

NUREG/CR-0960
SAND79-0438
RS

Safeguards Network Analysis Procedure (SNAP) - Overview

Leon D. Chapman, Dennis Engi

Printed August 1979



Sandia Laboratories

2900 Q(7-73)

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

8007280 053

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

The views expressed in this report are not necessarily those of the U. S. Nuclear Regulatory Commission

Available from
National Technical Information Service
Springfield, Virginia 22161

SAND79-0438
NUREG/CR-0960
RS

Safeguards Network Analysis Procedure (SNAP)
- Overview

Leon D. Chapman and Dennis Engi

Sandia Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Laboratories
for the
U.S. Department of Energy

Prepared for
Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555
Under Interagency agreement DOE 40-550-75
NRC FIN No. A1060-8

*Presented at the 20th Annual Meeting of the Institute of Nuclear
Materials Management, Albuquerque, NM, July 16-18, 1979

Abstract

Nuclear safeguards systems provide physical protection and control of nuclear materials. The Safeguards Network Analysis Procedure (SNAP)* provides a convenient and standard analysis methodology for the evaluation of physical protection 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 outputs provided by the SNAP simulation program supplements the safeguards analyst's evaluative capabilities and supports the evaluation of existing sites as well as alternative design possibilities. This paper describes the SNAP modeling technique and provides an example illustrating its use.

*SNAP was developed for Sandia Laboratories by Pritsker and Associates, Inc., West Lafayette, Indiana.

CONTENTS

	<u>Page</u>
Introduction -----	9
Modeling Philosophy -----	11
SNAP Symbology -----	12
SNAP Application -----	14
Commentary -----	18
References -----	19
Tables I and II -----	20
Table III -----	21
Figure 1 -----	22
Figures 2 and 3 -----	23
Figures 4 and 5 -----	24

Safeguards Network Analysis Procedure (SNAP) - Overview

Introduction

The development of models to aid in the evaluation of physical protection systems of nuclear facilities began at Sandia Laboratories as early as 1974¹. This work has been sponsored principally by the United States Nuclear Regulatory Commission. The purpose for developing these models is to construct techniques which can aid the physical protection system analyst. The goals of this systematic approach to evaluation are to provide:

1. A consistent approach to the evaluation of the effectiveness of physical protection systems in defending against a hypothesized adversary threat, and
2. A quantitative technique for determining upgrades to existent facilities and for designing new facilities.

The Safeguards Network Analysis Procedure (SNAP) developed through this research is a valuable technique which can be used by the physical protection system analyst in meeting these goals.

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 assists the analyst in evaluating the performance of proposed or existing safeguards system.

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. With SNAP, the focus is on micro-completeness and the analyst is afforded the flexibility to model individual scenarios to virtually any level of detail that is deemed appropriate.

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

SNAP is a simulation language developed specifically for modeling safeguards systems². With the SNAP approach, the analyst constructs a model of the safeguards system by interconnecting a set of SNAP symbols to represent the system elements and their interactions. The resulting SNAP networks are then translated to a computer compatible form by data cards representing the symbols and their interconnections.

Using the SNAP procedure for safeguards modeling, one combines knowledge of the system, scenarios, modeling objectives, and the SNAP symbology to develop a network model of the system under consideration. This network model is a graphic representation of the nuclear facility, guard operating policies, and adversary attack scenario. Typically, the elements of this network model will form a one-to-one correspondence with the components of the actual physical system and scenario being studied. Due to this relationship, a SNAP network provides an excellent communications vehicle. SNAP symbols have been designed to represent the individual elements of a nuclear safeguards system, thus the translation from a system element to the SNAP symbol should be direct.

A SNAP network model is composed of the facility subnetwork, the guard subnetwork, and the adversary subnetwork which interact to produce the overall behavior of the safeguards system. Items which flow through network models are referred to as transactions. The transactions which flow through a SNAP network are guard forces and adversary forces. The force is the most fundamental

level of detail in SNAP and represents one or more individuals acting as a single unit.

The facility subnetwork is the most basic of the three networks. It is a static network in the sense that transactions do not flow through it during the simulation. Its purpose is to define the various elements of the facility and their relationships. These elements may include fences, yards, nuclear material, storage vaults, doorways, room sensors, etc. The guard subnetwork defines guard operating policies and includes a representation of the guards' decision logic as well as their physical movement through the facility. Guard forces are the transactions which flow through the guard subnetwork. The adversary subnetwork is treated in a similar manner.

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 I. The PORTAL, SPACE, BARRIER, and TARGET elements identify actual facility system components. Adjacency and Precedence branches define their interrelationships. 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 I).

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 II. Each of these elements 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.

A unique data card has been defined for each symbol 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.

SNAP Application

In order to illustrate the use of the symbology and indicate the information available from the analysis the following example application is provided. This application illustrates the use of SNAP concepts and symbols to model systems 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 1. 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 access area. The material access area is monitored by sensor S2, a motion detector.

Figure 2 illustrates the corresponding SNAP facility subnetwork. This figure has been labeled so as to make a one-to-one correspondence between the storage site schematic and the model. 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 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 subnetwork is shown in Figure 3. 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 (MS2), 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 procedures which the guards will follow in this model. This guard subnetwork is typical of guard

responses to adversary intrusion for the hypothetical facility under consideration.

The adversary force subnetwork is shown in Figure 4. The adversary's 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 penetrate fence 1 (CF1). 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, they join and penetrate fence 2 (CF2), exiting the facility (EX2). Since the adversary objective is sabotage, the adversaries do not have to exit the network to be successful.

Figure 5 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 III. From these results, the user can obtain information concerning the behavior of the 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 was successful in penetrating sabotage on 13 percent of the attempts. 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. Other performance measures are available as indicated.

Commentary

The Safeguards Network Analysis Procedure 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 is easy to use and is currently being used in the analysis of real-world nuclear facilities.

It should be emphasized that the physical protection analyst should remain intimately involved with the analysis at every stage. Due to the complexity of physical protection problems, information gained by exercising SNAP, is intended to be of a supplementary nature only. That is, the analyst should consider the outputs of SNAP as inputs to the holistic evaluative process.

References

1. Chapman, L. D., et.al, "Safeguards Methodology Development History," Proceedings of the 1st Annual Symposium on Safeguards and Nuclear Material Management, April 1979.
2. Grant, 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, Albuquerque, NM, December 1978.

TABLE I
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		

TABLE II
Guard and Adversary Model Symbology



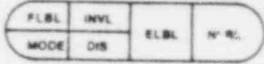

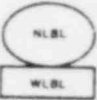
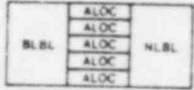




ENTER		Enter System
EXIT		Exit System
TASK		Perform Task
WAIT		Wait for Signal or Triggering Condition
SIGNAL		Signal WAIT Node
ALLOCATE		Allocate Guard Resources
RTB		Return Resources to Base
BASE	data card	Define Base Characteristics
OBJECTIVE	data card	Define Adversary Objective
REINFORCEMENT	data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

TABLE III

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.

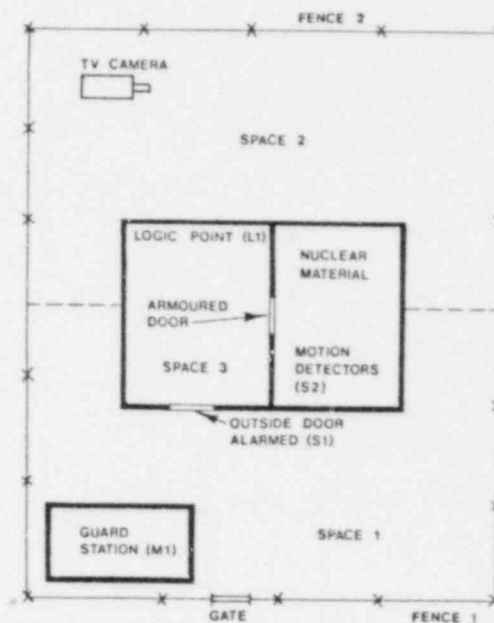


Figure 1. Exemplary Facility Schematic

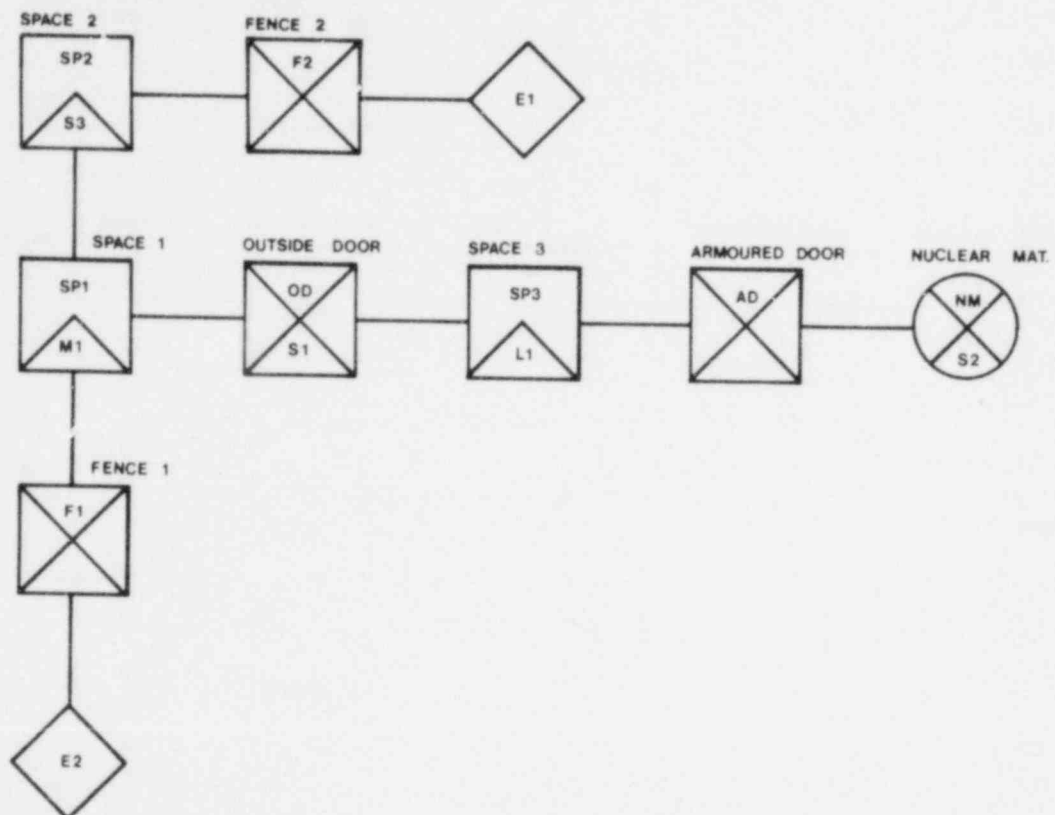


Figure 2. SNAP Model of the Exemplary Facility

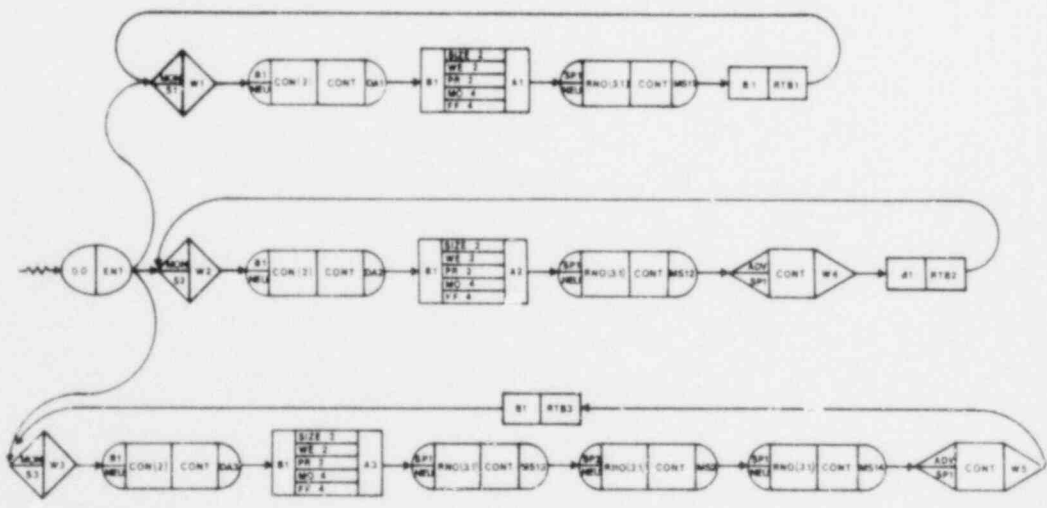


Figure 3. Guard Force Scenario Network

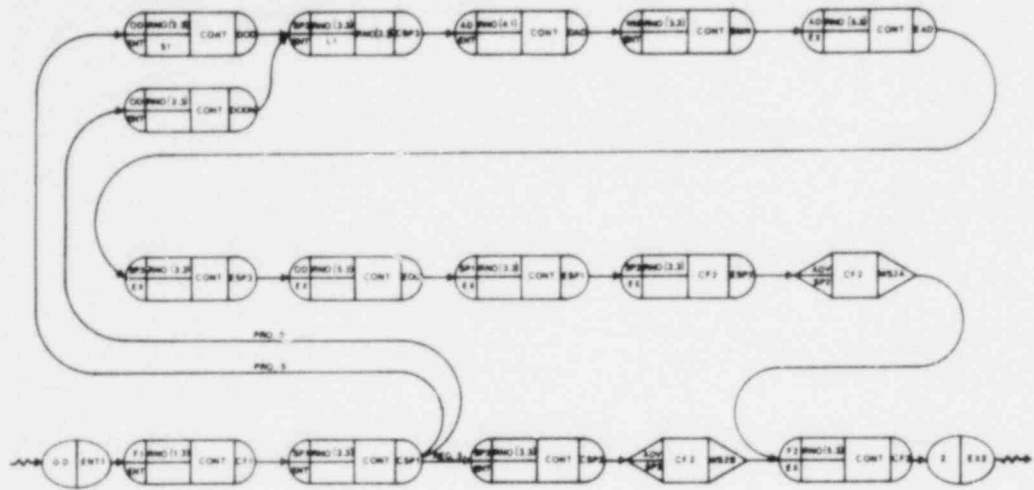


Figure 4. Adversary Force Scenario Network

```

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

```

FORCE	NODE LABEL	EVENT	FACILITY NODE	FORCE ATTRIBUTES					SENSOR LABEL	ASSOC. NODE LABEL	TIME
				SIZE	WE	PR	FF	MD			
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	
ADUER 1	ENT1	ENTER	F1	4.	8.00	8.00	8.00	8.00		0	
ADUER 1	ENT1	BRANCHED	F1	4.	8.00	8.00	8.00	8.00	CF1	0	
ADUER 1	CF1	START OF TASK	F1	4.	8.00	8.00	8.00	8.00		0	
ADUER 1	CF1	END OF TASK	F1	4.	8.00	8.00	8.00	8.00		.26	
ADUER 1	CF1	BRANCHED	F1	4.	8.00	8.00	8.00	8.00	CSP1	.26	
ADUER 1	CSP1	START OF TASK	SP1	4.	8.00	8.00	8.00	8.00		.26	
ADUER 1	CSP1	END OF TASK	SP1	4.	8.00	8.00	8.00	8.00		1.42	
ADUER 1	CSP1	BRANCHED	SP1	2.	4.00	4.00	4.00	4.00	DODN	1.42	
ADUER 2	CSP1	BRANCHED	SP1	2.	4.00	4.00	4.00	4.00	CSP2	1.42	
ADUER 1	DODN	START OF TASK	DD	2.	4.00	4.00	4.00	4.00		1.42	
ADUER 1	DODN	TRIGGERED SENSOR	DD	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 5. Simulation Trace Excerpt

DISTRIBUTION:

U.S. Nuclear Regulatory Commission (260 copies for RS)
Division of Document Control
Distribution Services Branch
7920 Norfolk Branch
Bethesda, MD 20014

U.S. Nuclear Regulatory Commission
MS 88155
Washington, DC 20555
Attn: M. Padden

U.S. Nuclear Regulatory Commission (2)
MS 1130SS
Washington, DC 20555
Attn: R. Robinson

Los Alamos Scientific Laboratory
Attn: G. R. Keepin, R. A. Gore, E. P. Schlonka, D. G. Rose
Los Alamos, NM 87544

Allied-General Nuclear Services
Attn: G. Molen
P.O. Box 847
Barnwell, SC 29812

Lawrence Livermore Laboratory
University of California
P.O. Box 808
Attn: A. Maimoni
Livermore, CA 94550

Pritsker and Associates, Inc.
P.O. Box 2413
Attn: F. H. Grant
West Lafayette, In 47906

Union Carbide Corporation
Nuclear Division
Bldg. 7601
Attn: D. Swindle
Oak Ridge, TN 37830

400 C. Winter
1000 G. A. Fcwler
1213 V. E. Gibbs
1230 W. L. Stevens, Attn: R. E. Smith, 1233
1700 W. C. Myre
1710 V. E. Blake, Attn: M. R. Madsen, J. W. Kane
1716 R. L. Wilde, Attn: B. D. Link, 1716
1730 C. H. Mauney, Attn: J. D. Williams, 1739
1750 J. E. Stiegler, Attn: M. J. Eaton, D. L. Mangan, 1759
1754 I. G. Waddoups, Attn: J. L. Todd, 1754
1758 C. E. Olson, Attn: D. D. Boozer, G. A. Kinemond, 1758
1760 J. Jacobs, Attn: M. N. Cravens, J. M. deMontmollin, 1760A
1761 T. A. Sellers, Attn: A. E. Winblad, J. L. Darby, 1761
1762 H. E. Hansen
1765 D. S. Miyoshi
4400 A. W. Snyder

DISTRIBUTION (Cont)

4410 D. J. McCloskey
4413 N. R. Ortiz
4414 D. E. Bennett
4414 S. L. Daniel
4414 M. S. Hill
4414 G. B. Varnado
4416 L. D. Chapman (4)
4416 K. G. Adams
4416 J. A. Allensworth
4416 H. A. Bennett
4416 D. Engi (5)
4416 L. M. Grady
4416 C. P. Harlan
4416 R. D. Jones
4416 M. T. Olascoaga
4416 C. J. Pavlakos
4416 J. R. Rowland
4416 D. W. Sasser
4416 D. R. Strip
5000 J. K. Galt
5600 D. B. Shuster, Attn: A. A. Lieber, M. M. Newsom, 5620,
R. C. Maydew 5630
5640 G. J. Simmons, Attn: R. J. Thompson, 5641,
L. F. Shampine, 5642
5641 C. A. Morgan
5642 B. L. Hulme
8266 E. A. Aas
3141 T. L. Werner (5)
3151 W. L. Garner (3)
For: DOE/TIC (Unlimited Release)
3172-3 R. P. Campbell (25)
For NRC Distribution to NTIS