidable task, which can grow beyond the capabilities of even a large computing facility like Livermore's. As a result, LLNL has sometimes had to limit or partition its stage four examinations. (Stages one through three are much less demanding.)

SAA is now documented by a multi-volume description structured to support the use of SAA in NRC's licensing proceedings. (We have not examined the forthcoming Volume IV, which includes code listings and technical discussions of SAA's analytic techniques.) SAA was used in examinations of four fuel cycle facilities (two of them hypothetical), and is to be used in two more NRC evaluations (one of them by NRC personnel) in FY 1982.

SAA is a formidable tool, with substantial capability for examination of sophisticated diversion possibilities in complex fuel cycle facilities. Full use of this capability is expensive, but may be a good investment where appropriate. DNA's physical security problems appear to be simpler, and probably do not require SAA's deepest analyses. Less elaborate techniques (possibly including SAA through stage three) are more suitable for most physical security evaluations.

BIBLIOGRAPHY

Parziale, A.A., and Sacks, I.J., The Structured Assessment Approach, Version I, Volumes I, II, III, NUREG/CR-1233, UCRL-52735, Lawrence Livermore National Laboratory, October, 1979 (Draft).

Parziale, A.A., Sacks, I.J., Rice, T.R., and Derby, S.L., The Structured Assessment of Facility X, Voulme I, Executive Summary, Lawrence Livermore Laboratory, 8 January 1979.

Sacks, I.J., "Techniques for the Determination of Potential Adversary Success with Tampering (Level 4.1)," MC-78-929-D, Lawrence Livermore Laboratory, 17 October 1979.

Sacks, I.J., Schrot, M., Long J., and Pariale, A.A., "A Structured Approach to the Assessment of Material Control and Accounting Procedures," MC-78-203, Lawrence Livermore Laboratory, March 1978.

2. SCENARIO SIMULATION METHODS

a. Security System Performance Assessment Method (SSPAM) (Mission Research Corporation)--The SSPAM concept is an ambitious attempt to carry out simulations which consider every physical and psychological factor of importance in determining an attacker's success against a physical security system. It envisions a three-tiered complex of computer codes which simulate the events of an hypothesized attack at low, medium, or high level of detail, as suitable to the user's particular application. MRC is now implementing the concpet, but has not yet produced a fully operational version. We described the full, conceptual version of SSPAM here, because it is the goal toward which the developers are proceeding. We also try to indicate where they are now along the road.

(1) Situation modeled--SSPAM is designed to simulate most situations which might plausibly arise at a protected facility in a fairly natural and straightforward way. The analyst first provides a detailed description of the people, procedures, structures, hardware, and environment that are to form the backdrop for what follows. A scenario is then provided in the form of an ordered list of objectives for each person (or each group of persons who are to act together). These lists are plans, not prescriptions. In response to changes in circumstances and perception during the course of the simulation, SSPAM may insert new objectives, or delay or abandon old ones. (One qualitative measure of the security system's success is the number of [illegible] objectives it forces the attackers to pursue.) SSPAM provides a range of guard and adversary objectives that is sufficient to allow for realistically complex strategy and tactics.

It treats insider adversaries straightforwardly within this framework by simply assigning them both guard and adversary objectives. SSPAM will treat both stealth and deceit on the part of the adversaries explicitly. For stealth, the method provides for evidence, which guards may discover, to be left in the course of certain adversary activities. For deceit, the method (in a future implementation) will evaluate attempts to use deception to evade certain administrative control.

(2) Adversary and guard force descriptions--Each person (or group of persons) who is to participate in the simulation is described in considerable detail. This description includes information about equipment (including transport, tools, weapons, and ammunition); physical, physiological, and psychological condition of personnel; access and control privileges; attitudes and skills; perceptions of the situation; and objectives. Objectives which might be pursued by any of the participants include movement to a specified location, identification of another participant, tracking or interception of another participant, or engagement of an opponent in combat.

Important possible objectives used in adversary planning include passage through a controlled portal, penetration of a barrier, tampering with security system hardware, creation of a diversion, evasion of some element of the security system, hiding, and preparation for an ambush. In a future implementation, "nervousness" arising from failure to meet a preplanned schedule may degrade adversary performance, especially after a perceived detection.

Possible objectives for members of the security force include monitoring or patrolling of a post, arming or resetting a warning or deterrence device, assessment of an alarm, issuance of a warning or challenge, providing escort for sensitive materials, changing guard shifts, and carrying out a search for persons or evidence.

(3) Facility description--SSPAM maintains a threefold representation of locations within or adjacent to the facility. The description of an object (sturctural element or security system hardware element) or a person includes both cartesian coordinates and assignment to a cell in a grid. Cells are in turn grouped into larger sectors. This helps SSPAM specify environmental conditions and simplifies certain searches. SSPAM treats fences, more substantial barriers, and portals in a common fashion. Each is characterized by the expected value of the time required for penetration (a function of the techniques and equipment employed and the nature of the barrier). Penetration may be accompanied by the production of evidence, which may be transient (like noise) or persistent (like the fragments of a door destroyed by explosives). The analyst can locate security system sensors at appropriate locations in the facility model, including potential sites of penetrations. The method characterizes sensors by the type(s) of stimulus to which they are sensitive, the field of view they monitor, and their sensitivity to activation. SSPAM models activation processes in great detail. It sensor descriptions also include false alarm probability, susceptibility to tampering, and the nature of the signal produced when activated. Activated sensors send signals to alarms or displays. The code will eventually describe the characteristics of these signals in much more detail than is customary in security models. Many aspects of the simulation are affected by the physical environment at various sectors of the facility. SSPAM's dynamic description of this environment includes lighting levels, topography, and various manifestation of the weather.

(4) Combat engagements--SSPAM's authors intend to use ideas published as part of other evaluation procedures for low- and medium-level of detail simulations of combat engagements, but they have not yet implemented these simulations. Capability to simulate engagements at a high level of detail, in a way consistent in philosophy with the rest of the method, is under development. Like some of the other high-detail engagement models described in this report, SSPAM's will in part be an adaptation of an existing small-scale combat model (SRI's Firefight-2). The SSPAM engagement model focuses on the two opposing groups, rather than on individuals within the groups. Time is stepped in variable increments reflecting the different density of events at the outset and during the main part of the battle. At the beginning of each step, the model calculates the probability that each participant has detected and identified each opponent. This information is then combined with data from personal descriptions to decide which of the allowed engagement activities each group is most likely to select for that time step. After some provision is made for inertia, the model assumes that the group makes the most likely choice. Activities that SSPAM will eventually model including advancing, retreating, seeking cover or a lower profile, pursuing a fleeing or retreating opponent, surrendering, freezing or fleeing in panic, and splitting the adversary group so that some can proceed to the target while the engagement continues. (Currently, the model includes only firing events.) A group will be able to choose to fire during most of the activities, but not when suppressed by incoming fire and not during activities that involve panic or surrender. The code examines the physical circumstances--and outcome--of firing in considerable detail. The engagement continues until one group (possibly only a key sub-group) is annihilated, surrenders, or succeeds in withdrawing.

(5) Treatment of stochastic variables--SSPAM uses most probable values for the great majority of the many stochastic variables which enter into its simulations. On occasion, it uses single random draws to determine the outcome of stochastic events. These procedures are economical in terms of computer time, but provides a more limited evaluation of the security system than a Monte Carlo simulation, which could sample the various possible courses of events more fully. MRC has made provision for automatic repetition of a scenario, but envisions only small numbers of repetitions (for economy).

(6) Presentation of evaluation results--SSPAM ouput consists of a detailed log of the simulation, which includes information on the performance of elements of the security system and of the adversary force. In the future, it may include various summaries.

(7) Documentation and application--MRC's early description of the SSPAM concept was a model document. In addition to the specifics of SSPAM, it contained many thoughtful general observations about security systems and their modeling. Naturally, it fell short of the specificity one would expect in a user's manual. The newer documents describing MRC's actual implementation of SSPAM are not nearly so outstanding. Only someone well acquainted with computers and modeling in general--and with the SSPAM concept document in particular--can extract useful information from them easily.

So far--as is appropriate for a model in its present stage of development--MRC has exercised SSPAM only on a set of model problems. Some of the problems, however, involve activities at an actual site.

(8) Assessment--In the previous RDA survey we expressed some skepticism that all of what was planned for SSPAM would be reduced to practice quickly. Though we recognized careful attention to the requirements of implementation in the concept description, we were nonetheless pleasantly surprised by MRC's progress in the last year and a half. We still have some doubts about the practicality of credibly modeling some of the elements of human behavior which were or are to be included (and which may, of necessity, have to be included in a model which attempts simulation in this degree of detail.) MRC made some attempts to address this question in a study for the Naval Personnel Development Center, but the focus of the work changed before the issue was resolved.

In any event, further development and better documentation are required if SSPAM is to realize its potential. The results of MRC's attempts to exercise this methodology continue to be of interest to the security-system-evaluation community.

BIBLIOGRAPHY

Sanderlin, J., Johanson, G., and Lomen, P., Security System Performance Assessment Methodology, Phase II.; Volume I: Executive Summary; Volume II: SSPAM Descriptions; Volume III: SSPAM Results; MRC-R-564, Mission Research Corporation, April 1980

Sanderlin, J.C., and Rathman, C.E., A Concept for Assessment of Physical Security System Performance, Phase I; Volume I: Executive Summary; Volume II: Concept Description, MRC-7850-1-1278, Mission Research Corporation, December 1980.

b. Fixed Site Neutralization Model (FSNM) (Vector Research, Inc., for Sandia Laboratories, Albuquerque)--FSNM is an advanced scenario oriented model that is fully developed, but has not yet been entirely debugged, completely tested, or evaluated. It simulates the physical and mental events of an adversary attack in more detail than is routinely incorporated in any modeling system currently available. It is a logical successor to earlier Sandia models like FESEM and ISEM, which were designed to carry out as realistic simulations as were possible at the time of *their* design. An important advantage of FSNM's approach is that it insures the incorporation of considerable modeling insight into any study made with the code, even a study that is conducted by analysts with minimal modeling experience.

(1) Situations modeled--Unlike most scenario oriented models, FSNM does not require the user to specify the attacker's activities in exhaustive detail before the simulation commences. Instead, he provides an ordered list of adversary goals, along with sufficient information about the participants and the facility to allow the modeling system to construct the smaller details of the scenario. This construction is accomplished dynamically during each simulated participant's continuing decision-making process, which is based on evolving perceptions. A goal takes the form of a requirement for a specified number of adversaries to occupy a specified location for a specified period of time with a specified list of equipment. The structure of FSNM places few important restrictions on the range of activities that can be considered in a simulation.

(2) Adversary and guard force descriptions--The basic element of an FSNM model is the simulated human participant, who is called a player. Each player is modeled in considerable physical and psychological detail. At each time step of

the simulation, each player chooses an activity. The most common choices are moving, observing, or firing, but surrendering to or capturing another player are also possible choices. When he can, the player chooses in accord with plans based on orders received from his leader. When the orders are somewhat general--for instance to move to a particular location--the player may have to add additional details--in this case a route based on minimization of anticipated travel time and danger. When no orders are available to guide him, he acts in accord with a set of general rules that are part of his psychological description.

In all cases, the player's decisions take into account *his perception* of the people and things around him. The outcome of his attempt to take some action is determined by the *actual* condition of the people and things around him, by the capabilities of the player and his equipment, and often by a random draw from some probability distribution. Separate provisions for recording both apparent and true allegiance, together with personal plans for each player, allow natural and realistic treatment of both insider adversaries and guards who infiltrate the intruder force.

In the conceptual design of FSNM, leaders of forces (consisting of players with associated vehicles) were to develop orders for the members of their forces. Leaders of small forces were to themselves be guided by orders from leaders of larger units. Plans at all levels would have reflected user input, possibly in the form of a set of standard operating procedures. The planning process would have included random elements, and reflected differences in the leadership styles of different individuals. (The developers were not satisfied with their initial attempt to do all of this. They have not yet had an opportunity to refine their first attempt.)

Guards can become aware of intruders by direct observation or by monitoring a central alarm system. One guard is permanently assigned this monitoring duty. Awareness of an attack and the perceived details of its nature are communicated among the guards with high priority. Response of a given guard to information of this sort is determined by the orders he receives, his standard operating procedures, and rules of behavior that were specified with him.

(3) Facility description--The FSNM facility description is unusually detailed. A long and somewhat redundant list of entities--e.g., floors, walls, and roofs as well as the buildings they comprise--is included in that description. The status--open, closed, locked, or secured--of each door is recorded, along with its location and physical characteristics; windows and stairs are described in similar detail. FSNM specifies positions of facility entities by providing both cartesian coordinates (in two dimensions) and statements of their adjacency to other entities. A description of an alarm system sensor includes its location, its type, and a list of locations, occupation of which may activate the alarm. It also includes a record of the alarm's status (alert, off, or activated), the station to which the alarm reports, and the nature of the report provided.

(4) Combat engagements--FSNM does not treat combat engagements as special occurrences requiring a separate model but rather as ordinary events of the simulation. Like other events, they are played out in great detail. For instance, engagement simulations explicitly consider the physical capabilities and empirical effectiveness of each of five weapon types against each of seven target types. They also consider each player's perceptions, physical capabilities, and psychlogical tendencies in the physical setting and under the environmental conditions of the confrontation, as a function

of time. Regarding psychological factors, they are the equal of any of the rest.

(5) Mathematical approach and performance measures--Somewhat surprisingly, the mathematics of FSNM is, for the most part, straightforward. Often, the occurrence of an event of interest is assigned a probability that is then simply modified by a series of multiplicative factors that reflect the modeled circumstances surrounding the event. A smiliar process is used to modify simple parametric models of various entities to reflect the influences of a complex environment. The relative simplicity of the mathematics stands in contrast, however, to the complexity of the data handling problem created by the combination of such a large number of separate calculations. FSNM solves this problem by using specially ordered and indexed lists for many of its data and parameters. Other data (primarily those concerning performance) are stored in conventioanl arrays. Both types of data structure are established by preprocessors and then maintained by the main FSNM code. At the conclusion of a simulation run, which examines the scenario in question once, two sorts of output are available: a detailed chronology of the simulation and a snapshot of the final state of participating players and objects. Only a highly trained user could interpret this output easily.

(6) Computational requirement--The FSNM system is written entirely in FORTRAN, which would seem to make it easily portable from one computer installation to another. Unfortunately, this has not proved to be the case. As of this writing it has not been possible to use FSNM on systems other than the virtual storage operating system of the University of Michigan Amdahl 470V/6 computer, on which FSNM was first tested. At simulated time, step sizes of 1/2 second, CPU time approaches the real time modeled. The cost of a statistically adequate Monte Carlo treatment of a realistic scenario

(which should include at least several hundred repetitions) is likely to be quite high.

(7) Documentation and application--Though its development is not yet completed, FSNM has good documentation. A well-written overview provides a very adequate description of the range and logic of the model. It also discusses possibilities for obtaining or generating the myriad data required by FSNM, and the logic to be used in manipulating them. As an exercise, Sandia and Nuclear Regulatory Commission staff members prepared a complete set of FSNM input data corresponding to an hypothetical facility used for training exercises in NRC's Guard Tactics Simulation game. We have not encountered published descriptions of FSNM use in the evaluation of an actual facility. Sandia indicates that FSNM development has been discontinued for the present.

(8) Assessment--Construction of a comprehensive, state of the art model like FSNM can be a useful exercise in that it helps synthesize the current insights of the modeling community. We judge the FSNM exercise to have been successful, in that the FSNM overview is an excellent textbook of current modeling procedures. The utility of FSNM as a practical tool for security system evaluation, however, is yet to be demonstrated. In certain situations it could be quite valuable, but as noted above, its use would probably be costly.

BIBLIOGRAPHY

Engi, D., and Harlan, C.P., A Study of the Fixed Site Neutralization Model (FSNM), NUREG/CR-0787, SAND79-0873, Sandia National Laboratories, November 1979.

Engi, D., Chapman, L.D., Judnick, W., Blum, R., Brofgler[sic], L., Lenz, J., Weinraub, A., and Ballard, D., Fixed Site Neutralization Model User's Manual, NUREG/CR-1307, SAND79-2241, Sandia National Laboratories, December 1979. (This seems to be identical--except for authors--to the VRI user's manual cited below.)

Blum, R. and Proegler, L., Developments, Extensions, and other Improvements to the Fixed Site Neutralization Model FSN (Mark II), VRI-Sandia-3-FR78- , Vector Research, Incorporated, October 1978. (We were not able to obtain a copy of this in time to use it in preparing the summary above.)

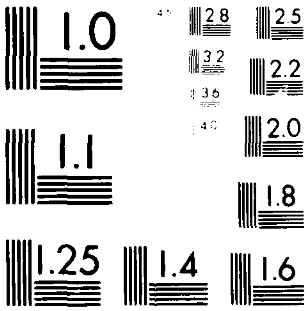
Ballard, D., Blum, R., Lenz, J., Proegler, L., Weintraub, A., Fixed Site Neutralization Model, VRI-Sandia-1-FR77-1, Vector Research Incorporated, 20 January 1978.

Judnick, W., Blum, R., Proegler, L., Lenz, J., Weintraub, A., Ballard, D., Fixed Site Neutralization Model User's Manual, VRI-Sandia-3-FR78-2, Vector Research, Incorporated, 9 June 1978.

Judnick, W., Blum, R., Proegler, L., Lenz, J., Weintraub, A., Ballard, D., Fixed Site Neutralization Model Programmer's Manual, VRI-Sandia-3-FR78-1, Vector Research, Incorporated, 9 June 1978.

AD-A109 726 R AND D ASSOCIATES ARLINGTON VA F/G 15/3
CURRENT METHODS FOR EVALUATION OF PHYSICAL SECURITY SYSTEM EFFE--ETC(U)
MAY 81 R B DAVIDSON, J W ROSENGREN DNA001-81-C-0109
UNCLASSIFIED RDA-TR-179200-001 DNA-TR-81-18 NL

2 OF 3
AD
A109 726



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

c. Protection System Evaluator (PROSE) (John E. Lenz, College of Business Administration, University of Wisconsin, Oshkosh)--PROSE bears a striking familial resemblance to FSNM. This is not surprising, as PROSE's author was an active participant in FSNM's development. PROSE's scope is somewhat broader than FSNM's in that it will model physical protection systems for both fixed sites and vehicles in transit. Conceptually, PROSE seems to have evolved by broadening ideas associated with combat engagement simulations to include other aspects of the confrontation between adversaries and the security system.

The resemblance between PROSE and FSNM is evident in the detailed attention they both devote to individual decision processes and to planning activities carried out by independent group leaders. A similarly wide range of simulated participant activities is available in the two models. Similar final measures of effectiveness summarize the course of both simulations. (PROSE's description mentions more activities and more measures of effectiveness than are available in the current version of FSNM.)

A distinctive feature of PROSE which makes it potentially attractive is its orientation toward events rather than slices of time. This *might* provide some relief from the massive computer time requirements characteristic of other high-detail scenario models. PROSE's fine-grained treatment of lines of sight and fire within and among buildings (and around vehicles, which are basically moveable buildings in PROSE) is another attractive feature, which might allow more realistic simulation of events on relatively small, clutter sites.

It is our understanding that while there is now a fairly detailed design for a PROSE code (as well as a concept), the design has not yet been translated into operational software.

BIBLIOGRAPHY

Lenz, J.E., "The PROSE (Protection System Evaluator) Model," Proc. 1979 Winter Simulation Conference, IEEE, 1979, pp. 319-328.

Lenz, J.E., The PROSE Model, a Protection System Evaluator, University of Wisconsin, Oshkosh (unpublished).

d. Safeguards Network Analysis Procedure (SNAP) (Pritsker and Associates for Sandia Laboratories, Albuquerque) --SNAP is a second-generation scenario oriented modeling system that allows for rather complex guard and adversary tactics and activities. It does so by providing a flexible specialized modeling language to describe the facility and the participants' actions within it. Along with the freedom SNAP's flexibility provides him, the user must accept a degree of responsibility for verification which is usually borne only by the originator of a high-detail scenario simulation model. SNAP's designers assume that its users will be sufficiently expert in security matters to welcome this responsibility.

Since the last RDA review, Sandia has set programs in motion to develop a SNAP Operating System (SOS) that should make SNAP easier to use. In one part of this effort, Sandia is developing a Graphical Input Editor (to allow entry and modification of SNAP input information from a CRT terminal) and a package of Safeguards Output Graphics (to provide a pictorial representation of the events of a SNAP simulation). Related efforts are devoted to developing code sections which will take information from Sandia's SAFE global modeling system and use it to construct the elements of a SNAP scenario model--corresponding to an interesting SAFE scenario--automatically. Finally, Sandia intends to include a library of standard model components in SOS. Sandia expects to have a documented version of SOS available at about the beginning of FY 1982.

(1) Situations modeled--There is no typical SNAP scenario. All SNAP models, however, consist of the same three parts. These represent the characteristics of the facility, the procedures of the guard force, and the planned activities of the attacker. As the scenario unfolds, the

three parts automatically interact with one another in a realistic way. The overall realism of the simulation thus depends upon the quality and compatibility of the three separate submodels. Unlike most modeling systems, SNAP places very few restrictions on the range of situations to which it can be applied. Some scenarios, however, can require much more skill for their construction than others.

(2) Adversary and guard force descriptions--The basic unit of a SNAP description of either the adversaries or the guard force is an activity, represented by a SNAP symbol. In addition to entry into or exit from the scenario, the major activities are performance of a task and waiting. Tasks can include all the standard adversary activities, including moving from place to place, penetrating a barrier, attaching explosives to a sabotage target, etc. Groups proceed from one activity to another according to a set of instructions specified in constructing the model of the scenario. These instructions may specify unconditional progress, branching of two or more subgroups to different paths, branching according to decisions based on current perceptions of the situation, or random choice of path consistent with some probability distribution. One of the things that can influence current perceptions is receipt of communications from allies or the alarm system. Associated with each activity is a distribution of times or a decision criterion which determines how long the activity will last. The facility location at which the activity takes place is also specified. (Movements from place to place can be specified implicitly during changes of activity.) SNAP's provisions for arbitrary (and changing) numbers of independent adversary groups and its sophisticated branching and decision-making elements should be quite useful in modeling real-world adversary strategies.

SNAP's treatment of insider assistance provides an instructive example of the range of scenarios that can be modeled by judicious combination of SNAP activities. It also indicates how much *modeling* strategy is sometimes required to cast common security situations into the SNAP format. The insiders enter the scenario in the guard force submodel and may initially carry out guard activities. At some point in the simulation they carry out a signaling activity, which activates an element of the adversary force which has been awaiting this signal (in a dormant state) since the beginning. The insiders are then removed from the guard force, and the newly activated adversaries proceed with their own agenda. One consequence of this approach is that after the transition it is somewhat awkward to have the insiders employ further deceit to accomplish their goals. It is also awkward to have them provide covert assistance to the attackers before the transition.

SNAP's model of guard force activity uses essentially the same set of symbols as its adversary activity model. (One difference in treatment is that SNAP pays special attention to allocation of members of the total guard force among the security system's assigned tasks.) In principle, a detailed set of standard operating procedures (SOPs) should be specified for the guards, covering both routine situations and responses to alarms, communications from other guards, etc. Because these SOPs include planned reactions to all comtemplated occurrences, they would typically be much more elaborate than the specification of adversary activities. To avoid the labor required to construct such an elaborate guard force description, the modeler may simplify the guard activity model to cover only those situations that have some impact on the specified adversary activities.

(3) Facility Description--Except for the special case of engagements, interactions of the adversaries and the guard force are mediated by the facility model. It provides the context for all activities and includes portals, spaces, barriers, and targets. Each of these can include an adversary detection device that may (with some probability) register the presence of adversaries and can be monitored by the guard force. At specified points within the facility adversaries can interfere with communication of alarms to the guard force. The SNAP facility description explicity identifies possible paths of movement from one part of the facility to another, and may specify whether travel can take place in either one or both directions.

(4) Combat Engagements--The duration and outcome of any combat engagement that may occur during the SNAP simulation is determined by a modified version of BATLE, a simple discrete-state attrition-rate confrontation model described elsewhere in this report. Guard and adversary group characteristics that are used by BATLE are specified as part of the input data for SNAP. These characteristics include type of weapons, firing proficiency, and number of members in the group. If more than one group of guards (or adversaries) arrives at an engagement, the groups remain separate. (They can, however, be merged during a wait either before or after the engagement.) At some times, some adversaries are immune from engagement by the guard force. This is SNAP's mechanism to represent successful hiding.

(5) Mathematical approach and performance measures--SNAP models use the mathematics of interacting networks. The adversary and guard activity networks are dynamic, with their transactions representing the movements of the respective forces. The facility model is, in this sense, static, though its interactions with the other networks affect their dynamics.

SNAP models that contain stochastic elements (almost all do) use Monte Carlo techniques to average their results over the various distribution functions. Each simulation can produce a detailed log that lists all transactions as a function of time. SNAP calculates a set of average performance measures at the end of each set of modeling runs. These measures concentrate on the occurrence and outcomes of engagements. They also include an overall probability of adversary success in the specified scenario. SNAP can provide certain statistics related to the performance of elements of the facility model, if desired.

(6) Computational requirements--SNAP is written in FORTRAN. Its central memory requirements vary with the complexity of the scenario modeled, ranging upward from about 33,000 words. Execution times, too, are highly variable, ranging from 10 to 100 seconds of CDC 6600 CPU time for sets of 100-repetition scenario simulations. Available memory size may in some cases place a limit on the complexity of the facility and activity descriptions that can be accommodated. Sandia reports that an internal virtual memory option is available in SNAP to circumvent this problem (at the expense of increased execution time).

(7) Documentation and Applications--SNAP is well documented. Recent Sandia SNAP publications include an overview, a general description that could serve quite well as a manual for the general user, and a user's guide for the more technically oriented. Another publication describes applications of SNAP (and other Sandia models) to an hypothetical nuclear fuel cycle facility and to an hypothetical reactor complex. The Navy Surface Weapon Center has applied SNAP to ship designs. There is considerable enthusiasm at Sandia for future use.

(8) Assessment--SNAP's flexibility, which is its greatest strength, may also be a potential weakness. The user's guide indicates that SNAP is intended for use by security experts who have little desire to become computer modelers. We fear that people with a deep intuitive understanding of security systems may tend to take certain things for granted that SNAP does not. This could produce models that are thought to be sufficiently detailed, but that lack something important. The experienced modeler, who is more acutely aware that machines take nothing for granted and is used to their discipline, may therefore produce better SNAP models than someone with more extensive knowledge of the subject area. (This is not necessarily bad, but indicates that experienced modelers should always be included alongside security system experts on SNAP assessment teams.)

These reservations aside, we feel that SNAP can be a powerful tool for security system evaluation (within the limits of a scenario-oriented model). Effective use of this tool may require considerable skill. SNAP's relative freedom from limits on the modeler's ingenuity is unique among current systems.

BIBLIOGRAPHY

Chapman, L.D., and Engi, D., Safeguards Network Analysis Procedure (SNAP)--Overview, NUREG/CR-0960, SAND79-0438, Sandia Laboratories, August 1979.

Grant III, F.H., Miner, R.J., Chapman, L.D., and Engi, D., Safeguards Network Analysis Procedure (SNAP), NUREG/CR-0725, SAND79-0617, Sandia Laboratories, March 1979.

Grant III, F.H., Engi, D., and Chapman, L.D., User's Guide for SNAP, NUREG/CR-1245, SAND80-0315, Sandia National Laboratories, January 1981. (Except for some differences in authorship, and the inclusion of appendices describing advanced SNAP capabilities and SNAP error messages, this is nearly identical to the November 1978 Pritsker User's Guide.)

Grant III, F.H., Miner, R.J., and Engi, D., A Network Modeling and Analysis Technique for the Evaluation of Nuclear Safeguards Effectiveness, SAND78-0671, Sandia Laboratories, December 1978.

Miner, R.J., and Grant III, F.H., User's Guide for SNAP, Pritsker & Associates, Inc., November 1978.

e. Forcible Entry Safeguards Effectiveness Model (FESEM) (Sandia National Laboratories)--FESEM is one of the oldest of Sandia's physical protection models. It treats user specified attacks on a facility by a single group of adversaries. The facility, the guard force, and the attackers are described at a consistent, moderate level of detail. Except for new provisions for input and output at a time sharing terminal, FESEM is unchanged since the last RDA assessment, as is essentially, the discussion that follows.

(1) Situations modeled--Each user specification of a path allows FESEM to examine up to four scenarios: sabotage or theft can be the objective, and for either objective the attack can involve external attackers alone or outsiders assisted by internal allies. In any of the scenarios the adversary group proceeds to its target at a rate determined by the characteristics of the parts of the facility it encounters and by its own level of capability. If an alarm is activated at a barrier along the way, the onsite guard force responds. (If the alarm is sufficiently serious, off-site security personnel also respond.) After delays for response, assessment, possible communication with off-site security forces, and arrival of a sufficient number of guards, the secuirty system personnel on the scene generally initiate an engagement by ambushing the adversaries. The encounter results in either a defeat or a delay for the attackers. If they are only delayed, the adversaries resume their activities. They proceed as before until the target is reached, and they then spend enough time in its vicinity to accomplish their objective. If the goal is theft, they attempt to escape with the stolen material along the same path as was used for entry, but with no delays at barriers. If

ranges rather than singles values have been supplied for some parameters (as is allowed in the input process), the overall path is traced many times to test the system over the full range of parameters.

(2) Adversary description--A single, undifferentiated group of adversaries attempts the hostile action. The group's level of performance in several of the tasks in the scenario reflects the quality of its weapons (small arms or automatic weapons), its penetration equipment (including high explosives or not), and its transportation (by foot, ground vehicle or aircraft). The outcome of engagements is influenced by an estimate of the group's ability and dedication. The user can specify all of these attributes, or, alternatively, specify ranges for them so that effectiveness of the security system against a broad cross section of potential adversaries can be examined. Insider allies of the adversaries do not participate directly in any of the group's activities; their sole contribution is to degrade the alarm and communication systems.

(3) Guard force description--In contrast with its restriction to a single group of active adversaries, FESEM allows for the presence of several groups of guards on site--and for several groups of off-site guards as well. All guards have a common level of dedication and ability. Each guard group is characterized by its size, its response time distribution, and its communication probability. The response time and communication probability do not depend on where along the adversary's path they occur, but in general they differ between insider-assistance scenarios and all outsider attacks. For some groups of guards, an alert delay precedes the response delay.

(4) Facility description--A description of the barriers encountered along the adversary path is the essence of FESEM's site specification. The numerical order of the barriers specifies the adversary path. Associated with each barrier is its delay time distribution, which reflects the time required to penetrate the barrier (a function of the attacker's barrier penetration capabilities), and the time to reach the next barrier (which depends on the distance to the next barrier and on adversary transport capabilities.) If explosives are used at a barrier in a scenario an additional delay time distribution specifies the time required to emplace them. Alarms may be associated with any of the barriers. The alarms have one probability of activation for an external attack and another (generally lower) probability of activation for an internally assisted attack. (This degradation of alarm performance is FESEM's treatment of insider assistance.) Area sensor and alarm systems (such as intrusion detectors and closed-circuit-TV monitors) that are not associated with specific barriers can be included in FESEM facility descriptions by placing them at zero-delay dummy barriers. Certain alarms activate the emplacement of additional barriers (after a suitable delay). After an assessment delay chosen from a specified distribution, all activated alarms produce a response by the guard force. "Serious" alarms--signifying high explosive detection, adversary detection at the final barrier before the target, or initiation of a battle--produce response from every group of guards that are made aware of them by successful communication.

(5) Combat engagements--When guards arrive to engage the attackers, FESEM's elaborate attrition-rate-type conflict model allows for some complexity of tactics.

Unless sabotage is imminent, or escape after theft is underway, there may at the outset be a delay to await the arrival of a critical number of guards. Moreover, the time-varying coefficients in the differential equations of the model will reflect an ambush of the attackers by the security force. (If desired, specification of an alternative set of coefficients can model a pre-planned ambush of the guards by the adversaries.) Combatants incur and inflict casualties at rates that reflect their relative advantage and their dedication and training. These rates evolve in reasonable ways during the course of a battle. The engagement will terminate when a side has exceeded its "quit fraction", a casualty fraction which is a characteristic of each force. If at the end of the engagement at least one adversary is left, he continues toward his goal.

(6) Mathematical treatment and performance measures --FESEM uses Monte Carlo techniques to predict the average performance of the security system against a range of threats. If the range is sufficiently comprehensive, assessment is global with respect to the specified path. Events that may require randomly varying times--such as barrier penetration, alarm activation, travel from barrier to barrier, etc.--are also treated in a probabilistic fashion. Combat engagements, however, are not: once the equations and initial conditions are specified, the outcome is determined. FESEM's output, which is rather voluminous and somewhat difficult to read, includes a wealth of detail about the simulation. The user can extract several useful measures of system performance from it. Most of them are probabilities of attacker success, broken down to reveal the effect of various variables on those probabilities. Some indicate the effectiveness of each barrier, each

sensor system, and the guard force. Others indicate the duration of successful attacks.

(7) Computational requirements--As befits a moderately detailed scenario simulation, FESEM is only moderately demanding of computational resources. The current version requires 35,000 words of central memory. Sandia reports that 500 examinations of a single path that involved ten barriers required about five minutes of CDC 6600 time. If many more repetitions were required to examine a wider range of adversary capabilities in a more complex scenario, FESEM's needs might become burdensome.

(8) Documentation and application--A detailed description of FESEM is available in a published user's guide. The guide describes the model, information required for input, results available for output and several examples, along with appendices of data from the Sandia Physical Protection Handbooks (Ref. 7) for use in input preparation. The user's guide also provides a program listing. Since the last RDA survey, Sandia has released a new version of FESEM, which allows for interactive entry of input information and receipt of output at a time sharing terminal. FESEM is mature and has been extensively applied: a Sandia presentation mentions 21 facility studies, including 7 which are described as "detailed". Extensive discussion of these applications are, understandably, not available in the open literature.

(9) Assessment--The attempt in FESEM to treat the physical protection problem in a relatively comprehensive manner is more successful than one would have expected an early modeling effort to be. However, with the availability of simpler, easier to use models that reflect many of the same scenario features included in FESEM (and of some newer, more elaborate models that include scenario complexity beyond FESEM's range) it seems unlikely that use of this code will grow.

BIBLIOGRAPHY

Sasser, D.W. and Barker, B.E., User's Guide to Interactive FESEM, NUREG/CR-0976, SAND79-1595, Sandia National Laboratories, January 1980.

Pavlakos, C.J., Chapman, L.D., Grant, F.H., and Kimpel, C.H., Application of Sandia Physical Protection Methods, NUREG/CR-1893, Sandia National Laboratories, March 1981.

Chapman, L.D., Kinemond, G.A., Sasser, D.W., User's Guide for Evaluating Alternative Fixed-Site Physical Protection Systems Using "FESEM", SAND77-1367, Sandia Laboratories, November 1977.

Bennett, H.A., A Security Force-Adversary Engagement Simulation, SAND75-0658, Sandia Laboratories, April 1976.

Bennett, H.A., Boozer, D.D., Chapman, L.D., Daniel, S.L., Engi, D., Hulme, B.L., and Varnado, G.B., Safeguards System Effectiveness Modeling, SAND76-0428, Sandia Laboratories, September 1976.

f. NEWMOD (Technical Support Organization, Brookhaven National Laboratories)--NEWMOD is a simple, deterministic scenario simulation program, which TSO applied during a number of physical protection system assessments at Department of Energy facilities a few years ago. It is an updated version of an earlier BNL model called PROTMOD. NEWMOD has not changed since the last RDA assessment. The description which follows is taken from that report.

(1) Situations modeled--Essentially, NEWMOD plays out a race between one or more guards and a single group of adversaries. The "finish line" is located at a protected target within the facility. The adversaries may be delayed by barriers they encounter along their path. If the attacker's path takes them past an alarm, the alarm is activated. When that happens, each guard moves toward the target (after a delay for communication and preparation). If one or more guards arrive at the target before the adversaries begin their activities there, a battle ensues. (NEWMOD does not model interruption during the attacker's stay at the target.) The outcome of a battle, which is either defeat or a delay of varying length for the adversaries, is determined by the ratio of guards to attackers at the scene.

If the adversaries have reached the target--either unopposed or after defeating the guard force--and carried out their activities there, they may attempt to escape. The escape phase is a second race, similar to the entry phase, involving the same set of competitors but different paths, barriers, and performance parameters. If sufficient guards to defeat the adversaries as they leave the target have not arrived during the intruder's stay there, all participants will attempt to proceed along straight lines toward a specified interception point on the outermost barrier. If guards arrive there in time, another battle--"modeled" as before--may be fought.

(2) Adversary and guard force descriptions--The adversary group is characterized by its size, its initial position, its mode of transportation, and its barrier penetration capabilities. For each guard, NEWMOD's description includes the length of his path to the target, his speed of travel along that path, and his delay between the time an alarm is sounded and the time he actually starts for the target.

(3) Facility description--Up to ten barriers may be modeled along the adversaries' path. Same barriers, like vault doors which are normally open, may only become activated after an alarm sounds. Behind each barrier but the last (assumed to surround the target directly) is an area, which is to be crossed using the same mode of transportation that was employed to traverse the barrier. A perfect alarm, which never fails,and which functions even if the barrier on which the alarm is located has not been activated, may be placed on, in, or behind each of the modeled obstacles. Barrier penetration times are taken from a table indexed according to barrier type, penetration equipment type, and mode of transportation. The quickest available method of penetration is always chosen for the adversaries.

(4) Combat engagements--Combat engagements are handled in a very simple way. If attackers outnumber guards by more than two to one when an engagement might otherwise commence, there is no engagement then. If sufficient guards to outnumber the adversaries arrive at any time during an engagement, the security system wins. Under other circumstances, the battle is generally modeled as a delay for the attackers, the duration of which is linearly related to the ratio of adversaries to guards on the scene. The delay can, if desired, be preset to zero to produce a more conservative assessment. Combat in NEWMOD simulations does not result in casualties which eliminate participants from subsequent engagements.

(5) Evaluation results presentation--NEWMOD output consists of a log of the simulation and a graph of the number of guards who have arrived at the target vs. simulated time. The program repeats its calculations, progressively disabling a list of specified alarms, so as to explore the implications of failure or absence of those warning systems.

(6) Computational requirements and documentation--NEWMOD is written in standard FORTRAN, and (as might be expected) its computational requirements are modest. On a BNL CDC 6600 computer system, it requires about 25,000 words of storage and executes in a few seconds. It can be used (and often is) from remote terminals. A description, instructions for use, suggested values for the barrier penetration data base, and a set of input work sheets are found in the user's manual.

(7) Assessment--NEWMOD's simplicity and economy suggest it might be particularly useful in training, in quick on-the-spot assessments during plant visits, or in a restricted class of sensitivity studies. Confined to these tasks--which it should do well--it can be a useful tool.

BIBLIOGRAPHY

Bieber, Jr., A., NEWMOD: A Computer Model for Physical Protection Assessment at Nuclear Facilities, Program Description and User's Guide,BNL-26339, Brookhaven National Laboratory, October 1978.

Zimmerman, R.E., Models for the Evaluation of Safeguards Systems as Required by Regulation 10 CFR 73.55, Office of Nuclear Regulatory Research, USNRC, 9 June 1977.

g. Generic Physical Protection Logic Trees (GPPLT) (Sandia National Laboratories)--Sandia developed GPPLT to help an analyst to examine the progress of an adversary in a scenario of the analyst's choice, without assistance from a computer model. The analysis is qualitative: at its conclusion, the security system is determined to be either likely or unlikely to defeat the postulated attack. The GPPLT analyst uses judgement rather than simulation in deciding the many performance questions (e.g., Will the adversary defeat this sensor?) that constitute the primary events of the logic trees.

(1) Situation and adversary activities examined--GPPLT can be used to examine theft or sabotage scenarios, attempted by insiders or outsiders. The adversaries can use force, stealth, deceit, or combinations of these tactics. GPPLT can be used to examine a very wide range of possible scenarios, because the generic logic trees are both flexible and inclusive. The generic logic trees examine adversary attempts to carry out five types of activity: penetrate a protected boundary, cross a protected area, enter a building, acquire special nuclear material (SNM), or release SNM. GPPLT provides a separate tree for each activity performed by force, by stealth, or by deceit. (One tree--enter a building by deceit--is omitted because it is redundant with penetrate a boundary by deceit. Another one--release SNM by deceit--is omitted because GPPLT's authors consider it impossible.)

(2) Approach--Naturally, each generic logic tree has primary events related to accomplishment of the activity. Stealth trees also have primary events related to avoiding detection (possibly by neutralizing a detecting guard). Force logic trees have primary events related to overcoming opposition to the adversaries' activities. At the outset of the

analysis, the user chooses appropriate generic logic trees, and ‿hen edits them to remove any inapplicable elements. Next he qualitatively analyzes the remaining primary events. Finally, he propagates the results of that analysis through the logic trees mechanically to determine if the end event is accomplished. The GPPLT user's manual suggests that the analyst should conduct the analysis for all logically permissable combinations of tactics, and for all significant site conditions. The manual suggests that use of force logic trees for all activities provides the most stringent examination of the security system's delay functions, and that use of stealth logic trees for all activities provides the most stringent examination of the security system's detection functions. GPPLT does not treat response force activities explicitly.

(3) Documentation and Applications--Sandia describes GPPLT well in the equivalent of a computer program user's manual. (The draft version available to us omitted the complete generic logic trees, which were to be included in an appendix.) Sandia has applied GPPLT in examining several DoE material handling facilities, and has used GPPLT during exercises in its physical protection workshops.

(4) Assessment--GPPLT identifies the contributions of individual security system elements to prevention of adversary activities in a particularly straightforward way. It is particularly easy for the GPPLT analyst to distinguish adversary activities that must be opposed from those that can be safely ignored. Unfortunately, GPPLT may require the analyst to make binary adequate-or-inadequate judgements of security system element performance at a stage of the anlysis when such judgements are premature. In many applications an overall adequate-or-inadequate judgement may be less useful than the ranking of alternatives that other techniques provide.

BIBLIOGRAPHY

Paulus, W.K., Generic Physical Protection Logic Trees, SAND79-1382, Sandia National Laboratories, February 1981.

h. SOURCE (Sandia National Laboratories, Livermore)--Sandia/Livermore developed SOURCE as part of a program concerned with physical protection of nuclear materials in transit. SOURCE is designed to help the analyst examine convoy personnel survival and alarm communication during the initial stage of an adversary ambush. It allows the analyst to vary factors such as road convoy configuration, defensive driving tactics, and vehicle vulnerability. SOURCE follows the course of the ambush until the convoy has escaped or regrouped to defend itself (or until all convoy personnel have been incapacitated). SOURCE models different elements of the simulated ambush at different levels of detail, concentrating its attention of factors which are within the control of the protection system designer. SOURCE is a companion to another Sandia/Livermore code, called SABRES, which examines the combat engagement which ensues when the halted convoy returns fire to defend itself.

(1) Situation modeled--In a SOURCE simulation, a convoy of vehicles (nuclear material transporters and their escorts) is ambushed by one or more hidden adversaries as it travels along a straight stretch of road. Each adversary fires on convoy members within range, attempting to incapacitate the guards, disable the vehicles, and prevent communication of an alarm to other convoy elements. The ambushers may use a roadblock to stop the lead vehicle. They continue to fire until no convoy member is in range, the guards are all neutralized, or the convoy members have rearranged themselves for defense and are about to return fire. Guards on a vehicle only become aware of the attack when they are attacked, see another vehicle attacked, or receive an alarm transmitted by another vehicle (which has been attacked). Members of the convoy that are aware

of the attack take defensive actions such as accelerating to get out of range of the ambushers. They also try to send an alarm to other convoy vehicles (and possibly to a home base). If an alerted vehicle is not under fire, it may stop, or attempt to rendezvous with other convoy members for defense, or attempt to escape. Vehicles cannot leave the road to seek cover.

(2) Adversary description--SOURCE models characteristics of the adversaries at a relatively low level of detail. All adversaries are located a fixed distance from the road, at (static) positions specified by the analyst. The unclassified version of SOURCE distributed by Sandia provides parameters for attackers armed with hunting rifles (30-30 or 3-06), though the code can accommodate other armaments. The adversaries' strategy is simple. Once a designated vehicle has come to within a specified distance of a "lead" adversary (possibly at a roadblock), that adversary fires, beginning the ambush. Thereafter, as soon as they have paused to aim, all attackers fire at the closest vehicle within their fields of fire as long as there is such a vehicle and their weapons are still loaded. The adversaries aim to incapacitate key defenders (drivers, then co-drivers, then guards), to disable the vehicles, or to interfere with communication. Bullets land in Gaussian distributions about the aimpoints with standard deviations determined by weapon type, and with ability to do damage determined by weapon type, point of impact on the target, and range.

(3) Convoy description--SOURCE describes its nuclear material transport trucks and their escort vans in terms of their ability to accelerate and decelerate (the escort vans can do both more quickly), and of their vulnerabilities as targets. For the latter purpose, SOURCE represents each vehicle by a front and side profile, consisting of 10cm squares--of variable vulnerability--arranged to represent

components of the vehicles and their occupants. Standard profiles, which the analyst may modify, are built into the SOURCE code. Each kind of vulnerability corresponds to a set of consequences which would follow upon a hit in a particular area. Such consequences can include injury or death (to a guard), various degrees of damage (to a vehicle), or loss of communication.

Any combination of up to 10 vehicles, either escorts (each carrying up to 6 guards) or transports (each carrying up to 3 guards) can travel in a SOURCE convoy. Either type of vehicle may be armored. Different members of the convoy can have different strategies (stopping, speeding away, or traveling to a predetermined rendezvous position) for use when they are aware of an attack but not under fire. The analyst can also specify whether the convoy's drivers can be replaced if they become incapacitated and healthy replacements are available. Prior to the ambush, the convoy travels at a specified average speed. The analyst can specify initial positions of the vehicles either at precise points on the road or in variable length regions (where placement is random).

If a convoy member comes under fire (or sees another vehicle sustain visible damage), he tries to send an alarm to the other vehicles and to any home base. This takes time, which varies with the kind of communication equipment available. Only if the operator and his equipment are still capable at the end of a suitable delay is the alarm transmitted to convoy members who are able to receive it.

(4) Mathematical treatment and performance measures --SOURCE is a fixed-time-stepped Monte Carlo simulation. At the conclusion of each simulation within a Monte Carlo

set, SOURCE provides information on the position of each vehicle, and on the status of each vehicle and guard. It also prints a log of attempts to transmit alarms during that simulation. At the conclusion of each set of simulations, SOURCE produces a series of histograms. These include one that show where combat-effective guards were likely to be found at the end of SOURCE's simulation (as a function of the number of combat effective guards remaining); another shows the most likely final positions of the transporters; and a third records simulations in which no alarms were sent, divided according to whether the transporter escaped or not. Finally, SOURCE provides the total number of times the transporter was able to escape without firing a shot.

Post-processor programs can use SOURCE data files to plot other interesting quantities. These include average numbers of combat-effective guards, operational vehicles, operational communication systems, and transmitted alarms, as functions of time.

(5) Computational requirements--The developmental version of SOURCE is written in FORTRAN and requires about 33,000 words of storage. Sandia mentions a single simulation of 200 seconds of real time that required one second of CDC 6600 CPU time. The computer time would vary with the scenario, but in any event, SOURCE's computational requirements do not seem impractically large.

(6) Documentation and applications--SOURCE is adequately documented. Sandia has published both an overview of the model (including a description of a hypothetical application) and a detailed user's guide. We are not aware of published descriptions of applications of SOURCE.

(7) Assessment--SOURCE has interesting capabilities which are quite unusual (among the models examined in this study), particularly its ability to examine vehicle survivability in a credible way within the context of a security system problem. Only Jaycor's SAS model has similar capabilities. SOURCE is older and less elaborate than SAS. (Those are not necessarily disadvantages.) Side-by-side applications of the two methods (to a problem within the range of both) would be interesting.

BIBLIOGRAPHY

Stimmell, K.G., SOURCE: A Convoy Ambush Simulation Code, NUREG/CR-0641, SAND78-8034, Sandia National Laboratories, January 1979.

Stimmel, K.G., Mitchell, D.L., and Cupps, F.J., SOURCE User's Guide, NUREG/CR-0919, SAND79-8004, Sandia National Laboratories, December 1979.

i. SABRES (Sandia National Laboratories, Livermore)--SABRES is a computer code which simulates a combat engagement between two small groups of individuals equipped with small arms. Sandia/Livermore developed SABRES as part of a program concerned with physical protection of nuclear materials in transit. The code examines alternative strategies, tactics, and systems of equipment for use by a group of guards who must defend a road convoy which has been brought to a halt by an ambush. (The ambush phase is modeled by another Sandia/Livermore code called SOURCE.)

Compared to SABRES I, which was briefly described in the previous RDA review, SABRES II is said to incorporate several significant improvements. SABRES now treats effects of terrain and vegetation in some detail. A more elaborate representation of the bodies of combatants allows a more realistic estimation of casualties. SABRES combatants can now move during the course of the engagement, and SABRES' treatment of target detection is now considerably more elaborate. SABRES scope has been extended to include adversary penetration activities at the transporter. Finally, SABRES II has a system for scheduling the activities of individual participants through a series of plans. Sandia adapted parts of TRW's Small Independent Action Forces (SIAF) model to provide many of SABRES II's new features.

(1) Situations modeled--Each SABRES combatant begins the simulation at a position specified by the analyst. (A SOURCE simulation may have suggested who should be where.) The combatant follows one of several sets of plans provided by the analyst. He may switch from one set to another as circumstances change in the course of the simulation. An adversary will generally try to move to the transporter that contains nuclear material he wants to steal. Along the way,

the adversary may fire at any defenders he encounters. When he reaches the transporter, he will try to penetrate it to remove the nuclear material. If successful, he will try to escape. Defenders, each following his own plan, try to prevent all this by moving to defensive positions and firing at the adversaries.

A participant may withdraw if the density of enemy fire in his immediate vicinity is too high for too long. He may also withdraw if he has insufficient ammunition to continue. An entire group (guards or adversaries) may withdraw if it attains its objective, if too many of its members sustain casualties, or if the battle lasts too long. Participants who withdraw are not pursued.

(2) Combatant features and activities--Each participant's description includes his physical size and reflectivity, his skill level, his weapon (one of 21 types of small arms), and a measure of his susceptibility to suppression by incoming fire. SABRES also maintains a long list of current status data for each combatant, which together determine what he is doing, where he is, where he is going, and whether and how well he can perform the tasks available to him. Tasks which can be included in a combatant's plans include firing, moving, and waiting. Attackers can also work to penetrate the nuclear material transporter. The participant begins each task (when its turn comes in his plan) only if applicable preconditions are satisfied. He may discontinue the task when certain termination conditions occur, even if he has not completed it.

Firing tasks generally begin with a period of observation time, during which a combatant may detect opponents and choose one of them as the target. SABRES models the detection process as elaborately as any of the simulations we have examined. It considers conditions in the opponent's vicinity; conditions in the path between the opponent and the viewer (including terrain and weather conditions) that affect transmission of the opponent's image; and conditions in the vicinity of the combatant (including his current status) that affect his ability to recognize the opponent's image as a potential target. Among detected opponents, the firing combatant chooses one who is relatively close, preferring targets he has recently fired upon before and targets who are firing at him. The shooter then aims, fires, re-aims, fires, etc., until it is time for another period of observation (or some other task). For each burst of fire, SABRES makes a random draw (based on the firer's weapon, his posture, his distance from the target, his level of skill and his physical and mental state) to determine whether a round hit home. If one did, SABRES determines the target's resulting level of incapacitation, based on the firer's weapon, the range between firer and target, and the body part on his target the firer hit. SABRES records near misses, and may use them to modify the target participant's activities to reflect suppression.

Movement tasks carry a participant toward a location specified in his current plan. If the distance to the objective is short (or no cover or concealment is available), the participant goes directly to his destination. For longer distances, he travels via a path which takes advantage of any cover and concealment available to him enroute. The combatant travels over the same detailed map of terrain and vegetation that SABRES uses in determining lines of sight and visibility in the detection process. His rate of progress is determined by the slope, texture, and vegetation cover of the terrain; by his posture and level of skill; by the local ambient light level; and by current and recent incoming fire. A movement task concludes when the participant reaches his objective. If this requires more than one time step, he may be distracted by changed circumstances before he completes his journey.

Attacker transporter penetration tasks proceed at a rate determined by the time it would take an optimal number of undisturbed adversaries to enter the transporter and remove the nuclear material. SABRES "credits" the adversaries with a fraction of the penetration task for each adversary that spends a time step in this activity. Adversaries accomplish a smaller fraction of the task if their performance is degraded by injuries or by reaction to incoming fire.

(3) Mathematical treatment and performance measures--Sandia/Livermore developed two distinct versions of SABRES II. In one, the analyst interacts with the program, making all the strategic and tactical decisions which arise as the simulation procedes. In the other, which is not run interactively, the analyst provides a set of plans at the outset. The computer then repeats the simulation many times in Monte Carlo fashion to derive statistical measures of the course of the battle.

Both versions of SABRES II can produce a detailed log of the engagement's status at each time step. The interactive version can also produce a summary of the status of the participants at specified simulated intervals. The Monte Carlo version can provide a summary trace organized around important events which take place during each simulation. A postprocessor in the Monte Carlo version calculates such statistics as the fraction of "wins" by each side; the average battle time for each outcome; the fraction of each kind of participant that survived, disengaged, or was killed in the course of the engagement; the average ammunition expenditure of surviving participants, the survival odds of each participant for each outcome; and the average barrier penetration time.

(4) Computational requirements--SABRES II is written in FORTRAN, and runs on Sandia/Livermore's CDC 6600. The

interactive version requires a graphic display terminal and associated software(the DISSPLA system is used at Sandia); it is overlaid, and uses 33,000 words of storage. Sandia mentions CPU time expenditures of a few seconds to simulate battle periods of a few tens of seconds.

The Monte Carlo version is (as might be expected for such a detailed simulation) rather demanding of computational resources. Sandia mentions a trial application involving 100 repetitions of an engagement between 4 attackers and 4 defenders which consumed 1.25 hours of central processor time. This version of the program requires 80,000 words of storage.

(5) Documentation and applications--SABRES II is adequately documented. An overview document describes the method (in both Monte Carlo and interactive versions) and presents a clear illustrative application; an appendix contains detailed flow charts. Sandia has also published a user's manual, which contains both a detailed description and a listing of the code. We are not aware of published applications of SABRES.

(6) Assessment--SABRES II is an impressive model, especially in its treatment of the physical (as opposed to psychological) factors which come into play during this type of engagement. A user who wanted to explore such factors in some detail could find it quite useful. He would, however, have to weigh the relatively high cost in computer time of such an exploration against its anticipated benefits.

BIBLIOGRAPHY

DeLaquil III, P., SABRES II: An Individual Resolution Small Arms Combat Simulation Model, NUREG/CR-0929, SAND79-8249, Sandia National Laboratories, Livermore, March 1980.

DeLaquil III, P., SABRES II: Code Description and Users Manual, NUREG/CR-1178, SAND79-8268, Sandia National Laboratories, Livermore, March 1980.

DeLaquil III, P., Simulating Barrier Penetration During Combat, NUREG/CR-0364, SAND79-8235, Sandia National Laboratories, Livermore, April 1980.

Keeton, S.C., SABRES I: Conflict Simulation Model for Surface Transport Systems, NUREG/CR-0445, SAND78-8249, Sandia Laboratories, Livermore, September 1978.

j. Stand-off Attack Simulation (SAS) (Jaycor)--Jaycor developed SAS (for DNA) as a simulation tool for use in examining the security of nuclear weapon transports. SAS differs from most of the other combat engagement models examined in this review in that it places comparable emphasis on representing combatants and the assets over which they contend, so that it can examine both conventional security considerations and protected asset survivability in a single analysis. (Only Sandia/Livermore's SOURCE is similar in this regard).

(1) Situation, participant and target description--SAS considers the effects of exchanges of fire between adversaries and defenders. In the current version of SAS the two groups are confined to a pair of fixed parallel planes (one for each group). Members of each group (and their vehicles) can move within the plane during the course of the engagement. SAS participants can move; take or leave cover; select a strategy, a weapon or a firing rate; or aim or fire a weapon. The analyst specifies a fixed schedule of these activities at the outset of the simulation. A participant's event schedule cannot change to reflect changes in the status of another participant (but he has a low probability of choosing targets that have a low probability of existence at the time he is scheduled to fire). SAS describes a participant in terms of his position (possibly an uncertain position within a specified area), his weapon type (one of seven effective stand-off weapons), his ammunition supply, his "response time" (the time, relative to the beginning of the simulation, at which he begins to fire), and his "strategy" (a prioritized list of aim points). SAS treats material objects that it models--such as vulnerable parts of vehicles or nuclear weapons carried inside vehicles--as participants who cannot fire. Uniquely among the models we examined, SAS simulates blast damage to nearby targets when

potentially explosive targets (e.g., fuel tanks, HE components of nuclear weapons) are hit, or when grenades or antitank rocket rounds explode.

(2) Mathematical approach and presentation of results--At the outset of the simulation (and at each time step when relations of potential firers and targets have changed) SAS calculates a set a set of probabilities that each possible firer, aiming at each possible aimpoint, hits each possible target. To do so, SAS carries out a Monte Carlo simulation of the results of the firing process in which a number of simulated "rounds" land in the vicinity of the aim points. The simulated points of impact are randomly distributed according to empirically parameterized weapons effectiveness functions. SAS substitutes the derived Monte Carlo probabilities into straightforward analytic expressions, to calculate probabilities of continued existence for each target at each time step of the simulation. (The probabilities reflect the possibility of both direct and collateral destruction.) If desired, the SAS analyst can combine probabilities of existence for related targets to calculate expected values for the number of remaining targets in the group as a function of time.

(3) Documentation and applications--Jaycor describes SAS in a draft user's guide that includes a description of the method, instructions for use of the SAS computer codes, an example application (to a nuclear weapons transport convoy problem), and an extensively annotated listing of the program. SAS is a new model, and, to our knowledge, Jaycor has not yet published descriptions of applications to the theater nuclear force security/survivability problems for which it was developed.

(4) Assessment--SAS's capability to examine vehicle and cargo survivability (including the effects of "collateral damage") is quite appealing. Among the models examined for this survey, only Sandia/Livermore's SOURCE has anything comparable. SAS has not yet had much opportunity to demonstrate its utility in applications. Such a demonstration (particularly if it were to include a side-by-side application of SOURCE for comparison) would be quite interesting.

BIBLIOGRAPHY

Clark, C.M., Humphrey, J.T., Kennedy, L.W., and Reynolds, S.G., User's Guide for the SAS (Standoff Attack Simulation) Computer Model, Jaycor 2182-05, Jaycor, March 1981.

k. Securıty Analytic Methodology (SAM) (Los Alamos National Laboratory for Aır Force Weapons Laboratory)--LANL composed the SAM computer program to help the Air Force examine the security of nuclear weapon systems, from storage sites to launch sites. SAM uses Sandıa's EASI and BATLE codes (discussed in Section III.1.a (3) of this survey) to calculate probabilities of adversary success. It also considers probabilities of attempt (derived from Air Force route threat studies) and expected monetary costs should the postulated attack take place.

To estimate the total probability of an attack on a set of protected weapons SAM divides the route the weapons would travel from storage site to launch site into a series of segments. Within each segment the threat to the weapons is approximately constant (as deduced from estimates of likely frequency of attack and level of vulnerability of the weapon systems). SAM adds the probabilities of attack for the segments, taking their duratıon ınto account.

The SAM analyst then calculates probability of adversary success using EASI and BATLE. It ıs the analyst's responsıbılity to provide a set of "independent" scenarıos that adequately test the security system. (This may be easier for road convoys than it ıs for the complex facilitıes usually examined by physical security evaluation methods.) We refer the reader to the previously cited discussion of EASI and BATLE for details of the calculations. SAM adds probabilities of adversary success for a set of scenarios to get a total probabılity of adversary success. SAM can use EASI's provision for automated analysis of a range of threats or security system options if the analyst desires.

SAM calculates expected total costs of possible attacks on the protected weapons by combining analyst estimates of spe:ific component costs. These include vehicle overhead and replacement costs, personnel overhead and replacement costs, and costs for possible attack consequences (for both successful and unsuccessful attacks). SAM combines the costs using probability of adversary success (and possibly probability of attack) as weights in an average.

SAM is described in an AFWL report on Minuteman III operations (which includes a complete listing of the code). At present there is no user's manual, but the code provides automated assistance in entering the required data. In addition to the Minuteman III study, LANL and AFWL have applied SAM in an examination of the security of ground-launched cruise missiles.

SAM has been useful to its developers, but we doubt that it will find wide application. The computational assistance it provides adds little to what are basically subjective parts of the analysis, and may simply obscure their subjectivity.

BIBLIOGRAPHY

Technique for Security Analysis Applied to the Minuteman III Logistic Operation, Air Force Weapons Laboratory, Unpublished.

Ground Launched Cruise Missile (GLCM) Security Analysis, Air Force Weapons Laboratory, Unpublished.

1. Insider Safeguards Effectiveness Model (ISEM) (Sandia National Laboratories)--This older Sandia model provides an estimate of the effectiveness of a security system against one or more persons with authorized access to the protected facility. It consists of submodels of: the facility (consisting of areas, portals and barriers), the alarm system sensors (protecting areas or specific objects), the guard system's response to alarms, and the engagements which may occur between guards and the ISEM's single active insider. ISEM is unchanged since the last RDA survey, as, in essence, is the description which follows.

(1) Situations modeled--Scenarios for which ISEM is an appropriate model unfold as follows. The active insider attempts an unauthorized activity by moving from area to area through portals and/or barriers. In any area, or at any portal or barrier, he may encounter an alarm sensor which has some probability of activating the alarm. He (or an otherwise inactive insider ally) may be able to prevent the alarm from alerting the security force. Should the guards become alerted, however, they will execute a preplanned response (which may include the emplacement of additional barriers). If responding guards meet the adversary insider while he is in a portal, the adversary is trapped and loses. If the guards meet the adversary elsewhere, an engagement ensues which either leads to the insider's defeat or delays his progress. In modeling theft, ISEM assumes that the malevolent intruder leaves the same way as he arrives. The scenario procedes until the adversary either achieves his objective or is defeated.

(2) Adversary description--The principal actor in ISEM is a single disloyal employee who attempts sabotage

of the installation or theft of SNM. He may be carrying explosives or SNM, and he has authorized access to up to four areas of the facility. His level of skill in an engagement can be either low, medium, or high; he can be armed with a pistol, a rifle, or an automatic weapon. In addition to the principal adversary, there may be other employees allied with him (some of whom may be guards) whose sole adversary function is to degrade the alarm system. This is done covertly: the insider's allies cannot participate in engagements. Each insider has his own list of authorized access privileges, which identifies the element of the alarm system with which he can tamper. His probability of success decreases when others are or might be watching.

(3) Guard force description--Any number of guards may respond when an alarm has been recognized by the security system. Each of the alarms produces a predetermined response pattern. (Some care is required to make these responses realistic.) In addition, the security force as a whole will respond to a special alarm that can be issued by a guard who has arrived at a battle. Like the adversaries, the guards can have handguns, rifles or automatic weapons and can display low, medium, or high levels of competence in an engagement.

(4) Facility description--The facility submodel treats the areas, portals, and barriers which make up the installation as entities which introduce distributions of delay times. Each may contain alarm system sensors. In addition, areas may contain people, who somewhat degrade the ability of insiders to tamper successfully with alarm system elements in their vicinity. Most alarm sensors are characterized by a single probability of alarm when there

is no tampering. High explosive and SNM detectors are modeled in greater detail; their level of performance depends upon the amount, type, and location (on the adversary) of material to which they are sensitive, and their performance is impaired by shielding of that material. Some alarms can be neutralized by insiders with appropriate access.

(5) Combat engagements--Should an alarm be activated, alert the guard force, and produce a guard response which results in a confrontation with the active insider, ISEM examines the resulting engagement to determine the victor (and the delay time for the adversary should he be the victor). ISEM uses an attrition model called BATLE (described elsewhere in this report) to accomplish this. Briefly, the engagement moves from state to state (a state being characterized by the number of combatants on each side) at rates determined by the relative sizes and capabilities of the contending forces. (ISEM engagements involve states with only one adversary combatant and an arbitrary number of guards). The engagement terminates when the adversary is neutralized or no guards survive. The engagement time is the sum of the times spent in each of the states through which the engagement passes.

(6) Mathematical approach and performance measures --Because several things modeled in ISEM (such as delays, travel times, operation of alarms, outcome of engagements) are treated probabilistically, each user-specified scenario is repeated many times (in Monte Carlo fashion) to produce statistical estimates of various security system performance measures. The principal measure is the probability that the security system will defeat the postulated attack. Important supplementary figures of merit which may be calculated include the probability that at least one alarm

will alert the guard force, the probability that at least one engagement will occur, and the probability that each time an alarm alerts the security system at least one engagement will ensue.

(7) Computational requirements--The ISEM code is written in FORTRAN, using some of the features of the GASP IV simulation system. A 500 scan simulation of a scenario of modest complexity on the Sandia National Laboratories CDC 6600 required about 40 seconds of central processor time for execution. About 35,000 60-bit words of storage were used. This indicates that the code is moderately demanding of computational resources.

(8) Documentation and applications--ISEM is a mature model, and is described in some detail in several documents. These documents include a users guide with both a listing of the code and a very complete example involving a hypothetical facility. The guide also describes sample input and output, and lists the program. Key appendices to the guide describe distribution functions used in the Monte Carlo simulation and discuss the engagement submodel in some detail. Other Sandia documents describe applications of ISEM in studies of personnel control systems and guard tactics. We have not encountered published descriptions of applications to real facilities, though applications to seven facilities are mentioned in unpublished material provided by Sandia. Several of the submodels of ISEM require performance, parameters which are not readily available from the data base in the current version of the code. Thus, applications to actual facilities may require considerable input preparation effort, which, however produces a capability to examine many paths through the facility with little further preparation.

(9) Assessment--ISEM represented the state of the art for the insider problem when it was written in 1976, but the range of scenarios to which it is confined now seems narrow. More recent models can treat a wider range of insider threats more realistically (certain SNAP models) or examine the implications of insider privilege more exhaustively (MAIT). They are now preferred tools for analysis of the insider threat.

BIBLIOGRAPHY

Pavlakos, C.J., Chapman, L.D., Grant, F.H., and Kimpel, C.H., Application of Sandia Physical Protection Methods, NUREG/CR-1893, Sandia National Laboratories, March 1981.

Boozer, D.D., and Engi, D., Insider Safeguards Effectiveness Model (ISEM) User's Guide, SAND77-0043, Sandia Laboratories, November 1977.

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

Boozer, D.D., and Engi, D., Simulation of Personnel Control Systems With the Insider Safeguards Effectiveness Model (ISEM), SAND76-0682, Sandia Laboratories, April 1977.

Bennett, H.A., Boozer, D.D., Chapman, L.D., Daniel, S.L., Engi, D., Hulme, B.L., and Varnado, G.B., Safeguards System Effectiveness Modeling, SAND76-0428, Sandia Laboratories, September 1976.

IV. DISCUSSION OF EVALUATION METHODS

1. TABULAR COMPARISON OF THE METHODS

For the convenience of the reader, we have summarized some of the properties of the evaluation systems examined in this review in the series of tables that follows. In using these tables to compare the capabilities of different models, the reader should note that some of the entries reflect close judgements, and that others reflect RDA's interpretation of terms that are used differently by different members of the modeling community. The reader should refer to the discussions in the previous chapter for finer distinctions.

Table 1 indicates the designations used to identify the methods. Table 3 records the state of development and documentation of various techniques as of April 1981. Table 4 provides a rough indication of computational requirements.

Table 5 summarizes the range of coverage and capabilities of the evaluation aids. Table 6 and 7 provide more detail, respectively, about the adversary attributes and the adversary activities considered by each method. Table 8 compares the guard force descriptions. Table 9 examines representations of the facility and its security system hardware. Table 10 lists the security system activities each method considers.

Table 11 compares treatments of stochastic elements, and Table 12 characterizes the data base provided in some evaluation systems. Finally, Table 13 indicates the nature of the reports each method provides on security system performance.

TABLE 1. DESIGNATIONS OF SECURITY EVALUATION METHODS

DESIGNATION	TITLE AND ORGANIZATION
"GLOBAL" EVALUATION	
SAFE	Safeguards Automated Facility Evaluation (Sandia National Laboratories)
SSEM	Site Security Evaluation Model (TRW)
PANL	Path Analysis (Sandia National Laboratories)
VISA	Vulnerability of Integrated Safeguards Analysis (Science Applications, Inc.)
ASM	Aggregated Systems Model (Lawrence Livermore Laboratory)
SURE	Safeguards Upgrade Rule Evaluation (Sandia National Laboratories)
MAIT	Matrix Analysis of the Insider Threat (Science Applications, Inc.)
SVAP	Safeguard Vulnerability Analysis Program (Lawrence Livermore Laboratory)
SSNI	Sensor System Nullification by Insiders (Sandia National Laboratories)
SAA	Structured Assessment Analysis (Analytic Information Processing and Lawrence Livermore Laboratory)
SCENARIO EXAMINATION	
SSPAM	Security System Performance Assessment Method (Mission Research Corporation)
FSNM	Fixed Site Neutralization Model (Vector Research, Inc., for Sandia Laboratories, Albuquerque)
PROSE	Protection System Evaluator (John E. Lenz University of Wisconsin at Oshkosh)
SNAP	Safeguards Network Analysis Procedure (Pritsker and Associates for Sandia National Laboratories)
FESEM	Forcible Entry Safeguards Effectiveness Model (Sandia National Laboratories)

TABLE 1. DESIGNATIONS OF SECURITY EVALUATION METHODS (continued)

DESIGNATION	TITLE AND ORGANIZATION
NEWMOD	(Technical Support Organization, Brookhaven National Laboratory)
GPPLT	Generic Physical Protection Logic Trees (Sandia National Laboratories)
SOURCE	(Sandia National Laboratories)
SABRES	(Sandia National Laboratories)
SAS	Stand-Off Attack Simulation (Jaycor)
SAM	Security Analytic Methodology (Los Alamos National Laboratory for Air Force Weapons Laboratory)
ISEM	Insider Safeguards Effectiveness Model (Sandia National Laboratories)
BOARD GAMES	
GTS	Guard Tactics Simulation (Nuclear Regulatory Commission)
NWSSBG	Nuclear Weapon Storage Site Board Game (Booz-Allen and Hamilton)
SKIRMISH/ AMBUSH	(Sandia National Laboratories)

TABLE 3. AVAILABILITY OF SECURITY EVALUATION AIDS

METHOD	STATUS	PAST APPLICATION	DOCUMENTATION*	UTILIZATION LIMITATIONS
SAFE	Exists	Several fuel cycle and storage fac.	Comprehensive user's manual	--
SSEM	Exists	Numerous sites, incl. 3 wpns. storage sites	Comprehensive user's manual (Secret)	Can be run by TRW or government users
PANL	Exists	Several DoE facilities, DoD weapons storage sites	Program user's manual (method description in classified TRW report	--
VISA-2	Methodology exists (no specialized codes)	Weapon storage sites	Meeting paper abstract, briefing charts	--
ASM	Exists	Two fabrication facilities	Overview, several detailed worked examples	Requires better documentation. Can be applied by LLNL.
SURE	Exists (including computer aids)	One application to an hypothetical security system	Comprehensive user's manual	Evaluation against NRC's safeguards upgrade rule only
MAIT	Exists	DoE storage site	Comprehensive user's manual	--
SVAP	Exists	2 DoE storage sites, a reactor, 2 fuel cycle facilities	Comprehensive user's manual	--
SSNI	Parts of the analysis use existing codes	None	Method outline with an example	Much of the analysis must be done by hand
SAA	Exists	One for an NRC physical protection problem, several to MC&A systems	Comprehensive user's manual	--
SSPAM	80% implemented	Exercises, including some for actual sites	Concept description, preliminary programmer's manual	Requires further development and documentation

TABLE 3. AVAILABILITY OF SECURITY EVALUATION AIDS (continued)

METHOD	STATUS	PAST APPLICATION	DOCUMENTATION*	UTILIZATION LIMITATIONS
FSNM	Runs on one special computer	Input prepared for one hypothetical facility	Comprehensive user's manual	Requires final debugging & testing
PROSE	Some implementation planning completed	None	Concept description (including some implementation plans)	Not yet implemented
SNAP	Exists	A fuel cycle facility, a reactor, a ship	User's manual, general description	--
FESEM	Exists	Numerous facility studies	Comprehensive user's manual	--
NEWMOD	Exists	Several DoE facilities	Comprehensive user's manual	--
GPPLT	Exists (no computer assistance)	Physical protection training school applications	Comprehensive user's manual	--
SOURCE	Exists	?	Comprehensive user's manual	Ambush phase of road convoy attack only
SABRES	Exists	?	Comprehensive user's manual	Combat engagement only
SAS	Exists (improvements in progress)	Road convoy example	Comprehensive user's manual	May require further exercise and testing
SAM	Exists (uses EASI/BATLE from SAFE)	Nuclear weapon system transport, field dispersal problems	Comprehensive user's manual	--
ISEM	Exists	7 facilities	Comprehensive user's manual	--

*Comprehensive user's manual = Description + instructions for program use + detailed code description or listing

TABLE 4. COMPUTER IMPLEMENTATION OF METHODS

METHOD	COMPUTER	PROGRAMMING LANGUAGE	RESOURCE REQUIREMENTS (Memory Size, Time)
SAFE	CDC 6600 + TEKTRONIX 4050	FORTRAN + BASIC + Graphics Software	33,000 x 60 bit, few minutes per run
SSEM	IBM 360/158, etc., + H-P 9800	FORTRAN + BASIC	100,000 x 64 bit, tens of minutes
PANL	CDC 6600	FORTRAN + Graphics Software	
VISA	Generally None	---	---
ASM	CDC 6400		10,000 words, few seconds.
SURE	CDC 6600 (for scoring questionnaires)	FORTRAN	Modest
MAIT	DEC System 10	FORTRAN	42,000 x 32 bit, minutes to tens of minutes
SVAP	CDC 7600 + TEKTRONIX 4050	LLLTRAN & BASIC	Strongly dependent on problem complexity
SSNI	CDC 6600 (for SETS)	FORTRAN	Strongly dependent on problem complexity
SAA	CDC 7600		"Few thousand" to 426,000 x 60 bit; a few minutes through level 3; minutes to an hour for level 4.
SSPAM	DEC VAX 11/780	FORTRAN	Few minutes (~0.5 x simulated time)
FSNM	AMDAHL 470V/6	FORTRAN	100,000 x 32 bit with virtual memory; 300,000 words otherwise
SNAP	CDC 6600	FORTRAN	33,000 x 60 bit (virtual memory internal to code), 10s to 100 seconds (strongly dependent on model complexity)

TABLE 4. COMPUTER IMPLEMENTATION OF METHODS (continued)

METHOD	COMPUTER	PROGRAMMING LANGUAGE	RESOURCE REQUIREMENTS (Memory size, time)
FESEM	CDC 6600	Gasp IV, FORTRAN	35,000 x 60 bit, few tens of seconds
NEWMOD	CDC 6600	FORTRAN	25,000 x 60 bit, few seconds
GPPLT	none	---	---
SOURCE	CDC 6600	FORTRAN	33,000 x 60 bit, ~1 second
SABRES	CDC 6600	FORTRAN (+ Graphics software for interactive version)	Interactive: 33,000 x 60 bit, few seconds to few tens of seconds Monte Carlo: 80,000 x 60 bit, 1.25 hours
SAS	VAX 11/780	FORTRAN	
SAM	CDC 7600	FORTRAN + Graphics software	Few seconds per run (10s to 100s for sensitivity studies)
ISEM	CDC 6600	Gasp IV, FORTRAN	35,000 x 60 bit, <10 seconds

TABLE 5. SCOPE OF SECURITY ASSESSMENT METHODS

METHOD	ADVERSARY GOALS	ADVERSARY MODES	SECURITY SYSTEM FUNCTIONS*	SECURITY SYSTEM ELEMENTS**	OUTPUT (SEE TABLE IV-12)
SAFE	Theft (T) or sabotage (S)	Stealth, force	Complete	Complete	Critical paths, probability of detection, interruption, or adversary success
SSEM	T[†] or S	Stealth, force (against obstacles), limited deceit	Detection	Complete	Critical paths, probability of interruption
PANL	T or S	Stealth, force	Detection, delay, reaction	∿Complete	Critical paths, probability of interruptions, or adversary success
VISA	T or S	Note A	Note A	Note A	Choice of several quantitative measures of effectiveness for "worst" cases
ASM	T	Stealth	Detection	Monitors, guards, records	Performance of safeguards against most threatening attack
SURE	T or S	Note B	Complete	Complete	Score for compliance with 10 CFR 73.45 requirements.
MAIT	Access for T or S	Stealth, insider privilege	Access control	Detection and delay devices	Critical access routes; critical insider combinations
SVAP	T	Stealth, insider privilege, deceit	Detection, communication, reaction	Monitors, communication system, power system	Critical diversion paths; critical insider combinations
SSNI	T	Insider privilege	Access control	Access control procedures	Critical insider combinations
SAA	T	Stealth, insider privilege, tampering	Detection communication	Monitors, communication system, power system	Critical diversion paths, critical adversaries
SSPAM	T or S	Stealth, force, deceit	Complete	Complete	Log of scenario, including performing of security system elements
FSNM	T or S	Stealth, force, deceit	Complete	Complete	Log of scenario
PROSE	T or S	Stealth, force, deceit	Complete	Complete	Not yet implemented

TABLE 5. SCOPE OF SECURITY ASSESSMENT METHODS (continued)

METHOD	ADVERSARY GOALS	ADVERSARY MODES	SECURITY SYSTEM FUNCTIONS*	SECURITY SYSTEM ELEMENTS**	OUTPUT (SEE TABLE IV-12)
SNAP	T or S	Stealth, force, deceit	Complete***	Complete***	Log of scenario
FESEM	T or S	Stealth, force, limited deceit	Complete	Complete	Log of scenario
NEWMOD	T or S	Stealth, force	Delay and part of reaction	Note C	Numbers of adversaries and guards vs. time at protected area and intercept point
GPPLT	T or S	Stealth, force, deceit	Complete	Complete	Verdict of security system adequacy in scenario, identity of weak elements
SOURCE	Convoy ambush	Force	Complete	Guards, communication equipment	Scenario logs, expected status at end of ambush.
SABRES	T or S	Force	Delay, neutralization	Barriers, locks, guards	Scenario log, statistics of combat outcomes
SAS	S (from a distance)	Force	Delay, neutralization	Guards, armor	Probability log for scenario
SAM	T or S	Stealth, force	Complete	Complete	Probability of adversary success (possibly for a range of threats)
ISEM	T or S	Stealth, force limited deceit	Complete	Complete	Probability of detection and defeat for specified scenario

*"Complete" - Detection, communication, delay and reaction.
**"Complete"- Barriers, locks, sensors, alarms, procedural controls, guards, communication, response forces.
***If modeler chooses to include all capabilities.
†For theft, SSEM treats access phase only.

Note A - As considered by the analyst (not prescribed by methodology).
Note B - Adversary activities treated only implicitly.
Note C - Complete, except limited treatment of probability for detection or alarm.

TABLE 6. ADVERSARY ATTRIBUTES CONSIDERED

METHOD	Number/Size of Independent Groups	Physical Capability/ Performance Estimates	Weapons	Penetration Equipment	Transport	Communication System Performance	Insider Privileges/ Combat Assistance	Psychological Characteristics	Tactical SOP's	Plans/Leadership	SUMMARY	
SAFE	1/N*	/	x	/	/	--	--/--	--	--	--	SAFE	Single group; no explicit insiders; variable weapons, combat training; penetration capabilities implicit in task parameters (delay times and detection probabilities).
SSEM	1/N	X	--	x	--	--	x/--	--	--	--	SSEM	Single group; insiders or outsiders, not both; variable penetration capabilities.
PANL	1/N	x	x	--	x	--	x/--	--	--	--	PANL	Single group chosen from 14 standard types; adversary attributes considered in deriving detection and delay expressions.
VISA	N/N	--	-	--	--	--	--	--	--	--	VISA	Adversary characteristics considered vary from analysis to analysis.
ASM	1/N	--	--	--	--	--	x/--	x	--	--	ASM	Adversaries chosen from standard classes; adversary attributes, including level of adversion to capture considered in estimating some model parameters.
SURE	--	--	--	--	--	--	--	--	--	--	SURE	Adversary attributes considered only implicitly.
MAIT	1/1 or 2	--	--	--	--	--	x/--	--	--	--	MAIT	All possible single insiders † or pairs of insiders; access privileges, control privileges.
SVAP	1/N	--	--	--	--	--	x/--	--	--	--	SVAP	Insider privileges are only characteristic considered.
SSNI	1/N	--	--	--	--	--	x/--	--	--	--	SSNI	Insider privileges are only characteristic considered.
SAA	1/N	--	--	--	--	--	x/--	--	--	--	SAA	Insider privileges are only characteristic considered explicitly; tampering ability is implicitly assumed.
SSPAM	N/N	x	x	x	x	x	x/x	x	x	x	SSPAM	Multiple groups; insiders; variable sizes, capabilities, weapons, equipment, transportation.
ESNM	N/N	x	x	x	x	x	x/x	x	x	x	ESNM	Multiple groups; insiders, variable sizes, capabilities, weapons, equipment, transportation.
SNAP	N/N	x	x	x	x	x	--/x	--	x	--	SNAP	Multiple, variable groups; active** insiders; variable weapons, training, etc.

TABLE 6. ADVERSARY ATTRIBUTES CONSIDERED (continued)

METHOD	Number Size of Independent Groups	Physical Capability/ Performance Estimates	Weapons	Penetration Equipment	Transport	Communication System Performance	Insider Privileges/ Combat Assistance	Psychological Characteristics	Tactical SOP's	Plans/Leadership	SUMMARY	
FLSEM	1/N	/	x	x	x	--	x/--	--	--	--	FLSEM	Single group; limited insiders; variable weapons, penetration equipment, transportation, general capability, detection.
NEWMOD	1/N	x	--	x	x	--	--	--	--	--	NEWMOD	Single group; variable performance capability, penetration equipment, transportation.
GPPLT	1/N	--	--	--	--	--	--/--	--	--	--	GPPLT	Analyst implicitly considers adversary attributes in analyzing primary events of logic trees.
SOURCE	N/1	--	x	--	--	--	--/--	--	--	--	SOURCE	One or more adversaries, positioned to fire at a convoy from ambush.
SABRES	N/1	/	x	/	--	--	--/--	/	x	--	SABRES	Independent individuals, variable target characteristics, weapons, physical and psychological status; common penetration capability for all adversaries; preset individual plan sets.
SAS	N/1	--	x	--	--	--	--/--	--	--	--	SAS	Independent individuals with fixed event lists, variable weapons.
SAM	1/N	/	x	/	/	--	--/--	--	--	--	SAM	As for SAFE.
ISEM	1/1 +covert assistance	/	/	/	/	--	x/--	--	--	--	ISEM	Single active** insider; covert insider assistance; variable capabilities, weapons, penetration equipment.

*"N" represents any reasonable matter
x = yes
/ = in part
-- = not explicitly

+ For MAIT, an insider is anyone who can exercise access or control privileges. He can be an outsider who deceives the security system.

** The term "active" means that the insider adopts a role equivalent to that of an outsider. This can involve both stealth and force.

TABLE 7. ADVERSARY ACTIVITIES CONSIDERED

METHOD	Attack Guard Forces	Tamper with Sensors and Alarms	Tamper with Security System Communications	Penetrate Barriers	Damage Protected Asset (Sabotage)	Remove Protected Asset (Theft)
SAFE	--	--	--	x	x	x
SSEM	--	x	--	x	/	/**
PANL	--	--	--	x	x	x
VISA	--	--	--	x	x	x
ASM	--	--	--	/	--	x
SURE	--	/	/	/	--	--
MAIT	--	x	--	--	/	/
SVAP	--	/	/	--	--	x
SSNI	--	--	--	--	--	x
SAA	--	x	x	--	--	x
SSPAM	x	x	x	x	x	x
FSNM	x	x	x	x	x	x
SNAP	x	x	x	x	x	x
FESEM	x*	/	/	x	x	x
NEWMOD	--	--	--	x	x	x
GPPLT	x	x	--	x	x	x
SOURCE	x	--	--	--	--	--
SABRES	x	--	--	x	--	x
SAS	x	--	--	--	x	--
SAM	--	--	--	x	x	x
ISEM	--	x	--	x	x	x

x = Yes
/ = In part
-- = Not explicitly

*At the outset of an engagement which would take place anyway
**For theft, SSEM models access phase only

TABLE 8. GUARD ATTRIBUTES CONSIDERED

METHOD	Number/Size of Independent Groups	Physical Capability/ Performance Estimates	Tactical SOP's	Communication System Performance	Weapons	Response Time Estimates	Command and Control System
SAFE	N/N	x	--	--	x	x	--
SSEM	N/N	x	x	--	--	x	x
PANL	N/N	/	--	--	x	x	--
VISA	N/N	--	--	--	--	--	--
ASM	--/--	/	--	--	--	--	--
SURE	N/N	x	x	x	x	x	x
MAIT	--/--	--	--	--	--	--	--
SVAP	N/N	--	x	--	--	--	--
SSNI	--/--	--	--	--	--	--	--
SAA	--/--	--	--	/	--	--	/
SSPAM	N/N	x	x	x	x	x	x
FSNM	N/N	x	x	x	x	x	x
SNAP	N/N	x	x	x	x	x	x
FESEM	N/N	x	x	x	/	x	/
NEWMOD	N/N	--	--	--	--	x	--
GGPLT	--/--	--	--	/	--	/	/
SOURCE	N/1	--	x	x	--	/	/
SABRES	N/1	x	x	--	x	--	--
SAS	N/1	--	--	--	x	/	--
SAM	N/N	x	--	--	x	x	--
ISEM	N/N	x	x	/	x	x	--

N = Any reasonable number

x = Yes

/ - In part

-- = Not explicitly

TABLE 9. SECURITY SYSTEM HARDWARE

METHOD	Facility Spatial Layout	Facility Expressed as List of Locations and Interconnections	Facility Expressed as Path = List of Barriers, Etc.	Component Performance Estimates	Subsystem Performance Estimates	Component/Subsystem Vulnerability
SAFE	X	X	--	X	--	--
SSEM	X	--	--	X	--	X
PANL	--	--	X	X	--	--
VISA	--	--	/	/	/	--
ASM	--	--	X	X	X	--
SURE	/	--	--	X	X	X
MAIT	--	X	--	--	--	/
SVAP	--	X	--	--	/	/
SSNI	--	X	--	--	--	--
SAA	--	X	--	X	--	X
SSPAM	X	--	--	X	--	X
FSNM	--	X	--	X	--	X
SNAP	--	X	--	X	--	X
FESEM	--	--	X	X	--	X
NEWMOD	--	--	X	/	--	/
GPPLT	--	--	X	X	--	X
SOURCE	X	--	--	--	--	X
SABRES	X	--	--	--	--	--
SAS	X	--	--	--	--	X
SAM	--	--	X	X	--	--
ISEM	--	--	X	X	--	X

X = Yes
/ = In part
-- = No

TABLE 10. SECURITY SYSTEM ACTIVITIES CONSIDERED

METHOD	Surveillance	Detection	Communication	Assessment (Delay)	Reaction (Delay)	Combat Engagement	Adversary Delay (Via Barrier Activation or Engagement)
SAFE	--	X	--	--	X	X	X
SSEM	X	X	*	--	*	--	--
PANL	--	--	--	--	X	X	X
VISA	--	--	--	--	--	--	--
ASM	X	X	--	X	--	--	--
SURE	X	X	X	X	X	X	--
MAIT	--	--	--	--	--	--	--
SVAP	X	X	--	--	X	--	--
SSNI	--	--	--	--	--	--	--
SAA	--	--	--	--	--	--	--
SSPAM	X	X	X	X	X	X	X
FSNM	X	X	X	X	X	X	X
SNAP	X	X	X	X	X	X	X
FESEM	--	X	X	--	X	X	X
NEWMOD	--	--	--	--	X	--	X
GPPLT	X	X	--	--	X	X	--
SOURCE	X	X	X	X	--	--	--
SABRES	X	X	--	--	--	X	X
SAS	--	--	--	--	X	X	--
SAM	--	X	--	--	X	X	X
ISEM	--	X	--	--	X	X	X

X = Yes
-- = Not explicitly
* = In auxiliary submodels

TABLE 11. TREATMENT OF PROBABILITY IN SIMULATION

METHOD	Analytic Probability Calculation	Single Random Draw	Monte Carlo
SAFE	/	--	/
SSEM	X	--	--
PANL	X	--	--
VISA	/	--	--
ASM	X	--	--
MAIT	--	--	--
SVAP	--	--	--
SSNI	--	--	--
SAA	X	--	--
SSPAM	/	/	--
FSNM	/	/	--
SNAP	/	--	/
FESEM	/	--	/
NEWMOD	X	--	--
GPPLT	--	--	--
SOURCE	--	--	X
SABRES	--	/	/
SAS	/	--	/
SAM	X	--	--
ISEM	/	--	/

X = Yes
/ = In part
-- = No

TABLE 12. DATA BASE

METHOD	Barrier Performance Data	Detection System Performance Data	Adversary Equipment Performance Data	Guard Equipment Performance Data	Adversary Human Factors Data	Guard Human Factors Data
SAFE*	X	S	/	/	/	/
SSEM	X	X	/	/	/	/
PANL	R	R	/	/	/	/
ASM	--	R	/	--	R	--
SURE	S	S	--	S	--	R
MAIT	--	--	--	--	--	--
SVAP	--	--	--	--	--	--
SSNI	--	--	--	--	--	--
SAA	--	R	--	--	--	--
SSPAM	X	X	X	X	R	R
FSNM	R	R	R	R	R	R
SNAP	R	R	R	R	R	R
FESEM	S	S	S	S	/	/
NEWMOD	X	--	X	--	/	/
GPPLT	R	R	R	R	R	R
SOURCE	--	--	X	X	/	--
SABRES	R	--	X	X	R	R
SAS	--	--	X	X	--	--
SAM	R	R	/	/	/	/
ISEM	R	R	/	/	/	/

X = Extensive data provided in the code
/ = Limited data provided in the code
S = Suggested input data provided in documentation
R = Required as input but not provided
-- = Not considered explicitly

*with SEAD interface

TABLE 13. OUTPUTS

METHOD	Probability of Success	Probability of Timely Detection	Probability of Interruption	Probability of Detection	Outsome of Scenario(s)					Critical Security System Elements	Critical Paths	Critical Insiders
					Time to Complete	Winner	Objective Accomplished	Details of Scenario Chronology	Details of Security System Elements Performance			
SAFE	X	X	X	X	X	X	--	--	--	/	X	--
SSEM	/	--	X	X	/	/	/	--	X	/	X	--
PANL	X	X	--	--	--	X	X	--	--	/	X	--
VISA	X	--	--	--	--	X	X	--	--	--	--	--
ASM	X	--	--	X	--	/	/	--	--	/	/	--
SURE*	--	--	--	--	--	--	--	--	X	--	--	--
MAIT	--	--	--	--	--	--	--	--	--	X	X	X
SVAP	--	--	--	--	--	--	--	--	--	X	X	X
SSNI	--	--	--	--	--	--	--	--	--	/	/	X
SAA	--	--	--	X	--	--	--	--	X	X	X	X
SSPAM	--	--	--	--	X	X	X	X	X	--	--	--
FSNM	--	--	--	--	X	X	X	X	X	--	--	--
SNAP	X	--	X	X	X	X	X	X	X	--	--	--
FESEM	X	--	X	X	X	X	X	--	X	--	--	--
NEWMOD	/	--	X	--	/	/	/	/	--	--	--	--
GPPLT	X	--	--	/	--	X	X	--	--	--	--	--
SOURCE	X	--	--	--	X	X	X	/	--	--	--	--
SABRES	X	--	--	--	/	/	/	X	--	--	--	--
SAS	X	--	--	--	X	X	X	X	--	--	--	--
SAM	X	--	--	X	/	X	X	X	--	--	--	--
ISEM	X	--	X	X	--	X	X	--	--	--	--	--

X = Routinely provided.
/ = Available on request or easily extracted.
-- = Not routinely available.
*Output = Score for compliance with 10 CFR 73.45.

2. A PHYSICAL SECURITY SYSTEM EVALUATION TOOL KIT

An ideal physical security evaluation technique would meet a number of demanding requirements. First it should be easy to learn and use. It should provide extensive assistance in data entry and verification, including access to a compatible data base containing reliable experimental performance parameters (or agreed-upon parameters chosen by security community consensus). Using sound, credible analytic techniques, the method should produce useful results, and present them clearly. It should help the analyst to identify all the important vulnerabilities of a security system, and to trace those vulnerabilities to limiting elements in the system's design. The technique should provide assistance in carrying out sensitivity studies which accurately reflect changes in security system performance when elements of the system or the threat are modified. Finally, the ideal technique should be economical in its requirements for analyst skill and time. (Economy of computer resources is also desirable, but this has become a less important constraint as computing power has become less costly.)

No currently available evaluation technique meets all of these criteria. Moreover, no single current method provides all of the available capabilities that a security system evaluator or planner could profitably employ in a facility examination.* Much would be gained in economy and consistency if one system of evaluation techniques with a single set of input requirements and a common data base *could* carry out all evaluation functions. At present, complementary techniques are separately available which *together* can provide considerable insight into the adequacy

*The modeling groups sponsored at Sandia Laboratories by the Nuclear Regulatory Commission and the Department of Energy have made substantial progress toward this goal over the last few years.

of a physical security system. In the remainder of this section we suggest some possible choices for a useful mosaic of methods.

a. Global evaluations--To obtain an overview of the vulnerability of a security system to physical assault, the model of choice at present is probably SAFE. It is mature, readily available, adequately documented, and supported by a strong ongoing development effort at Sandia. SAFE's recently documented provisions for automated input assistance have made it much easier to use. Automatic access to Physical Protection Handbook data (Ref. 7), which would make it even more easy to use, is likely to be added quickly when the matter of safeguards classification is resolved in the near future. SAFE's minimum-timely-detection-probability criterion for critical paths is as sound as any now in use. Its preliminary examination of critical paths using EASI and BATLE provides a good starting point for further evaluation. When the SAFE-SNAP interface is completed, SAFE analysts will be able to carry out detailed critical path examinations quite efficiently.

SSEM is a close competitor for the global evaluation function. It offers some advantages over SAFE in certain applications, particularly those in which unusual circumstances cast tabulated component performance data into doubt. The security classification of the SSEM code and its documentation, which has been an important impediment to widespread use of SSEM, does not present a problem for DNA.

7. Intrusion Detection Systems Handbook, SAND76-0554, Sandia National Laboratories, October 1977.
Entry Control Systems Handbook, SAND77-1033, Sandia National Laboratories, September 1977.
Barrier Technology Handbook, SAND77-0777, Sandia National Laboratories, April 1978.

Preparation of input data for SSEM is relatively simple, since many of the required data are built into the code for user selection. Full integration of a good combat engagement model (for completion of the critical path examination) would make it an even stronger competitor.*

To provide a global examination of the security consequences of insider privileges in relatively simple installations, we would choose to use MAIT. It is relatively easy to use, conservative from the point of view of the security system, and thorough within its range of concern. Those qualities (and its transparent simplicity) have won it wide acceptance in the security system evaluation community.

b. Scenario Examination Techniques--Choice of a model to simulate an interesting scenario--suggested by a global evaluation model or by the evaluator's imagination--presents the same difficulties now as it did at the time of RDA's last assessment.

If a simple treatment is adequate, as is often the case, the stand-alone version of SAFE's EASI/BATLE combination is as good as anything currently available. It is sound, well documented, and treats--in some way--all the basic processes in the physical protection problem (detection, adversary progress and delay, guard force response, and combat engagement). It is as easy to use as any current evaluation tool.

The more detailed scenario simulation models continue to present difficult choices. SSPAM is not quite complete, and will require more testing and documentation before it can be used with confidence. FSNM has had some limited tests but is not yet entirely debugged. It cannot now be

*We do not know whether TRW's plans to acquire and run SABRES II extend to integration of that code with SSEM, i.e., use of common data, matching of SSEM output with SABRES input, etc.

used on most computer systems, and there are no immediate plans for further development. Both SSPAM and FSNM require human factors data that are not now available, and that may prove difficult or impossible to obtain. SABRES II, which shares this problem, is complete and documented. Unfortunately, it treats only the combat engagement phase of a scenario.

SNAP is the only currently available, adequately documented modeling system that can carry out general detailed scenario simulations. Because it is uniquely flexible, it almost certainly belongs in the standard security system evaluation modeling kit. It is not, however, a convenient substitute for more rigidly defined models like SSPAM and FSNM, which should require less user attention to completeness and validation.

c. Special purpose models--The global models and complete scenario simulations just described are designed to examine the performance of conventional security systems at relatively large fixed sites. More specialized tools could be quite useful to the analyst in examining other situations.

Stand-off attack simulation provides an example of this within DNA's range of concerns, which include examination of small site and transport scenarios. As noted in our discussions of models in Chapter III, survivability of equipment (especially vehicles, and protected assets) is a more important consideration in such situations than it is for the more commonly modeled attacks. The two models we have examined that attempt to address survivability within the context of security problems--Sandia/Livermore's SOURCE and Jaycor's SAS--have differing strengths and weaknesses, which makes a choice between them difficult (and perhaps inappropriate). SOURCE deals with most important aspects of the convoy problem, but does not allow the vehicles to seek cover or the guard force to return fire. (Its companion engagement model, SABRES II, does not examine vehicle or cargo vulnerability.) SAS allows guards to return fire and to move a bit more freely, but treats some convoy characteristics in a less natural way than SOURCE. Both SOURCE and SAS impose artificial geometric constraints on the analyst's freedom to specify realistic scenarios. Despite their shortcomings,both could be useful.

d. Hardware for security system modeling--Though we have not done a detailed analysis of the computing requirements of an hypothetical modeling group, we have noticed significant convergence of opinion in the modeling community, and can report a tentative consensus. The basic computational tool chosen by most modeling groups at the time of our last survey was a large main frame computer. Increasingly, this choice has shifted to high performance minicomputers (the Digital Equipment VAX 11 is a strong favorite) with virtual memory operating systems. Most modelers now consider a graphic tablet attached to an interactive data entry system (with built-in display capabilities) almost essential for accurate, cost effective preparation of input for the more elaborate models. Most modeling groups prefer TEKTRONIX 4050 series microcomputers, with various compatible tablets, to support this part of the system.

3. OBSERVATIONS ON SECURITY SYSTEM MODELING

It is impractical (if not impossible) to

- incorporate *all* relevant features in a security system simulation or
- *definitively* validate a security system model.

Some analysts will always have low confidence in a simulation that does not consider every known factor in great detail. Unfortunately, even if such detailed simulations were computationally feasible, many of the required data are unavailable (and likely to remain so). This data problem is the most convincing argument against the common assumption that greater detail necessarily implies either greater accuracy or greater credibility. Problems of practicality and validation do not excuse the modeler from his responsibility to:

- create practical models that include the *most important* relevant features to produce suggestive, useful and demonstrably plausible results and
- select data and submodels that reflect the realities of the security systems as closely as the state of the art will allow.

Two useful aids in fulfilling the model designer's responsibilities are trial sensitivity studies--in which simulation runs are compared with one another to see if the results reflect changes in parameters and data in a reasonable way--and test examinations of real-world facilities--which allow evaluations based on modeling to be compared with conclusions of security system professionals.

Calculation of either human or mechanical component performance measures by modeling is conceptually separable from the process of combining those performance measures to simulate overall system behavior. A modeling system that attempts both may carry out one of these tasks (component or system modeling) better than it does the other. It may be sensible to separate these two tasks, at least during model development, so that their contributions to shortcomings in system evaluation capabilities or to excessive demand for computational resources can be distinguished.

Several modeling groups have found that detailed simulations that use fixed time steps tend to become very demanding of computer time in scenarios of even moderate complexit,. They blame part of the problem on the fact that the time step size must be set at a value that reflects the shortest event to be simulated. They hope that variable time step simulations--in which only those events that are fast are examined in fine temporal detail--will prove much more efficient.

Much has been learned in each attempt to produce a new generation of physical security system evaluation algorithms. An important part of the learning process takes place when model developers make a serious attempt to identify and correct the deficiencies of the previous generation's methodology.

4. OBSERVATIONS ON SECURITY SYSTEM EVALUATION

Standardized evaluation procedures (that are updated at intervals of a few years to reflect current understanding of the physical security problem) can be valuable aids to security system designers. Computer models can play a valuable role in such procedures.

The comprehensive requirements of an adequate simulation can structure the initial data-gathering phase of a security system evaluation in a particular fruitful way. In fact, a significant fraction of the benefit of such an evaluation is often realized in this phase, as "obvious" weaknesses are uncovered.

Because computer models can be unusually thorough, they may uncover vulnerabilities which would elude a human evaluator. However, because no model or group of models is likely to consider the more imaginative attacks a creative professional might suggest, computerized procedures can constitute only part of a sound evaluation process. A promising candidate for such a process is one in which experts and modelers interact, with each identifying the vulnerabilities their technique is best at uncovering and then providing their findings to the other group, for reexamination using a different set of tools.

Models can provide a framework within which experts can reach consensus decisions on security system adequacy. It should be much easier to reach agreement on parameters and methodology in the abstract than it would be to blend personal judgements of specific total systems. Moreover, expert opinions on well-defined and circumscribed questions of component performance are likely to be more credible (and sounder) than the same experts' global evaluations.

An assessment that compares the performance of two candidate security system designs against unrealistically capable adversaries is likely to find both systems seriously wanting. More might be learned in a comparison that includes a variety of adversaries with varying capabilities (perhaps over a range that *culminates* at human limits).

Examination of a security system for adequacy against insider threats is important. Personnel clearance programs have such a low rate of rejection that they cannot be presumed to provide significant protection (Ref. 8), and so insiders must be considered as potential adversaries. In addition, if an evaluation technique can adequately treat threats arising from adversaries with insider privileges, and the security system defeats these threats in the simulations, the system is likely to perform well against adversary deceit, which includes illegitimate attempts to exercise insider privileges.

Some plausible adversary activities are much more difficult to model than others. There is an understandable tendency to omit them, or to treat them in some awkward way. The evaluator has a special responsibility to consider activities that are difficult to simulate separately, *outside* the context of automated assistance, in assessing the adequacy of a security system.

Code originators, who know all the peculiarities of a given model (including the precise meaning of the numbers that go in at the beginning and come out at the end) are very effective--if not essential--members of teams that use the model in security system evaluations. Conversely, site personnel should be actively involved in data gathering and analysis. (Often, safeguards or procedures are brought to the attention of the analyst only when site personnel become aware that neglect of them has produced a poor initial rating.)

8. Perry, R.W., Bennett, C.A., Wood, M.T., The Role of Security Clearances and Personnel Reliability Programs in Protecting Against Insider Threats, B-HARC-411-018, Battelle Human Affairs Research Centers, July 1979.

5. OBSERVATIONS ON THE USES OF PHYSICAL SECURITY SYSTEM EVALUATION METHODS

Properly used, systematic security system evaluation techniques can be useful to policymakers, managers, system designers, and researchers.

Policymakers and researchers can use these techniques to examine a broad range of real or hypothetical systems, to identify and understand factors that determine the success or failure of security systems. Researchers do so to advance the state of the art, policymakers to develop criteria for guidance of designers and evaluators. The questions both ask are some variant of "What kinds of system elements, in what combinations, can provide adequate levels of protection?"

Managers and system designers tend to focus more sharply on specific systems, often within a relatively narrow range of excursions from a base case. They may be interested in evaluating operational systems, current available hardware and procedure options (for improvement of systems in place), designs of potential options (for next generation systems), or projects and proposals for development of future options (advanced concepts). Their question is "How well will a particular system, with its particular set of functional characteristics, perform specific protective functions?"

Both sets of users will take advantage of whatever capabilities their chosen methods provide to screen many options economically. Typically, they will examine a candidate design, modify it in ways suggested by the examination, subject it to analysis again to uncover new modification possibilities, etc. The evaluation method's basic function in this process (whatever its object) is to rank alternatives in a systematic and consistent way.

REFERENCES

1. Davidson, R.B., and Rosengren, J.W., An Assessment of Current Physical Security Models, R & D Associates, RDA-TR-111500-001, October 1979.

2. Gref, L.G., and Rosengren, J.W., An Assessment of Some Safeguards Evaluation Techniques, R & D Associates, NUREG-0141, RDA-TR-5000-002, February 1977.

3. Department of Defense, Security Criteria and Standards for Protecting Nuclear Weapons, Directive 52140.41, 30 July 1974.

4. Department of Defense, Nuclear Weapons Security Manual, Unpublished.

5. Dowdy, E.J., and Mangan, D.L., A Review of Safeguards and Security Systems Effectiveness Evaluation Methodologies, Office of Safeguards and Security, Department of Energy, January 1980.

6. Paulus, W.K., Survey of Insider Safeguards Effectiveness Evaluation Models, Sandia National Laboratories, SAND 80-2580, October 1980.

7. Intrusion Detection Systems Handbook, SAND 76-0554, Sandia National Laboratories, October 1977.
   Entry Control Systems Handbook, SAND 77-1033, Sandia National Laboratories, September 1977.
   Barrier Technology Handbook, SAND 77-0777, Sandia National Laboratories, April 1978.

8. Perry, R.W., Bennet, C.A., Wood, M.T., The Role of Security Clearnaces and Personnel Reliability Programs in Protecting Against Insider Threats, B-HARC-411-018, Battelle Human Affairs Research Centers, July 1979.

APPENDIX A. GLOSSARY OF SELECTED TERMS IN PHYSICAL SECURITY AND MODELING*

Access Privilege: Authorization to enter a protected area or to have access to a security system component or to a protected object.

Adversary: An individual or an organized group threatening health, safety, or national security through an intention to commit malevolent acts involving protected objects, e.g., nuclear weapons.

Adversary Action Mode: Force, stealth, deceit, or a combination of these; a property or characteristic of particular adversary actions.

Alarm: A mechanism to warn or alert the guard force; generally consisting of some form of sensor, e.g., an interruptable microwave beam and detector, and a device to communicate signals from the sensor to the security force.

Assessment (of an alarm): Action by members of the security force, to determine whether an activated alarm indicates an actual threatening situation or is a false alarm, or to collect further information on the origin of an alarm signal.

Barrier: A material object or set of objects that separates, demarcates, or (most usually) impedes passage, e.g., a locked vault door.

Component (security-system component): A mechanism that helps carry out one or more of the assigned functions of the security system, e.g., an alarm or a barrier.

*This glossary defines terms in the context in which they are used in this report; the definitions may differ somewhat from those used by other authors.

PRECEDING PAGE BLANK-NOT FILMED

Control Privilege: Authorization to control operation or operability of a security system component or a security system procedure, e.g., access control at a portal, activation of an intrusion sensor.

Covert Activity: An activity that has not been recognized by the security system.

Critical Insiders: An insider, or some combination of a few insiders, that has high capability or the highest capability (based on access and control privileges) to carry out successfully an adversary action.

Critical Path: A penetration path that, by some measure, provides an adversary with a high probability (or the highest probability) of successful accomplishment of his goal.

Data Base: An organized collection of data designed to provide its information on demand for some purpose; a body of information integral to a computer code, e.g., describing performance capabilities of various intrusion sensors.

Deceit (mode): An action mode wherein the adversary seeks to overcome some element of the security system by misrepresentation or deception, e.g., by wearing a bogus uniform or using counterfeit identification.

Delay: An increase in the time required for completion of some activity. For the security system, this might be the time required to assess an alarm, before initiating full response; for the adversaries it might be the time required to penetrate a barrier.

Detection: Generation of a signal that indicates that an adversary action is in progress or has been completed. (This is usually followed by assessment or response.)

Deterministic (treatment of stochastic elements): A type of mathematical treatment wherein any random elements in a system are not explicitly retained. They may be reflected in values chosen for certain parameters, e.g., mean values for stochastic variables. The results in any defined situation are precisely determined. (The results may be given in the form of a probability statement).

Distribution Function (probability): A mathematical function describing the relative probabilities of various possible values of some quantity, expressed in terms of one or more parameters.

Diversionary Activity: An adversary activity, the main objective of which is to divert the attention of the security system (or its capability to respond) from another, more important adversary action.

Facility: A complex (as a weapon-storage site or a ship loading installation) that is built, installed, or established to serve a particular purpose. In this report (but not all the security system literature), the term includes the various security system hardware components as well as architectural features.

Facility Layout: A plan describing the arrangement of a facility.

Fault Tree Analysis: A technique that identifies those sequences of events that lead to some defined end event. The analysis reveals combinations of basic antecedent events that result in the outcome of interest.

Force (mode): An action mode wherein the adversary employs overt aggressive activities--such as violence, compulsion, constraint, or the proximate threat of these--against people or things, in order to overcome some element of the security system.

Global Assessment: An evaluation (of a security system) that is, in some well-defined sense, comprehensive with respect to the entire range of adversary actions that are judged to threaten the protected facility. For example, a model might estimate the "worst-case" probability of success for a single group of up to 12 men (with defined capabilities) that might attempt to penetrate to a weapon storage space and escape with a weapon, along any path through the facility.

Human Factor Data: Data that describe capabilities and likely responses of human participants in situations of security system interest. These might include target kill probabilities for guard force personnel, as a function of target range, lighting level, target velocity, time available, and weapon type. In the psychological area, the data might include probabilities of adversary surrender, as a function of motivating goals, fraction of comrades killed, perceived ratio of forces, recency of training, etc.

Insider: Someone with legitimate authorization to carry out some activity within the protected facility.

Insider Privilege: An activity or capability authorized to some insider in the interest of legitimate operation of the protected facility, e.g., maintenance personnel access to the interior of a restricted area.

Interacting Networks: A set of mathematical entities which

1) individually, provide a descriptive framework of possible activities for the constituent participants in a simulation and

2) collectively, allow for the synchronization and mutual influence of actual activities in the individual networks.

Interruption: A security system action, e.g., the arrival of a guard and the initiation of a combat engagement, that breaks into an adversary action sequence, leading at least to a delay or shift in adversary action.

Monte Carlo Calculation: The statistical estimation of some quantity by repetitive execution of a series of calculations using an appropriately weighted random sampling of a parameter space.

Neutralization: Defeat of an adversary force by a security system, in a combat engagement or by other means.

Outsider: A person that interacts with a facility without legitimate authorization, i.e., someone other than an insider.

Overt Activity: An activity that is recognized (noted) by the security system.

Path (adversary path): A possible route for an adversary between specified points of interest at a protected facility, e.g., from a point at the perimeter to a target (protected asset) location, from the target to the perimeter, or both combined.

Pathfinding Procedure: A procedure that identifies adversary paths that meet certain criteria, e.g., the path from the facility perimeter to an interior target for which an adversary using stealth would have the highest probability of avoiding detection.

Performance Parameter: A numerical quantity, the value of which describes the level of performance of a person, system, subsystem, piece of equipment, or component in relation to a specified objective or function.

Physical Security (Protection) System: A system, based on physical means, intended to defeat adversary actions at or within protected boundaries through delay, detection, and reaction. Resisted adversary actions include intrusion attempts by outsiders or certain malevolent acts by an insider. In particular, the system is to resist theft or sabotage.

Portal: A passageway through a barrier, e.g., a doorway through a wall.

Postprocessor: A computer code that operates on the data produced in some independent computational process in order to extract or correlate certain data, produce a graphical display or report, etc.

Preprocessor: A computer code that operates on input information in order to transform it into a form required for input to another independent computer program.

Protected Asset: An object (e.g., a nuclear weapon) or a material shielded from theft, sabotage, or both, by a physical protection system.

Reaction: Response of a guard force to a detected intrusion or to an attempt to perform a malevolent act; an action taken to interrupt or delay an adversary action sequence and to reduce the potential consequences.

Response Time: The time required for a guard force to respond to a perceived threat to protected assets. This can include time for assessment of an alarm, for communication between guards, and for travel between different points in the facility. In the case of off-site response forces, it may include time for preparation and transportation.

Scenario-Oriented Model: A model that provides a capability to simulate the events of specific scenarios when provided with [illegible] a specified set of starting conditions and adversary objectives [illegible] detailed specification of the main course of events.

Sensor: A device that responds to a physical stimulus (as sound, pressure, or a particular motion) and transmits a resulting impulse; generally a component of an alarm system.

Single Random Draw: Generation of a value for some quantity, such as a performance parameter or a binary decision variable, by a single random selection carried out in accord with an appropriate probability distribution function.

Stealth (mode): Adversary action directed at overcoming elements of the physical protection system by escaping detection. Such actions may include evasion, covert violent actions, etc..

Subsystem (physical security subsystem): A group of persons or devices (components) forming a unified whole that serve some common purpose as part of the security system, e.g., to detect intrusion through the perimeter fence using various sensors, power supplies, signal lines, signal amplifiers, an audible alarm unit, and a visual display unit.

Tactical Standard Operating Procedure (SOP): A defined procedure for a guard force or a group of adversaries, used in response to some particular stimulus.

Tampering: Covert alteration of some security system component or subsystem so as to weaken it or change it for the worse, e.g., the covert deactivation of an intrusion sensor.

Target: An object or location that must be reached by an adversary to accomplish his malevolent intentions, e.g., a nuclear weapon storage space or a particular weapon there.

Threat: Something that threatens, i.e., a potential adversary group. Alternatively, a description of the groups or activities that threaten a facility.

Timely Detection: Detection of an adversary activity in time to have some chance to prevent its successful conclusion, e.g., the detection of an intrusion in time to permit interception of the adversaries before they reach the target.

Unauthorized Activity: In a protected facility, an action that is not an authorized procedure or that is done by a person that is not authorized to do it, e.g., a procedure that violates the two-man rule.

Validation: As applied to a security system evaluation model, the collection of evidence that the results of the model's calculations are true, probable, or valid indications of the security system's ability to accomplish its objectives.

Virtual Storage: A data processing technique that transfers information between various storage media in a manner that is transparent to the user and that creates the appearance of a much larger central memeory capability than is provided by the actual computer hardware.

APPENDIX B. BOARD GAMES

NRC has developed several board games that reflect situations that might arise in safeguarding SNM at fixed sites or in transit. NRC designed these games to be played by guards as part of the guards' ongoing training in defensive tactics.

We discuss three guard tactics board games in the sections that follow. To our knowledge, they are not widely used in actual guard training. They, or something like them, could be a valuable addition to classroom instruction for guards because they provide experience in making tactical decisions on a realistic time scale.

One unfortunate aspect of guard tactics board games is their potential for use in adversary training. (The authors of NRC's GTS suggest ways to minimize inadvertent training of guards as adversaries in the course of play.) This problem could be avoided by removing the adversary player from the game. This could be done by use of an interactive computerized simulation model, with appropriate pauses for guard decisions. (The interactive version of Sabres II, discussed in section III.2.i. of this review, assigns decisions to the user but does so for *both* sides). The sophistication and popularity of recent video games suggests that imaginative use of microcomputers might produce very useful training tools.

Site-specific board games might be used as rough-and-ready scenario simulators in the field. For reasons discussed in section II. 5.c, simulations that use single random draws (as a board game does) to determine outcomes of their stochastic events are less satisfactory than treatments that use either most probable outcomes or Monte Carlo repetitions. If a rough-and-ready scenario simulation is needed, there are simple simulation methods available that use one of the preferred techniques. (EASI, discussed in section III. 1.a (3), requires only a hand-held calculator for computational support.) They may be easier to use as field simulators than board games, and they are likely to be more satisfactory.

1. GUARD TACTICS SIMULATION (GTS) (U.S. NUCLEAR REGULATORY COMMISSION)

NRC developed the GTS board game to provide a means of examining tactical procedures for use in defense of nucleaı fuel cycle facilities. GTS's exploration of tactics is site-specific, using boards derived from facility blueprints and realistic local police response times. The GTS guard force attempts to prevent the adversaries from removing SNM before local police arrive. The guards and guard commanders who play (or watch) GTS can "test" a wide range of response tactics, receiving immediate (though crude) feedback about the consequencies of their tactical choices.

Two players, a "guard commander" and an "adversary commander" contend in GTS. A third person acts as an active referee. (He communicates information, determines the outcome of partially random events, judges the feasibility of players' proposed moves, and ensures compliance with GTS's rules.) Each player has his own copy of the board, on which he places and moves markers that indicate where members of his force (and located members of the opponent force) are, and which way the members of his force are looking.

A GTS game generally begins with a toss of a coin by the referee to determine which player will take which role (guards or adversaries). The designated adversary player then takes ten to fifteen minutes to plan his assault and to describe his plan to the referee. (The guard player is absent during the planning period.) When the guard player returns he is given a few minutes to place his pieces to reflect actual guard placement under the conditions (time, day of week, season, weather) chosen by the adversary player for the attack. Each player completes a check-list assigning specific equipment or capabilities to specific members of his force. Depending on what surveillance activities the adversary player specified in this plan, the referree may reveal the positions of some of the guard pieces to him.

When actual play begins, GTS adversaries are concealed from the guard force. (Some guard positions may also be unknown to the adversaries.) Each player in turn (starting with the adversary player) has twenty seconds to move as many of his pieces as he chooses (to reflect a ten second period of activity). The adversary player must specify to the referee the nature of his pieces' activities. Should the referee judge that a particular activity would attract guard attention, he communicates to the guard player (at the guard player's next turn) the location and character of the signal guards would receive. If necessary, the guard player can act to confirm that an attack is in progress. When he has such confirmation, the guard player "summons" the local police, setting an undisclosed (to the adversary player) time limit for further activities.

After the guard player becomes aware of the attack, GTS adversaries continue to move, to look for guards, and to penetrate barriers in their attempt to steal SNM. GTS guards respond as the guard player decides (based on his knowledge of the attack). From time to time, GTS inserts random events unplanned by either side. If guards and adversaries confront one another, GTS determines the outcome of the resulting combat engagement using a set of rules involving one or more random draws and a set of decision tables.

A GTS game ends when adversaries have removed SNM from the facility (in which case the adversary player wins) or when local police arrive before the adversaries have removed SNM (in which case the guard player wins). NRC suggests a post-game review of critical events, in which both players can see and discuss each others' activities and decisions.

NRC has developed two sets of optional auxiliary aids to facilitate GTS play. One, an "audio enhancement," allows private communication between the referee and each of the players via microphones and headsets. (Without the enhancement, such communications involve cue cards and written messages, which are more awkward and less flexible.) The second aid is a hand-held calculator program that provides automated random draws, table look-ups, and timing assistance. Both aids help create a more realistic playing atmosphere. They also relieve the referee of some distracting routine tasks that would otherwise contribute to an already formidible set of demands on his capabilities.

In order to minimize training of guards as potential adversaries, NRC suggests that players should be designated as guards or adversaries at the last possible movement, that games in which the adversaries have insider assistance should be relatively infrequent, and that adversary player planning time should be strictly limited (to just enough to allow construction of a realistic challenage to the guard player). GTS's rules instruct the referee not to "correct" overambitious adversary plans at the outset of play.

If qualified referees are available (we suspect that they are difficult to find), GTS can provide valuable guard training. A guard commander might increase his tactical insight by observing GTS games. We do not recommend GTS as a simulation tool for other purposes.

BIBLIOGRAPHY

Drimer, J. and Oh, C. B., Guard Tactics Simulation, U.S. Nuclear Regulatory Commission (Draft).

South, C., Referee Support Program for the GTS, U.S. Nuclear Regulatory Commission, February 1979 (Draft).

Anonymous, Audio Enhancement Option for the GTS, U.S. Nuclear Regulatory Commission (Draft).

2. NUCLEAR WEAPONS STORAGE SITE BOARD GAME (NWSSBG) (BOOZ-ALLEN AND HAMILTON FOR DNA)

Booz-Allen is developing a version of NRC's GTS board game for use at DoD nuclear weapon storage sites. The game will use boards that represent actual storage sites, generally the ones at which the games are to be used. (Some smaller sites may use generic boards, to avoid the expense and delay associated with producing customized boards.) The DNA game package will include both the audio enhancement and the referee-assistance calculator.

Booz-Allen plans to modify GTS's rules to make them appropriate to the storage site security situation. The changes required are not extensive.

3. SKIRMISH/AMBUSH (SANDIA NATIONAL LABORATORIES)

The SKIRMISH and AMBUSH board games simulate an attempt to steal SNM from a truck convoy. Sandia/Livermore developed them as part of an NRC program concerned with physical protection of nuclear materials in transit, to help players develop insight into factors (especially tactical factors) that contribute to physical security system success.

SKIRMISH is a relatively simple game, intended for guard force training and for use as an introduction to AMBUSH. SKIRMISH is fully developed; Sandia has published complete instructions for its fabrication and use. Sandia has prepared only a preliminary version of AMBUSH, which is more complex and more ambitious. Draft rules for AMBUSH are available in Sandia's central technical files.

SKIRMISH treats the same phase of an attack on a convoy as Sandia/Livermore's computer simulation SABRES II (described in Section III.2.i of this review). Before play begins, at a point chosen by the "adversary player, the adversaries stop the nuclear material transporter (which transmits an alarm to its escort vehicles). The adversaries attempt to reach the transporter and to breach a barrier at the transporter to reach the SNM. In the standard SKIRMISH game, six adversaries--armed with pistols and either assault rifles or shotguns--attack a convoy consisting of the transporter and two escort vehicles (one preceeding and one following the transporter). Each vehicle is manned by at least two guards. At the outset of play, the "defender" player assigns a convoy commander (a third guard) to one of the three vehicles. The guards have the same kinds of weapons as the adversaries. The convoy travels on one of two roads (which pass through different terrain) on the SKIRMISH game board. The defender player chooses his route and direction of travel at the outset of play.

Each SKIRMISH "move" represents one minute of activity. (Generally, no time limit is imposed on the players, which seems unrealistic.) A game lasts up to twenty moves. Each move has four phases: planning, combat, movement and "maintenance". During each move, each of the simulated participants can carry out a combination of activities. These activities are limited by a clever system of "activity points" that reflect constraints imposed by time and attention. In each phase of each move, activities of all simulated participants proceed simultaneously.

In the planning phase, the players make and record activity plans for each of their simulated participants. At the end of the phase, the players reveal their written plans.

In the combat phase, SKIRMISH players determine results of planned firing activities. A simulated participant can fire if he has a clear line of sight to the opponent his activity plan calls for him to fire upon. The outcome of the firing event depends upon the attacker's weapon, the range to the target, the defender's rate of movement and cover status, and a throw of a die. The opponent can be missed, killed, or wounded. (A wounded participant moves slower, is less effective in combat, and cannot drive a vehicle or penetrate a barrier.)

In the movement phase, a SKIRMISH simulated participant moves at a rate determined by the nature of the terrain he is crossing, his status (healthy or wounded), and his mode of transportation (foot or--on a road--a vehicle). The total distance he travels during a move is limited by the fraction of his activity his plan calls for him to devote to movement.

In the "maintenance" phase, the SKIRMISH players carry out all the remaining activities of the move and record the results. Barrier work, which requires all of a simulated partic-icipant's activity points for a turn, takes place during this phase. The adversary player acquires work points depending on the number of effective simulated participants assigned to barrier penetration during the turn. (Some healthy participants may be suppressed by incoming fire and earn no work points.) The adversary player "wins" by acquiring enough work points before time runs out (or all his simulated participants are incapacitated). During the "maintanence" phase, simulated participants can also prepare themselves for combat during subsequent moves.

AMBUSH differs from SKIRMISH in providing more playing situations, and in encouraging the players to invent their own situations. AMBUSH provides more terrain maps, more possible weapon types, and more simulated cargo barriers. AMBUSH simulates communication between convoy members, and allows for arrival of response forces summoned with the communication system.

SKIRMISH (or AMBUSH, if its development were completed) could be a valuable training tool. Thc fact that no highly skilled referee is required is a desirable feature.

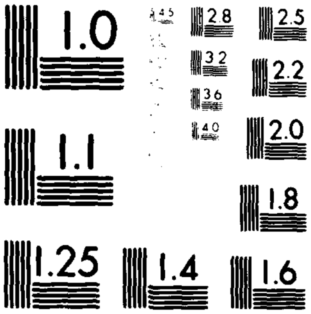
BIBLIOGRAPHY

Gallagher, R. J., and Keeton, S. C., SKIRMISH and AMBUSH--Tactical Board Games for Development and Evaluation of Road Transit Physical Protection Systems, NUREG/CR-1255, SAND79-8058, Sandia National Laboratories, March 1980.

AD-A109 726   R AND D ASSOCIATES ARLINGTON VA   F/G 15/3
CURRENT METHODS FOR EVALUATION OF PHYSICAL SECURITY SYSTEM EFFE--ETC(U)
MAY 81 R B DAVIDSON, J W ROSENGREN   DNA001-81-C-0109
UNCLASSIFIED RDA-TR-179200-001   DNA-TR-81-18   NL

3 OF 3
AD
A109 726

END
DATE
FILMED
2-82
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

DISTRIBUTION LIST

DEPARTMENT OF DEFENSE

Assistant to the Secretary of Defense
Atomic Energy
3 cy ATTN: Colonel Chesher

Defense Industrial Scty Institute
ATTN: Facilities Protection Dept

Defense Logistics Agency
ATTN: Major Gilmore

Defense Nuclear Agency
2 cy ATTN: STNA
2 cy ATTN: OAPS
4 cy ATTN: TITL
20 cy ATTN: PSNS

Defense Technical Information Center
12 cy ATTN: DD

Deputy Under Secretary of Defense Policy Review
5 cy ATTN: LTC Creeden

Field Command
Defense Nuclear Agency
3 cy ATTN: FCPRT

Joint Chiefs of Staff
2 cy ATTN: J-5, Plans & Policy/Nuclear Div

U.S. European Command
5 cy ATTN: ECJ4/7-LW

Under Secretary of Defense for Rsch & Engrg
10 cy ATTN: Chairman, Phy Sec Equip Action Grp,
C. Kuhla

DEPARTMENT OF THE ARMY

Deputy Chief of Staff for Ops & Plans
Department of the Army
5 cy ATTN: DAMO-NC

Department of the Army
2 cy ATTN: DAMA-CSC-ST

Deputy Chief of Staff for Personnel
Department of the Army
5 cy ATTN: DAPE-HRE

Headquarters, 59th Ordnance Brigade (SASCOM)
Department of the Army
2 cy ATTN: AEUSA-Z

Office of the Chief of Engineer
Department of the Army
2 cy ATTN: DAEN-MCD-D, Mr. Reynolds

Seneca Army Depot
2 cy ATTN: Provost Marshal
2 cy ATTN: Surety, Mrs. Jones

Sierra Army Depot
1 cy ATTN: Security Operations

DEPARTMENT OF THE ARMY (Continued)

Southern European Task Force
Department of the Army
ATTN: AESE-GCT-S

U.S. Army Armament Rsch Dev & Cmd
5 cy ATTN: DRDAR-LCN-F

U.S. Army Electronic Warfare Lab
ATTN: DELEW-I-S (Security Systems)

U.S. Army Engineer Div, Huntsville
ATTN: HNDED-SR, L. Ziegler

Commander-in-Chief
U.S. Army, Europe and Seventh Army
2 cy ATTN: AEAGC-NC
2 cy ATTN: AEAGD-MM-SW
2 cy ATTN: AEAPM-PS

U.S. Army Human Engineering Lab
5 cy ATTN: D. Egner

U.S. Army Intelligence Agency
ATTN: DELEW-I

U.S. Army J F Kennedy Center (MA)
5 cy ATTN: AFJK-GC
5 cy ATTN: G-3 (Special Projects)

U.S. Army Mat Cmd Proj Mngr for Nuc Munitions
2 cy ATTN: DRCPM-NVC

U.S. Army Materiel Dev & Readiness Cmd
2 cy ATTN: DRCSS
2 cy ATTN: DRCNC

U.S. Army Military Personnel Ctr
5 cy ATTN: ATZN-TD
5 cy ATTN: DALET (Phys & Scty Committee)
5 cy ATTN: ATZN-CD

U.S. Army Military Police School
5 cy ATTN: ATZN-MP-TD
5 cy ATTN: Phys Scty Committee
5 cy ATTN: ATZN-MP-CD
5 cy ATTN: ATZN-MP-TRC
5 cy ATTN: ATZN-MP-Library

U.S. Army Mobility Equip R&D Cmd
ATTN: DRDME-ZK
ATTN: DRDME-X1
ATTN: DRDME-X
ATTN: DRDME-ZPS
ATTN: DRDME-N
ATTN: DRDME-ES

U.S. Army Night Vision Laboratory
ATTN: DELNV-SI, Mr. Doepe

U.S. Army Nuclear & Chemical Agency
2 cy ATTN: MONA-SU

DEPARTMENT OF THE ARMY (Continued)

U.S. Army Training and Doctrine Comd
5 cy ATTN: ATCD

USAINSCOM Pentagon Counterintelligence Force
ATTN: Special Agent, T. Forman

DEPARTMENT OF THE NAVY

Naval Civil Engineering Laboratory
ATTN: Code L51
ATTN: L44
ATTN: L61
ATTN: L64

Naval Electronic Sys Engineering Center
ATTN: Code 04
ATTN: Code 404HS

Naval Electronic Systems Command
ATTN: PME-121-3, D. Morrison

Naval Facilities Engineering Command
ATTN: Code 032E

Naval Material Command
ATTN: MAT 0462, Mr. Bukolt, CPP

Naval Personnel Res & Dev Center
ATTN: Code P302

Naval Security Group Command
ATTN: G123, Phy Security Branch

Naval Surface Weapons Center
ATTN: J. Haben

Naval Weapons Support Center
ATTN: R. Henry

Office of Naval Research
ATTN: Code 452

Office of the Chief of Naval Operations
ATTN: OP 403
ATTN: OP 009D3

DEPARTMENT OF THE AIR FORCE

Air Force Office of Security Police
2 cy ATTN: SPOS-SPPC
3 cy ATTN: AFOSP/SPPC
5 cy ATTN: SPPX

Air Force Office of Special Investigations
ATTN: IVTS

Air Force Weapons Laboratory
Air Force Systems Command
ATTN: Lt Col Kries

Electronic Systems Division
Department of the Air Force
5 cy ATTN: Physical Security Sys Directorate

Interservice Nuclear Weapons School
Department of the Air Force
2 cy ATTN: 3416TTSQ/TTV

DEPARTMENT OF THE AIR FORCE (Continued)

Nuclear Surety
Department of the Air Force
ATTN: XXXXX

Deputy Chief of Staff
Research and Development
Department of the Air Force
2 cy ATTN: RDPE

U.S. Air Force
ATTN: IGS

Commander-in-Chief
U.S. Air Forces in Europe
2 cy ATTN: USAFE/SP

OTHER GOVERNMENT AGENCIES

Central Intelligence Agency
ATTN: Security Committee, W. Johnson

Department of Commerce
National Bureau of Standards
2 cy ATTN: R. T. Moore

U.S. Department of State
Office of Security
ATTN: Chief, Res & Dev Branch A/SY/OPS/T
ATTN: Chief, Div of Tech Services A/SY/OPS/T

U.S. Nuclear Regulatory Commission
ATTN: R. Whipp for M/S 881-SS, R. Erickson
ATTN: R. Whipp for M/S EW-359, J. James
ATTN: R. Whipp for M/S 1130SS, E. Richard
ATTN: R. Whipp for M/S EW-359, L. Bush

DEPARTMENT OF ENERGY CONTRACTOR

Sandia National Lab
5 cy ATTN: Div 1736

DEPARTMENT OF DEFENSE CONTRACTORS

Abbott Associates, Inc
ATTN: P. Abbott

Kaman Tempo
ATTN: DASIAC

Mission Research Corp
10 cy ATTN: D. Solomonson

Pacific-Sierra Research Corp
ATTN: H. Brode

R & D Associates
ATTN: P. Haas

R & D Associates
4 cy ATTN: R. Davidson
4 cy ATTN: J. Rosengren