A NETWORK MODELING AND ANALYSIS TECHNIQUE FOR THE EVALUATION OF NUCLEAR SAFEGUARDS SYSTEMS EFFECTIVENESS

Floyd H. Grant, III
Robin J. Miner
Dennis Engi

ABSTRACT

Nuclear safeguards systems are concerned with the physical protection and control of nuclear materials. The Safeguards Network Analysis Procedure (SNAP) provides a convenient and standard analysis methodology for the evaluation of safeguards system effectiveness. This is achieved through a standard set of symbols which characterize the various elements of safeguards systems and an analysis program to execute simulation models built using the SNAP symbology. The reports provided by the SNAP simulation program enable analysts to evaluate existing sites as well as alternative design possibilities. This paper describes the SNAP modeling technique and provides an example illustrating its use.

INTRODUCTION

Safeguards systems are concerned with the protection and control of nuclear materials. The existence of these safeguards systems is motivated by the possibility of loss of nuclear material due to unreliable equipment and procedures, or due to sabotage and theft. This research is concerned with those systems which are designed to protect nuclear material at a fixed site. The primary objective is to provide a means of evaluating the resistance of the system to sabotage or theft. Examples of safeguards systems include nuclear reactor sites, spent fuel storage sites, and fuel fabrication facilities.

The Safeguards Networks Analysis Procedure (SNAP) developed through this research fulfills this objective. SNAP employs the network modeling approach to problem solving. By combining the SNAP symbology with knowledge of the system, specific scenarios, and modeling objectives, a network model of the system may be developed. Standardized procedures have been defined for describing the model in a data form acceptable to a computer program. The SNAP analysis program is used to simulate the system of interest. Reports are generated by the program to provide information which allows the analyst to evaluate the performance of proposed or existing safeguards systems.

Models of fixed-site, nuclear facility, physical protection systems were under development as early as 1974. The need for such models is essentially two-fold: they offer a consistent approach to the objective evaluation of the effectiveness of a physical protection system in defending against some hypothesized adversary, and they provide a quantitative technique for upgrading extant facilities and designing new facilities.

Experience gained from the early modeling attempts provided the impetus for the development of SNAP. Methodological completeness was a primary issue in the conceptualization of SNAP. This completeness has been argued for and interpreted in two quite distinct ways--producing the dichotomy macro vs. micro-completeness. A safeguards methodology can be termed macro-complete if it can feasibly be used to evaluate effectiveness for all reasonable adversary scenarios. Alternatively, a micro-complete methodology is one in which safeguards effectiveness is evaluated for each individual scenario in sufficient detail to adequately represent all relevant considerations. In SNAP the intent is to treat both micro and macro completeness with the same level of emphasis.

In satisfying the implied Janus-faced completeness constraint, SNAP is conceptually appealing to the safeguards evaluator who has no previous experience with the use of models as well as to the professional modeler. This appeal is a result of the standard set of "safeguards symbols" which SNAP employs to characterize the various elements of the safeguards systems. These symbols enable the analyst to represent complex scenarios with a modest amount of effort. Once constructed, these symbolic representations translate directly into data for the SNAP computer program which, in turn, yields estimates for a variety of safeguards effectiveness measures.

MODELING PHILOSOPHY

The modeling philosophy of SNAP may be defined on two levels. On the general level, SNAP employs the network modeling approach to problem solving. On the specific level, SNAP provides a structure for safeguards systems analysis by dividing safeguards systems into three interacting submodels. These two levels of approach will be discussed in detail.

In using the network modeling approach to problem solving, a network symbology, system knowledge, specific scenarios, and modeling objectives are combined to form a network model of the system. Data describing the model and the SNAP Analysis Program are used in conjunction with a computer to produce reports that provide information to evaluate the performance of the safeguards system. One of the basic advantages of network simulation is that it frees the analyst from the programming task. Network modeling provides analysts with a communication and documentation vehicle as well.

In developing models of various safeguards systems, certain submodel elements are common to every situation. These various submodels interact with each other to produce the overall behavior of the system. This interaction is illustrated in Figure 1.

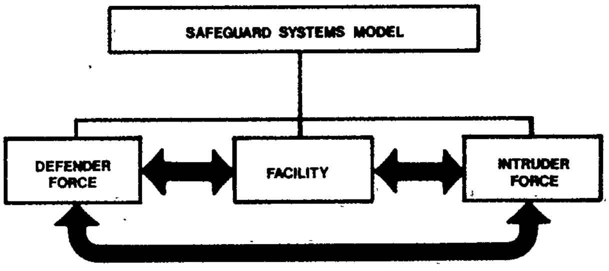


Figure 1. Safeguard Systems Model

The most fundamental submodel is concerned with the physical characteristics of the facility itself. In SNAP, this model is a static model, i.e., transactions do not flow through it. The facility model defines various components of the safeguards facility and their relationships.

A second submodel involves guard operating policies. The guard submodel includes a representation of the decision logic associated with guard forces as well as the physical movement of guards through the facility. Guards may make decisions based on system status information as they progress through the network.

A similar model of the adversary process is included. The decision logic and sequence of events which an adversary must complete to reach a certain target are represented in this submodel. Adversary forces also make decisions based on system status information.

The three submodels of the system have numerous points of interaction. The guard submodel interacts with the facility model through sensor detection, actual movement through the facility, etc. The adversary submodel interacts with the facility in a similar manner.

Interaction is also necessary between the guard submodel and the adversary submodel. This is accomplished in two ways. First, each group has some knowledge about the capabilities of the opposing force. This is accomplished by maintaining a set of attributes which define one group's knowledge of the other. As in the real system, the attributes contain information obtained only at the time of detection and it may or may not be current. These attributes are updated as guards and adversaries flow through their respective submodels. Decisions may be made based upon these attributes.

The second level of interaction between the two forces is the engagement. The model of the engagement is probabilistic in nature and is based on the characteristics of the forces involved. Future force movements and decisions may be made depending upon whether a force wins or loses the engagement. This engagement model is a Monte-Carlo version of BATLE (Brief Adversary Threat Loss Estimator), an analytic model developed at Sandia Laboratories (8).

In summary, SNAP provides analysts with a network modeling approach for the simulation and analysis of safeguards systems. Safeguards models are built by defining three subsystem models representing the facility, the guard force, and the adversary force. Guard and adversary forces interact with the facility model through their movement within that facility. They interact with each other through sensor detections and engagements. The next section will discuss the elements of the SNAP symbology.

SNAP SYMBOLOGY

The SNAP symbology is designed to form a one-to-one correspondence with the actual physical components and guard or adversary actions. That is, there is a set of symbols for modeling the facility of interest and for developing models of the adversary and guard force scenarios as they relate to that facility.

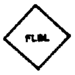
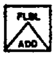
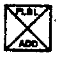
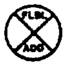
The procedure for modeling safeguards systems using the SNAP symbology is as follows:

> The analyst first builds the model for the facility that he wishes to study using the facility model symbology. Then, using the guard and adversary model symbologies, he constructs various scenarios. These scenarios, with the facility model, are simulated and information is generated to provide relative measures of system performance. Through this procedure, the analyst may evaluate various defender policies and facility design alternatives.

The SNAP symbology for the facility model is shown in Table 1. The PORTAL, SPACE, BARRIER, and TARGET elements identify actual facility system components. Adjacency and Precedence branches define their inter-relationships. Adversary Detection Devices (ADD) include sensors and monitors. The user identifies SNAP elements by alphanumeric labels. For example, the user specifies that a sensor label is associated with a certain node by entering the label for that sensor in the appropriate portion of the node (indicated by ADD in Table 1).

Based on the model of the facility of interest, the user then builds models of the guard and adversary scenarios to be considered. These models are built using the guard and adversary symbology shown in Table 2. Each of these elements will relate directly to a particular activity of the force being modeled. For example, the process of an adversary crossing a fence is modeled using a TASK node. This node is tied directly to the facility model node which represents the fence by its alphanumeric label, as indicated by FLBL on the TASK node. Similar procedures hold for the other nodes.

Table 1. Facility Model Symbology

PORTAL		System Entrance Point
SPACE		Space in Facility
BARRIER		Barrier in Facility
TARGET		Adversary Objective
ADD	data card	Adversary Detection Devices
Adjacency	———	
and		
Precedence	——→	

A unique data card has been defined for each element in the three models. Information specified on the user's network is transferred directly to these data cards, which are processed by the analysis program. The simulation of the model is then executed by running the SNAP analysis program and output reports are automatically generated.

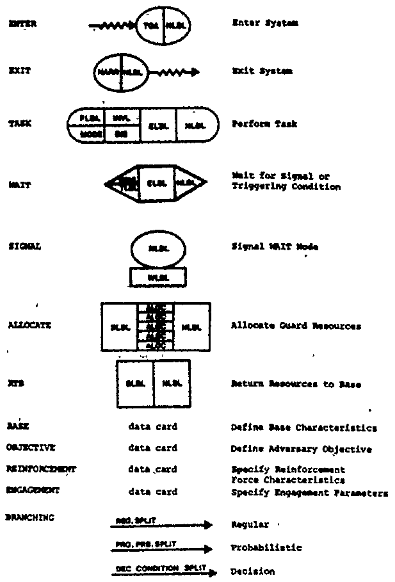
In order to illustrate the use of the symbology and indicate the analysis information available, the following example application is provided.

SNAP APPLICATION

This application illustrates the use of SNAP concepts and symbols to model systems

Safeguards Network Modeling (continued)

Table 2. Guard and Adversary Model Symbology


TOA
MLBL
PLBL
MODE
SLBL
ALOC

ENTER		Enter System
EXIT		Exit System
TASK		Perform Task
WAIT		Wait for Signal or Triggering Condition
SIGNAL		Signal WAIT Mode
ALLOCATE		Allocate Guard Resources
RTB		Return Resources to Base
BASE	data card	Define Base Characteristics
OBJECTIVE	data card	Define Adversary Objective
REINFORCEMENT	data card	Specify Reinforcement Force Characteristics
ENGAGEMENT	data card	Specify Engagement Parameters
BRANCHING	REG.SPLIT	Regular
	PRO.PRB.SPLIT	Probabilistic
	DEC CONDITION SPLIT	Decision

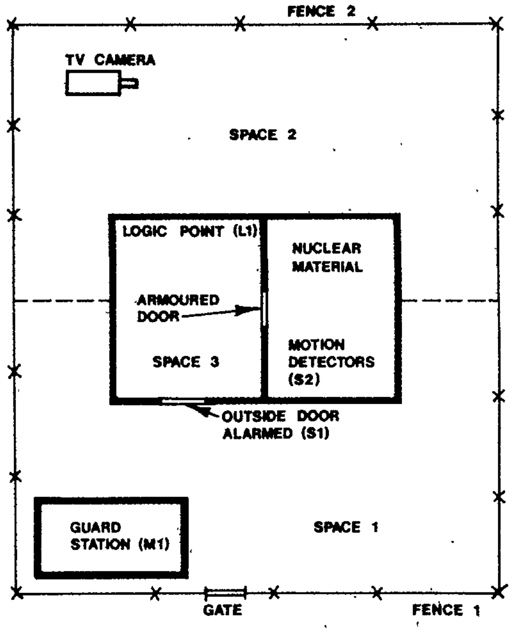


Figure 2. Exemplary Facility Schematic

concerned with protecting nuclear material from sabotage or theft.

A diagram of the exemplary nuclear storage facility to be used for this application is shown in Figure 2. A fence surrounds the storage building on all sides. For modeling purposes, the fence has been divided into two parts, fence 1 and fence 2. The space surrounding the storage building has also been divided into two parts, space 1 and space 2. There is a TV camera in space 2 monitoring that space. The TV camera functions as a sensor and will be referenced as sensor S3. A guard station which monitors all sensors on the site is located in space 1. The outside door is alarmed and may be entered from space 1. Space 3 contains the logic point L1 through which the signals from sensors S1, S2, and S3 must pass before reaching the monitor (M1) at the guard station. Disablement of logic point L1 would interrupt the flow of information from those sensors to the guard station monitor. An armoured door separates space 3 and the target, the nuclear material. The nuclear material is monitored by sensor S2, a motion detector.

Figure 3 presents the corresponding SNAP facility subnetwork. This figure has been labeled so as to make a correspondence between the storage site schematic and the model readily apparent. Note that there are two possible entrances by adversaries denoted by portal nodes E1 and E2. These are connected to two barrier nodes which represent fence 1 and fence 2. Paths that the adversary might take are easily determined for this model. Since

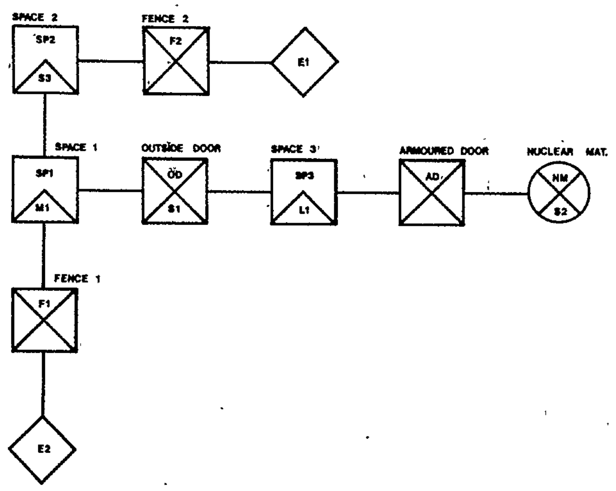


Figure 3. SNAP Model of the Exemplary Facility

adversary and guard forces may travel in either direction between the various facility components, only adjacency is indicated on the branches between the nodes in this model.

After the facility model is developed, the adversary and guard subnetworks are built in reference to that facility model.

The guard force subnetwork is shown in Figure 4. The guard force transaction enters (ENT) the guard subnetwork at time 0.0 and begins monitoring the three sensors (W1, W2, and W3).

Sensor S1 is the sensor on the alarmed outside door. If sensor S1 is triggered the guard force takes two minutes to muster forces (DA1). A force of two members is allocated (A1) from base B1. The guard force then moves (MS11) into space 1 to assess the situation. If no adversaries are detected during the time the guards are on patrol, the guard force returns to base (RTB1) and resumes the monitoring of sensor S1. If adversaries are encountered, an engagement will ensue.

Sensor S2 represents the motion detector in the material access area. If sensor S2 is triggered, the guard force takes two minutes to muster forces (DA2). A force consisting of two members is then allocated (A2) from base B1. This force is the same force that is allocated if sensor S1 is triggered. The guard force then moves (MS12) into space 1 to search for adversaries. If adversaries are encountered an engagement will ensue. If no adversaries are found, the guard force will wait (W4) at space 1 for an adversary force to arrive. If adversaries do arrive, an engagement will ensue. If the guards win, they return to base (RTB2) and begin monitoring sensors again.

Sensor S3 is the TV camera. If sensor S3 detects adversaries in space 2, the guard force musters (DA3) and allocates (A3) two guards from base B1. The force then enters space 1 (MS13) to search for adversaries. If none are found, the guard force moves into space 2 (MS12) continuing the search. After space 2 has been searched and if no adversaries have been found, the guards return to space 1 (MS14) to search again. If the guard force encounters an adversary force at any time during the searching of space 1 or space 2, an engagement will occur. If the guards win the engagement, they continue their search procedures to locate any other adversaries which may be present. After searching for adversaries in space 1 and space 2, the guards wait (W5) in space 1 for further instructions. If the guards encounter an adversary while they are waiting, an engagement will begin. If the guards win the engagement, they return to base (RTB3) and begin monitoring sensors again.

This summarizes the operating policies which the guards will follow in this model. This guard model is typical of guard responses to adversary intrusion for the hypothetical facility under consideration.

The adversary force subnetwork is shown in Figure 5. Their objective is to achieve a radiological release through sabotage of the nuclear material in space NM by using an explosive device. The adversaries enter (ENT1) at time 0.0 and immediately penetrates (CF1) fence 1. Next, they cross space 1 (CSP1) and divide their force in half. Half of the force moves into space 2 (CSP2) as a diversion. They wait in space 2 until the other half of their force joins them. The other half begins penetration of the alarmed outside door. Fifty percent of the time they will disable sensor S1 and not be detected (DOD or DODN). After penetrating the outside doors, this adversary force crosses space 3 (CSP3), and penetrates the armoured door (DAD). They then sabotage the nuclear material (SMN) by leaving an explosive device and retrace their steps through the armoured door (EAD), across space 3 (ESP3) and through the outside door (EOD), and into space 1 (ESP1). They cross space 1 and move into space 2 (ESP2) where they join with the other adversary force (WS2A). When both adversary forces are in space 2

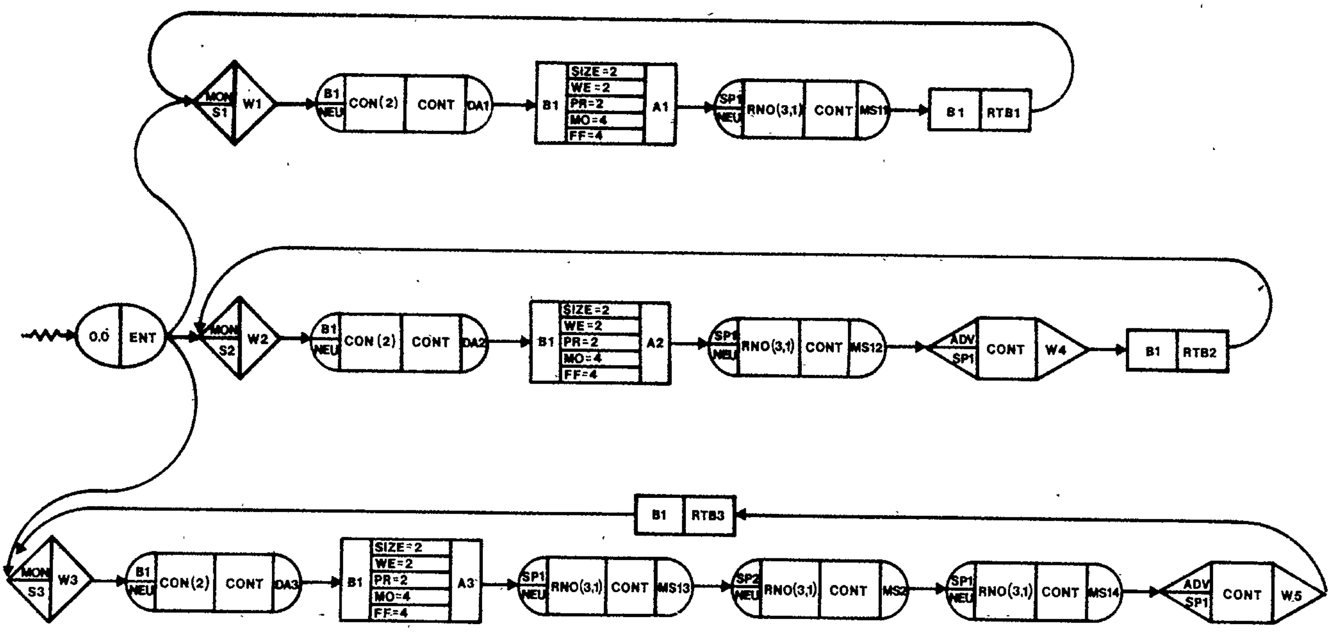


Figure 4. Guard Force Scenario Network

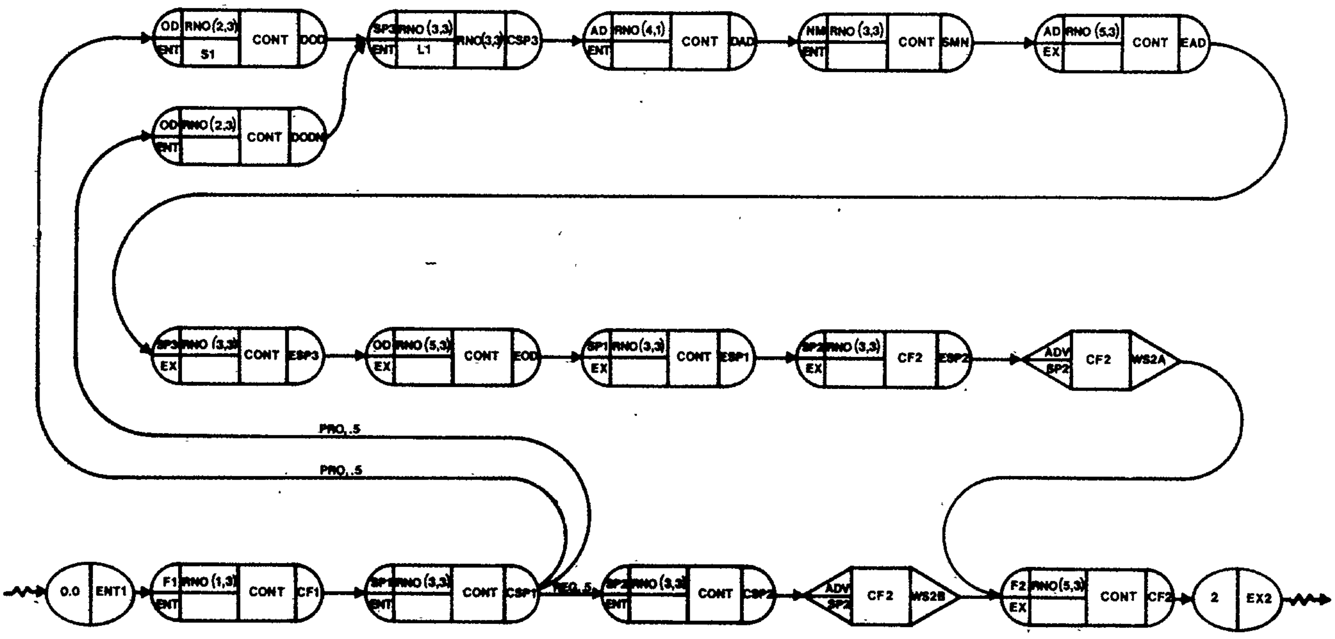


Figure 5. Adversary Force Scenario Network

they join and penetrate fence 2 (CF2), exiting the facility (EX2). Since the adversary objective is sabotage they do not have to exit the network to be successful.

Figure 6 shows a portion of the trace generated from a simulation run of this model. The guard force enters and begins monitoring the sensors. From this trace, an event-by-event account of one realization of the network can be obtained. The information on this trace relates directly to the networks defined by the user.

This model was simulated 500 times to generate statistics. The results of these simulations are shown in Table 3. From these results, the user can obtain information concerning the behavior of the existing system. The overall performance measure, the probability the adversary achieves his objective, was observed to be 0.13. That is, in this example, the adversary can sabotage the nuclear material 13% of the time. This would most likely be viewed as an unacceptable level of performance and indicate that revisions to the facility or guard operating policies are warranted. More specific performance measures are available as indicated.

CONCLUSION

The major objective in the development of SNAP was to build a network simulation technique specifically tailored for the modeling and analysis of safeguards systems. Using the SNAP symbology, models of safeguards systems are built in three interactive submodels. Through the application of data input procedures, the SNAP analysis program simulates the network model developed and provides summary reports concerning the behavior of the system. Thus, SNAP provides analysts with a tool for evaluating alternate safeguards systems designs and refining safeguards procedures at existing sites.

ACKNOWLEDGMENTS

This study was sponsored by the U.S. Nuclear Regulatory Commission; Office of Regulatory Research; Division of Safeguards, Fuel Cycle, and Environmental Research.

REFERENCES

1. R.E. Bach, Jr., L. Dolansky, and H.L. Stubbs, "Some Recent Contributions to the Lanchester Theory of Combat," Opns. Res., 10, 314-326, 1962.

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

3. H. Brackney, "The Dynamics of Military Combat," Opns. Res., 7, 30-44, 1959.

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

5. S.J. Deitchman, "A Lanchester Model of Guerrilla Warfare," Opns. Res., 10, 818-827, 1962.

6. J.H. Engel, "A Verification of Lanchester's Law," Opns. Res., 2, 163-171, 1954.

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

8. D. Engi and J.S. Shanken, Brief Adversary Threat Loss Estimator (BATLE) User's Guide, SAND78-1136, Sandia Laboratories, Albuquerque, New Mexico, November 1978.

9. F.H. Grant and R.J. Miner, Safeguards Network Analysis Procedure, Final Report, Pritsker & Associates, Inc., West Lafayette, Indiana, May 1978.

10. F.W. Lanchester, Aircraft in Warfare: The Dawn of the Fourth Arm, London England Constable, 1916.

11. P.M. Morse and G.E. Kimball, Methods of Operations Research. New York: John Wiley and Sons, 1951.

12. A.A.B. Pritsker, The GASP IV Simulation Language. New York: John Wiley and Sons, 1974.

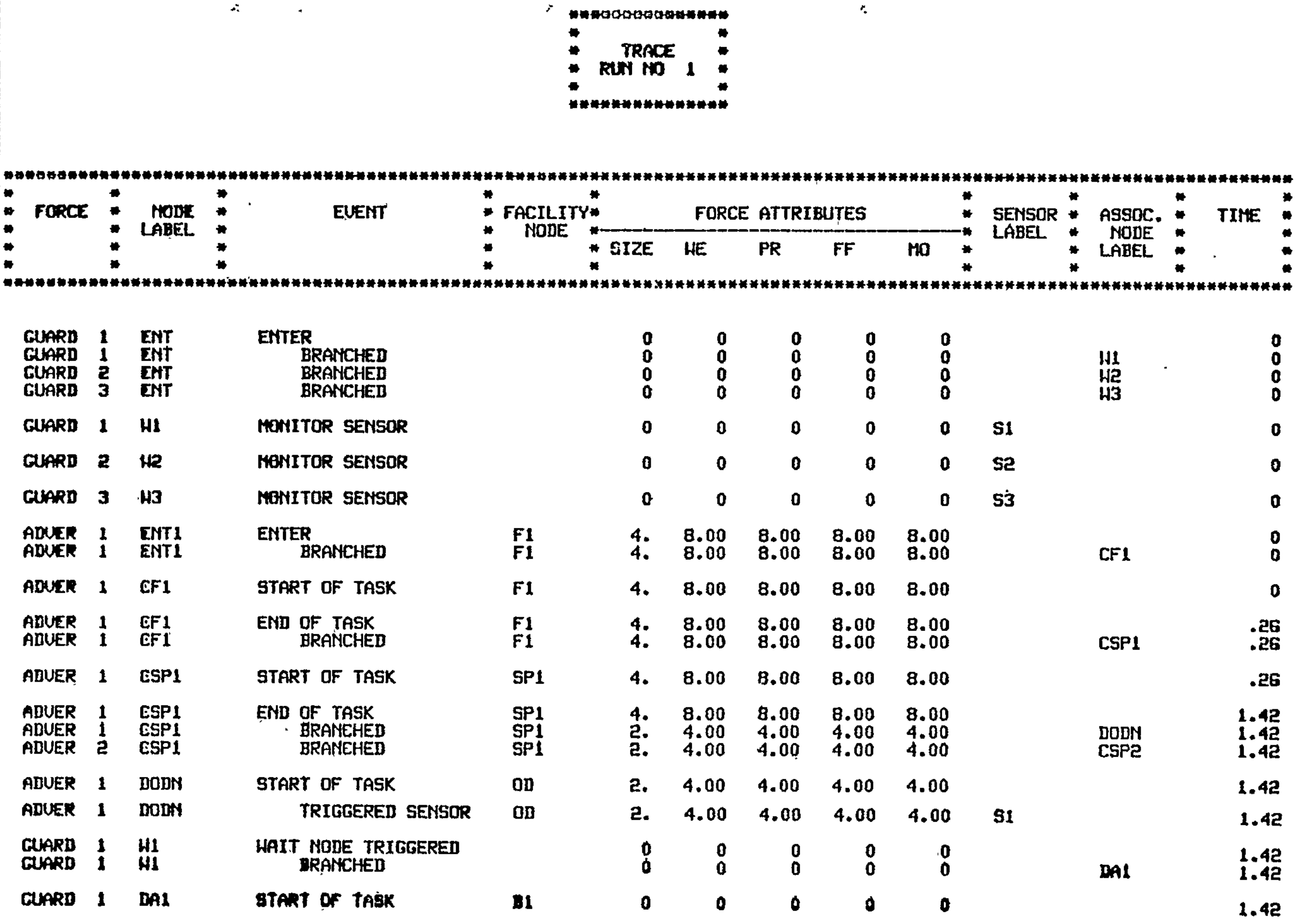
13. M.M. Schaffer, "Lanchester Models of Guerrilla Engagements," Opns. Res., 457-488, 1968.

14. H.K. Weiss, "Lanchester-Type Models of Warfare," Proc. First International Conf. on Operational Res., Oxford, September 1977.

Safeguards Network Modeling (continued)

Table 3. Performance Measures

Average Number of Engagements Per Run	1.97
Average Number of Engagements Won by Guards Per Run	1.42
Average Number of Engagements Won by Adversaries Per Run	0.55
Probability Adversary Achieves Objective	0.13
Number of Guard Casualties Per Run	2.42
Number of Adversary Casualties Per Run	3.00
Time for Engagement	5.51 min.
Total Engagement Time Per Run	10.87 min.
Number of Engagements Per Run	1.97
Time Between Adversary Entrance and First Engagement	3.29 min.
Scenario Simulation Time	16.21 min.
Scenario Simulation Time Given Adversary Succeeds	39.43 min.
Scenario Simulation Time Given Adversary Fails	12.58 min.



```
                                                  **************
                                                  *            *
                                                  *   TRACE    *
                                                  *  RUN NO  1 *
                                                  *            *
                                                  **************

**********************************************************************************************************
*         *         *                            * FACILITY*                                     *          *          *          *
*  FORCE  *  NODE   *           EVENT            *  NODE   *            FORCE ATTRIBUTES         *  SENSOR  *  ASSOC.  *   TIME   *
*         *  LABEL  *                            *         *-------------------------------------*  LABEL   *   NODE   *          *
*         *         *                            *         * SIZE    WE     PR     FF     MO     *          *  LABEL   *          *
*         *         *                            *         *                                     *          *          *          *
**********************************************************************************************************

  GUARD  1  ENT      ENTER                                    0     0      0      0      0                              0
  GUARD  1  ENT         BRANCHED                              0     0      0      0      0                 W1           0
  GUARD  2  ENT         BRANCHED                              0     0      0      0      0                 W2           0
  GUARD  3  ENT         BRANCHED                              0     0      0      0      0                 W3           0

  GUARD  1  W1       MONITOR SENSOR                           0     0      0      0      0      S1                      0

  GUARD  2  W2       MONITOR SENSOR                           0     0      0      0      0      S2                      0

  GUARD  3  W3       MONITOR SENSOR                           0     0      0      0      0      S3                      0

  ADVER  1  ENT1     ENTER                      F1           4.   8.00   8.00   8.00   8.00                             0
  ADVER  1  ENT1        BRANCHED                F1           4.   8.00   8.00   8.00   8.00                 CF1         0

  ADVER  1  CF1      START OF TASK              F1           4.   8.00   8.00   8.00   8.00                             0

  ADVER  1  CF1      END OF TASK                F1           4.   8.00   8.00   8.00   8.00                           .26
  ADVER  1  CF1         BRANCHED                F1           4.   8.00   8.00   8.00   8.00                 CSP1      .26

  ADVER  1  CSP1     START OF TASK              SP1          4.   8.00   8.00   8.00   8.00                           .26

  ADVER  1  CSP1     END OF TASK                SP1          4.   8.00   8.00   8.00   8.00                          1.42
  ADVER  1  CSP1        BRANCHED                SP1          2.   4.00   4.00   4.00   4.00                 DODN      1.42
  ADVER  2  CSP1        BRANCHED                SP1          2.   4.00   4.00   4.00   4.00                 CSP2      1.42

  ADVER  1  DODN     START OF TASK              OD           2.   4.00   4.00   4.00   4.00                          1.42
  ADVER  1  DODN        TRIGGERED SENSOR        OD           2.   4.00   4.00   4.00   4.00    S1                    1.42

  GUARD  1  W1       WAIT NODE TRIGGERED                      0     0      0      0      0                           1.42
  GUARD  1  W1          BRANCHED                              0     0      0      0      0                 DA1       1.42

  GUARD  1  DA1      START OF TASK              B1            0     0      0      0      0                           1.42
```

Figure 6. Simulation Trace Excerpt