Safeguard Systems at Nuclear Facilities: A Snap Application

Floyd H. Grant III, Alonzo F. Hixson III

Pritsker & Associates, Inc., P.O. Box 2413
West Lafayette, IN 47906

Dennis Engi, Ph.D.

Sandia Laboratories, Div. 5741,
Albuquerque, NM 87115

Abstract

Nuclear safeguards systems are primarily concerned with the physical protection of nuclear material. The Safeguards Network Analysis Procedure (SNAP) provides a convenient and standard analysis methodology for the evaluation of safeguards system effectiveness in its ability to resist theft or sabotage. 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 network modeling technique and provides an example illustrating its use.

INTRODUCTION

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.

SLAM embraces the network modeling philosophy in its approach to safeguards systems modeling and analysis. This approach provides the analyst with a highly flexible tool in which he may develop abstractions of his system in a timely manner and easily communicate those abstractions to others. The following sections will provide an overview of SNAP Network Modeling Philosophy and a brief discussion of the facility modeled as well as the guard and adversary tactics employed.

SNAP NETWORK MODELING PHILOSOPHY

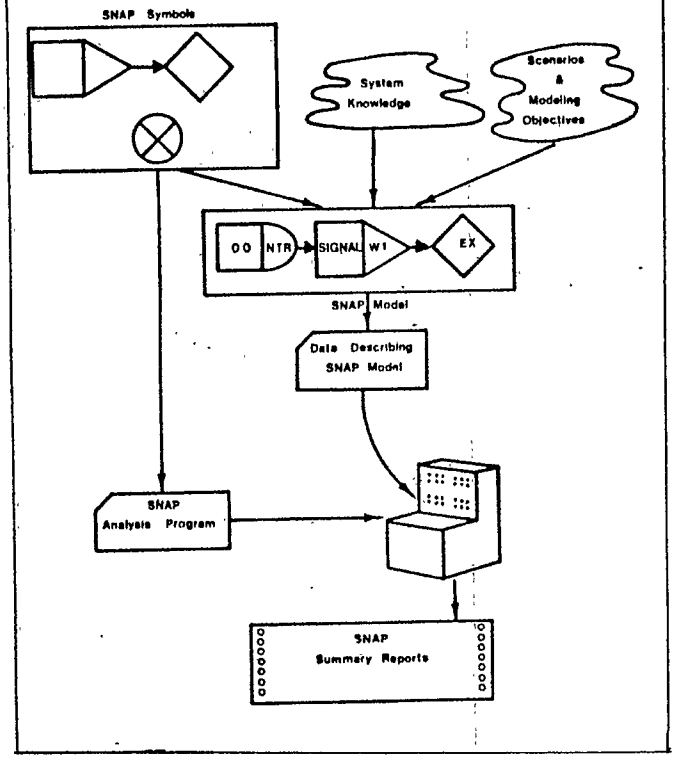
The modeling philosophy of SNAP may be defined on two levels. On the general level, SNAP employs the network modeling approach to problem solving. On the specific level, SNAP provides a structure for safeguards systems analysis by dividing safeguards systems into three interacting submodels. SNAP then provides procedures for modeling each of these submodels as well as the means for interaction. These two levels of approach will be summarized in the following discussion.

The network approach to modeling and simulation, which SNAP embraces, is illustrated in Figure 1. The analyst initially has specific knowledge of the system he wishes to analyze. In the case of safeguards systems, this might include a description of a facility, with its various sensors and guard operating policies. Additionally, the analyst has in mind a set of scenarios to be investigated and modeling objectives which he wishes to achieve through this analysis.

CH1437-3/79/0187-0192$00.75

1979 Winter Simulation Conference

Figure 1
SNAP Network Modeling Philosophy



These scenarios might include a set of alternative guard operating policies, and a set of adversary attack alternatives. In the analysis of safeguards systems, the primary modeling objective is to evaluate the effectivenss of a site and guard operating policies in countering an adversary attack. Specifically, he may wish to determine weak points in the system and the effectiveness of design alternatives for strengthening those weak points.

With specific system knowledge, a set of scenarios, and modeling objectives, the analyst employing the network approach to modeling is provided with a set of symbols which he may use to characterize his system. In SNAP, the user is provided with a unique set of symbols specifically designed for the characterization and modeling of safeguards system of interest. For example, symbols are provided to model such facility components as barriers, adversary targets, and adversary detection devices.

The analyst then combines his knowledge of the system, scenarios and modeling objectives, and the symbology provided to develop a network model of the system of interest. Typically, the elements of this network model will form a one-to-one correspondence with the components of the actual physical system or scenarios to be studied. Due to this relationship, an excellent communication vehicle is provided. Using this common set of symbols, system analysts may develop models of safeguards systems and efficiently communicate their analysis to each other.

Following the development of the network model of the system of interest, the analyst then transfers the model into data input records describing it. Specific procedures are defined for accomplishing this transformation and relate directly to the set of network symbols employed. That is, for each network symbol, there exists a corresponding data card describing the various parameters related to that symbol. These include such items as node labels, task duration time distributions, etc.

To process the data described in the network model, simulate the model, and provide summary reports indicating behavior of the system, the SNAP analysis program is provided. This analysis program first reads the data describing the network model into a data storage area. Then based on the data entered, simulations of the system are executed.

The simulation of the safeguards network produces summary reports that provide information on the probability of an adversary force achieving their objective and time duration of engagements. Additionally, a facility specific report is produced which includes information such as the occupation time by adversaries of various portions of the facility, and the probability that a facility point was reached by an adversary.

The network approach to modeling provides both a convenient communication vehicle and a model building device that requires no detailed computer programming. Thus speedy evaluations can be made and understood.

In developing models of various safeguards systems, three submodel components arise in every situation. These various submodels interact with each other to produce the overall behavior of the system.

The most fundamental submodel is concerned with the actual physical 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 facility and their relationships.

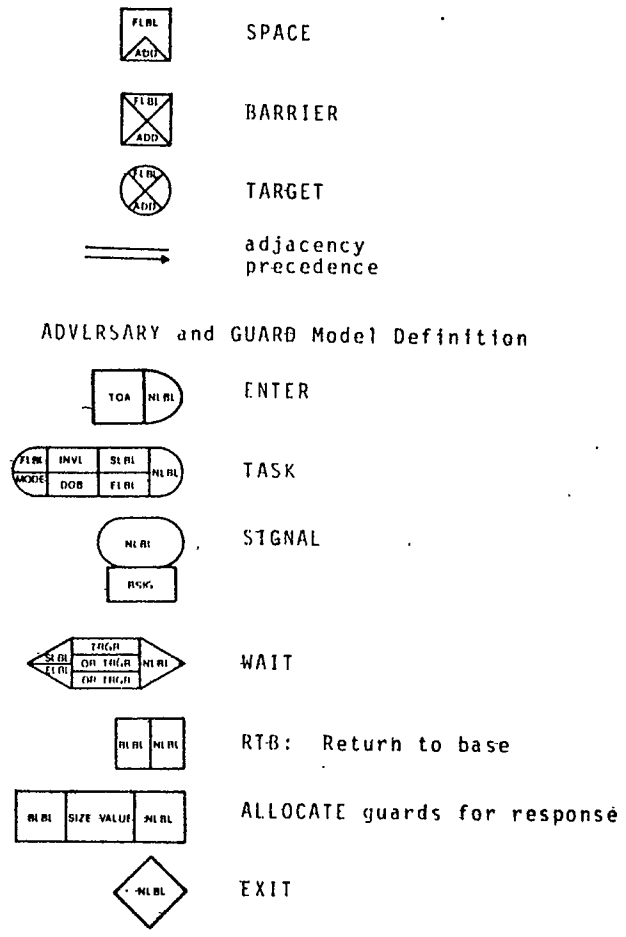
A second submodel involves guard operating policies. The guard submodel includes a representation of the decision logic associated with the guards as well as the physical movement of the guards through the facility. Guards may make decisions based on system status information as they progress through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

The third submodel is concerned with the adversary attack scenario. 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 model interacts with the facility model through sensor detection, actual movement through the facility, etc. The adversary model interacts with the facility in a similar manner. Interaction also occurs between the guard model and the adversary model. This is accomplished in two ways. First, each group may have 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. This information may or may not be current. These attributes are updated as guards and adversaries are processed through their respective submodels. Decisions may be made based upon these attributes. The second, more active form 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.

A set of symbols has been defined to characterize the various elements of safeguards systems for each of the three submodels. A list of the elements of the SNAP symbology is provided in Figure 2.

Figure 2
SNAP Symbology



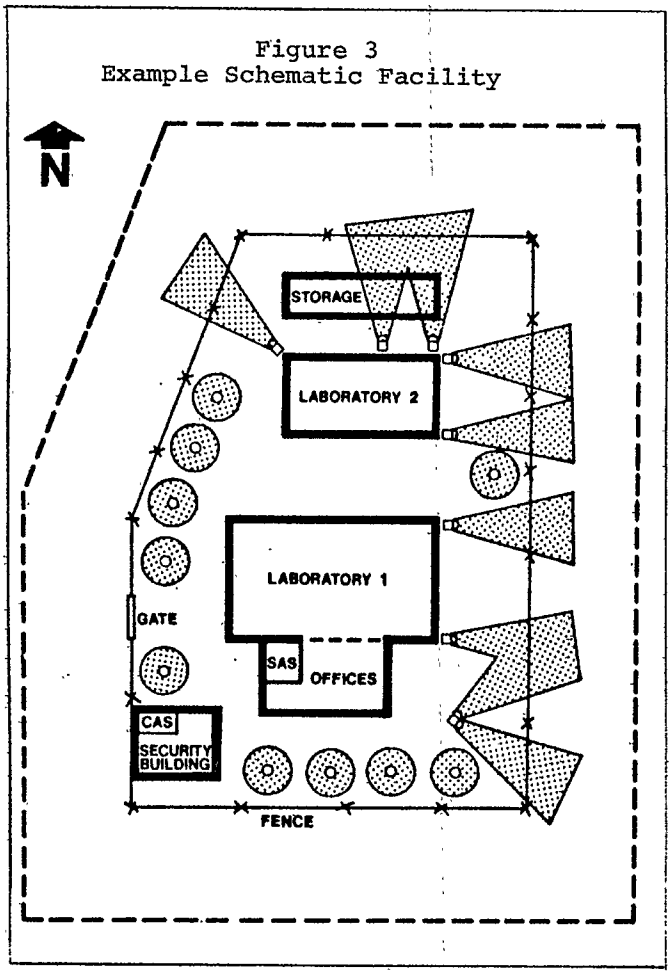
SNAP APPLICATION

Specific modeling procedures have been defined for developing SNAP models. Essentially, one constructs a model of the facility using the SNAP symbology. Based on this model, the user then develops models of the guard defense tactics and adversaries attack scenarios of interest.

The facility used in this model is a generic facility utilized by NRC personnel for various training exercises and tactics evaluations. Figure 3 provides an overall schematic of the facility. The facility consists of a fence enclosed area containing a security building and two laboratories. The Central Alarm Station (CAS) is located in the security building. The two laboratories each contain nuclear material and are potential adversary attack targets. Laboratory 1 also has offices attached to it, as well as a Secondary Alarm Station (SAS) which provides back-up monitoring of the facility.

Additionally, there is a storage area in the north portion of the facility consisting of small buildings and storage areas which could provide an adversary with

Figure 3
Example Schematic Facility



cover. Locations outside the fence which might represent adversary positions prior to actual fence penetration were also included in the SNAP model. Areas of higher lighting in the facility are illustrated by the spotlights or pole lamps in Figure 3. These areas provide higher visibility for individuals within that space, thus increasing neutralization potential given an engagement with an opposing force.

A variety of adversary detection devices are present in the facility. There are fence sensors on the perimeter fence segments and closed circuit TV (CCTV) cameras located at intervals along the perimeter fence. All external doors in the two laboratories have switch alarms which will be triggered if the doors are opened. Further, there are motion detectors inside each labortory. There is also a CCTV in the vault area in both Laboratories 1 and 2.

A set of general guard defense tactics to be included in the SNAP model were developed by Nuclear Regulatory Commission staff members. For this set of guard tactics, five guards are available at the site, typically armed with pistols. If an adversary confirmation state exists, a guard may have a shotgun. For the particular model developed, the guard tactics were restricted to offshift operations, as this was assumed to be the most likely time for adversary attack.

The guards and their patrol stations are as follows:

Guard 1 - The Central Alarm Station Operator; stationed permanently at the CAS;

Guard 2 - The Secondary Alarm Station Operator, stationed at the SAS;

Guard 3 - The Shift Supervisor stationed at the CAS;

Guard 4 - The Response Guard Stationed at the SAS; and

Guard 5 - The Patrol Guard stationed at the CAS.

Each of the guards has a number of responsibilities. These responsibilities are concerned with normal patrol operations as well as response and engagement operations given an adversary penetration.

The SNAP model of these guard procedures was designed to be as general as possible. The guard responses were tied to no particular attacks sequences against the defined guard tactics. In this application, the guard tactics model is by far the more complex of the three submodel components. This allows the analyst to readily evaluate adversary attack alternatives.

A number of adversary attack scenarios were modeled and exercised in conjunction with the guard defense tactics. To indicate briefly the results of some of the scenarios explored, Table 1 provides a primary system performance measure concerning each of these scenarios. A "system win" occurs when the guard force is successful in neutralizing the adversary threat. Therefore, the probability of system win represents a measure of the effectiveness of site safeguards in countering a specific adversary scenario.

Table 1
SNAP/GTS Guard Scenario Alternatives

	P(System Win)
1. Base case	.25
2. Guards in "normal" state locations	.22
3. Adversary SNM access time: 1/2 minute	.17
4. Patrol guard on east side of facility	.24
5. Guards on internal patrol in Laboratory 1	.05

In the base case scenario, adversaries attack from the west side of the facility, blowing a hole in the side of Laboratory 2 to access the nuclear material. They then exit using the same route. The adversaries are assumed to be detected when the explosion occurs. The adversary attack occurs just as the patrol guard begins his patrol of the external perimeter of the facility. As seen in Table 1, the base case scenario resulted in a probability of system win of .25.

In the second scenario, we see a slight drop in the probability of system win given that no guards are on patrol, and are at their normal stations. In the third case, the adversary SNM access time was reduced from 1 minute to 1/2 minute. This resulted in a reduction of the probability of system win to .17. The fourth modification was concerned with having the adversaries attack when the patrol guard was on the east side of the facility, at a point furthest from the point where the fence is penetrated. This resulted in a probability of system win similar to the base case. Finally, in the fifth case the adversaries attack when the guards are on internal patrol of Laboratory 1. Due to the excessive response time, the probability of system win was reduced to .05.

This section has provided indications concerning the system modeled and the type of analysis performed. The following will provide conclusions regarding SNAP research and applications.

CONCLUSIONS

The Safeguards Network Analysis Procedure (SNAP) provides analysts with a technique for modeling and evaluating various safeguards system design alternatives. The SNAP symbology also provides analysts with a vehicle for communication, thereby enhancing the model building process. The technique has been shown to be easy to use and requires no computer programming. SNAP is receiving extensive use in its application in the analysis of real-world nuclear facilities as well as the generic site discussed in this paper. SNAP is an effective tool for analyzing the safeguards effectiveness of a given nuclear site.

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

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

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

4. Chapman, L.D., 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. Deitchman, S.J., "A Lanchester Model of Guerrilla Warfare," Opns. Res., 10, 818-827, 1962.

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

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

8. Engi, D. and J.S. Shanken, Brief Adversary Threat Loss Estimator (BATLE) Users Guide, SAND, Sandia Laboratories, Albuquerque, New Mexico, December 1978.

9. Grant III, F.H. and A.F. Hixson, III, "A Preliminary SNAP Model of the SNM Transportation Problem," Sandia Laboratories, Albuquerque, New Mexico, November 1978.

10. Grant III, F.H. and R.J. Miner, "Safeguards Network Analysis Procedure (SNAP), Final Report," Sandia Laboratories, Albuquerque, New Mexico, May 1978.

11. Grant III, F.H., R.J. Miner, and D. Engi, "A Network Modeling and Analysis Technique for the Evaluation of Nuclear Safeguards Systems Effectiveness," Proceedings of the 1978 Winter Simulation Conference, 1978, 899-906.

12. Grant III, F.H. and C.D. Pegden, "The Design and Evaluation of a Gaming Capability in SNAP," Sandia Laboratories, Albuquerque, New Mexico, November 1978.

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

14. Miner, R.J. and F.H. Grant III, The SNAP User's Guide, Sandia Laboratories, Albuquerque, New Mexico, November 1978.

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

16. Pritsker, A.A.B, Modeling and Analysis Using Q-GERT Networks, John Wiley & Sons, New York, 1977.

17. Pritsker, A.A.B. and C.D. Pegden, Introduction to Simulation and SLAM, John Wiley & Sons, New York and Systems Publishing Corporation, West Lafayette, IN, 1979.

18. Schaffer, M.M. "Lanchester Models of Guerrilla Engagements," Opns. Res., 16, 457-488, 1968.

19. Weiss, H.K. "Lanchester-Type Models of Warfare," Proceedings, First International Conference on Operational Research, Oxford, September 1977.