NUREG/CR-1591
SAND80-0529
RS

A COMBINED SAFE/SNAP*
APPROACH TO SAFEGUARDS EVALUATION

D. Engi and L. D. Chapman
Sandia National Laboratories
Albuquerque, NM 87185

F. H. Grant and J. Polito
Pritsker & Associates, Inc.
West Lafayette, IN 47906

Printed: August 1980

Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
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, DC 20555
Under Interagency Agreement DOE 40-550-75
NRC FIN NO. A1060

and

Naval Surface Weapons Center
White Oak Laboratory
Silver Spring, MD 20910
Under Project Order No. N60921-79-W0064

*Presented at the 21st Annual INMM Conference, West Palm Beach, Florida, June 30-July 2, 1980.

ABSTRACT

Generally, the scope of a safeguards evaluation model can efficiently address one of two issues: (1) global safeguards effectiveness or (2) vulnerability analysis for individual scenarios. The Safeguards Automated Facility Evaluation (SAFE) focuses on the first issue, while the Safeguards Network Analysis Procedure (SNAP) is directed towards the second. SAFE addresses global safeguards effectiveness in that it considers the entire facility, i.e., the composite system of hardware and human components, in one "global" analysis. SNAP addresses individual-scenario vulnerability by providing a safeguards modeling symbology sufficiently flexible to represent quite complex scenarios from the standpoint of hardware interfaces, while also accounting for a rich variety of human decision making. A combined SAFE/SNAP approach to the problem of safeguards evaluation is described and illustrated through an example.

2

CONTENTS

Page

Executive Summary -- 9,10

Introduction -- 11

A Combined SAFE/SNAP Approach ---------------------------- 13

Future Development Activities for the SAFE/SNAP Approach -- 17

Summary--- 19

References -- 20

Figure 1: Model Orientation Categorization ---------------------- 12

Figure 2: SNAP Guard Scenario Played Against a SAFE Generated Adversary Scenario ----------------------- 15

EXECUTIVE SUMMARY

Generally, the scope of a safeguards evaluation model can efficiently address one of two issues: (1) global safeguards effectiveness or (2) vulnerability analysis for individual scenarios. The combined Safeguards Automated Facility Evaluation (SAFE)/Safeguards Network Analysis Procedure (SNAP) approach to safeguards evaluation provides a method of addressing both the global and scenario aspects of physical protection system evaluations. SAFE addresses global safeguards effectiveness in that it considers the entire facility, i.e., the composite system of hardware and human components, in one "global" analysis. SNAP addresses individual-scenario vulnerability by providing a safeguards modeling symbology sufficiently flexible to represent quite complex scenarios from the standpoint of hardward interfaces, while also accounting for a rich variety of human decision making. A combined SAFE/SNAP approach to the problem of safeguards evaluation is described and illustrated through an example. The new capabilities provided by the future developmental activities will substantially enhance the usability of the combined SAFE/SNAP approach and should provide an effective tool for safeguards evaluation.

INTRODUCTION

Generally stated, the objective of a physical protection system is two-fold. First, the system must protect against the theft of special nuclear material. In this context, theft refers to the removal of special nuclear material beyond the boundary of the nuclear facility. Second, the physical protection system must protect against the release of radiotoxic material beyond the facility boundary. The effectiveness of a physical protection system is determined by the degree to which this objective is achieved.

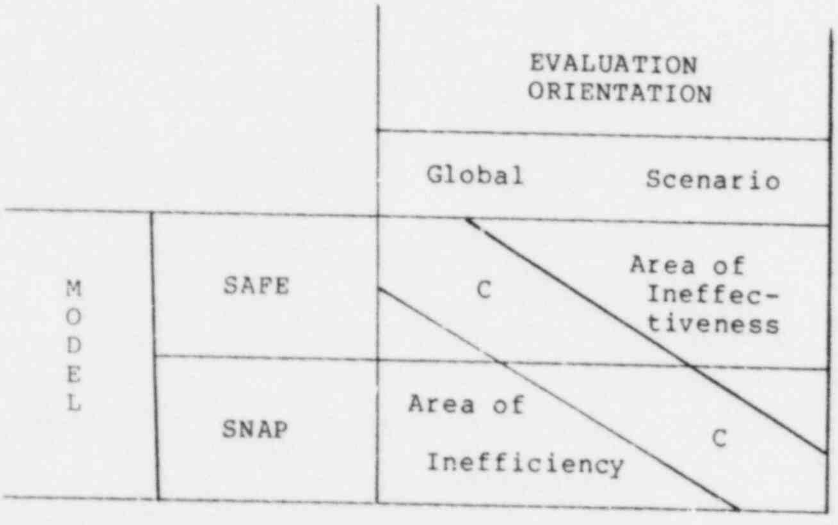
The development of models to aid in the evaluation of physical protection systems of nuclear facilities began at Sandia National Laboratories in 1974.[1] The purpose in developing these models is to fulfill the need for

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 existing facilities and for designing new facilities.

This developmental activity has led to two quite distinct approaches to modeling physical protection systems. One approach is to provide the capability to represent individual scenarios to virtually any level of detail. This "scenario-oriented" approach focuses primarily on the detailed representation of complex tactics that might be used by the adversaries as well as by the security forces. The ability to reflect this detail lends credibility to the evaluation of individual scenarios. However, an evaluation of the effectiveness of a physical protection system in countering individual adversary scenarios merely reflects the system's ability (or inability) to deal with those scenarios---it is likely to imply little concerning the safeguards system as a whole. Consequently, a "globally-oriented" approach which evaluates the physical protection system in its entirety is also warranted.

The Safeguards Automated Facility Evaluation (SAFE)[2] technique was developed with a global orientation. SAFE combines into a continuous stream of operation, a collection of functional modules for facility representation, component performance selection, adversary path analysis, and effectiveness evaluation. The Safeguards Network Analysis Procedure (SNAP)[3] is a sce'ario-oriented evaluation language developed specifically for physical protection systems. SNAP consists of a set of safeguards symbols and rules for interconnecting those symbols into network representations of the scenarios.

Figure 1 depicts a categorization of model orientation. The main diagonal represents congruent association, which means a given



C ∿ Congruent Association

Figure 1. Model Orientation Categorization

category is associated with the model which will deal most effectively and efficiently with it. This figure illustrates that SAFE is best suited for a global evaluation, while SNAP is more appropriate for evaluating individual scenarios. Below the main diagonal lies the area of inefficiency, wherein the SNAP analysis of individual scenarios is too detailed to allow for an efficient evaluation of more than a few scenarios. In contrast, above the main diagonal, the inability to incorporate detail into individual scenarios with SAFE yields an analysis that cannot effectively deal with complex tactics.

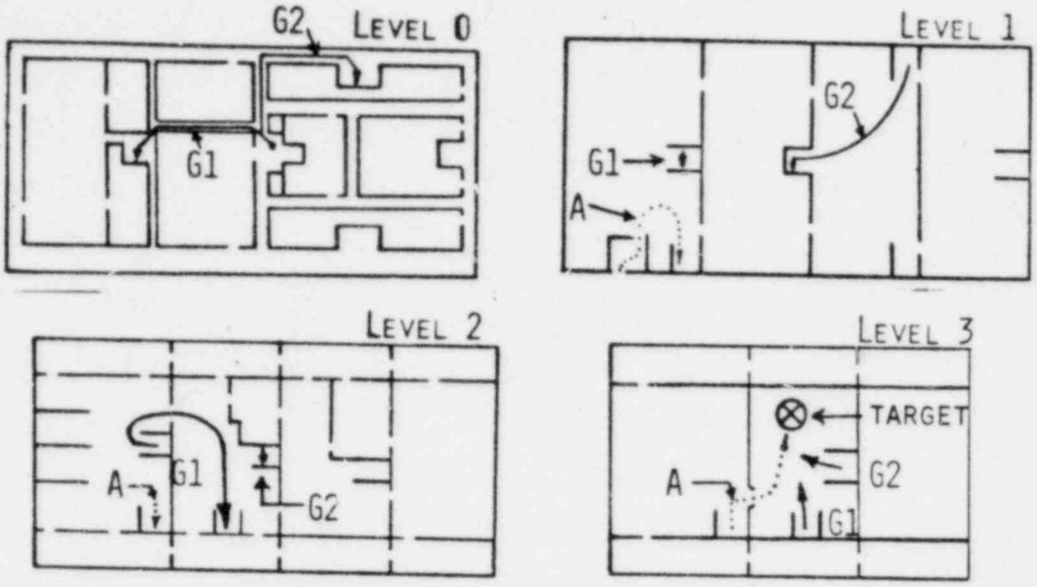
A combined SAFE/SNAP approach provides a methodology sufficiently broad in scope to encompass the global as well as the scenario aspects of the problem of evaluating a physical protection system. Moreover, if the techniques are judiciously applied, the physical protection system analyst can avoid the potential pitfalls described above. The next section illustrates a combined SAFE/SNAP approach to evaluation.

A COMBINED SAFE/SNAP APPROACH

In order to perform a SAFE analysis it is necessary to have a description of the facility that includes all of the points of entrance, the speed at which the adversary crosses open fields, rooms, hallways, etc., the times necessary to penetrate barriers, and the time to commit sabotage or theft. In addition, the position and effectiveness of sensors and communication systems must be known. Based on this information, SAFE will determine, from all of the possible routes to the target material, those paths that offer the adversary the highest probability of success. It does this by minimizing the probability of interruption which is the probability that the physical protection system will detect the adversary with sufficient delay time remaining in his sequence for the guard force to respond and confront the adversary. The guard force responds directly to interrupt the adversary once detection has occurred. The guard response times are determined by a systematic, analytic procedure.

Figure 2 represents four levels of a facility which is the subject of an adversary attack. The attack path was determined by SAFE. The adversaries enter on Level 1 through an alarmed industrial elevator and immediately enter a stairwell to descend to Level 3 where the target material is stored. They reach Level 3 and penetrate a wall to enter the target room. The target room is equipped with motion detectors. This path was determined considering a guard force which would respond to the target room after an adversary force is detected. Actual procedures call for the guards to assemble on Level 0 and split into two groups. As soon as a sufficient number of guards have assembled to form force G1, they will move through a corridor and descend a stairway to Level 2. On Level 2, they search for adversaries and then descend to Level 3 to protect the target material. Force G2, once assembled, descends by a different stairwell to Level 1, search for adversaries, and then descends directly to the target room.

It is clear from inspection of Figure 2 that the attack is a race between the adversaries, who are usually detected at the elevator, and the guards. Recommendations for improvements to the safeguards systems are often available from both the SAFE and the SNAP analyses. For example, if many of the adversary paths identified by SAFE traverse the same portion or portions of the facility, then, clearly, the adversary task times and/or detection devices should be made less favorable for the attacker. Similarly,



1. Guard forces Gl and G2 leave assembly point and descend stairways.
2. Gl continues down stairway
3. G2 reaches bottom of first stairway, exits and descends second stairway.
4. The Adversary Force (A) enters through an industrial elevator and descends through stairway.
5. Gl reaches bottom of stairway, searches for adversaries, and descends.
6. G2 and A continue descent in their respective stairways.
7. Gl and G2 enter to protect target material.
8. A penetrates wall.

Figure 2. SNAP Guard Scenario Played Against a SAFE Generated Adversary Scenario

the SNAP analysis may indicate deficiencies in the guard procedures. For the situation shown in Figure 2, the analysis indicates that guards usually interrupt the adversaries before they can complete their sabotage. However, the guards are armed with handguns only and, when faced with a well-armed adversary force, are usually defeated during the engagement in the target room. Thus, even though the guard response procedure is adequate to interrupt this particular attack scenario, the adversaries usually accomplish their mission because of superior firepower.

The paths that are output from SAFE are excellent candidates for evaluation with a SNAP method that can more thoroughly represent tactics. With SNAP, guard tactics such as patrols and responses to alarms can be modeled in detail, and these tactics can be "played against" specific adversary scenarios. SNAP cannot generate adversary scenarios, however. Thus, a combined SAFE/SNAP approach permits vulnerable adversary paths to be generated with SAFE from among all of the paths to the targets; SNAP can then be used to play these scenarios against realistic guard procedures.

Another advantage of the combined approach is that engagement statistics can be collected with SNAP for use in SAFE. The outcome of an engagement is highly dependent upon the characteristics of the physical environment, such as range, illumination, cover, number of combatants, arrivals of reinforcements, and delaying tactics. SNAP analyses indicate those locations in the facility at which engagements are likely to occur and thus provide data on cover, illumination, and other physical characteristics. Also, arrival time, reinforcements and delay tactics can be obtained as a function of guard and adversary tactics. This information can be used with the SAFE engagement model, BATLE[4], to provide more realistic data for SAFE and to investigate the effects of changes to physical site characteristics (e.g., illumination) and tactics (e.g., guards employ delay tactics).

A further advantage of the combined approach is that complex adversary attack scenarios can often be constructed from the results of sensitivity analysis performed with SAFE. For example, most nuclear facilities are protected by an alarmed fence, and the detection which occurs at the fence may be of critical importance to the success of the guards in interrupting the adversaries

A SAFE analysis that assumes no detection at the fence often reveals paths which have no detection until the adversaries are so close to their objective that they cannot be interrupted. SNAP adversary scenarios can be constructed to play these paths against the guards even though detection takes place at the fence. This can be done by permitting the adversaries to create diversions. An adversaiy force may penetrate the fence and be detected but then immediately splits into two or more groups, one of which follows the optimal path for no detection at the fence. The other adversary forces draw attention to themselves by tripping other sensors, engaging the guards, or creating a disturbance with gunfire, artillery simulators, grenades, etc.

FUTURE DEVELOPMENT ACTIVITIES FOR THE SAFE/SNAP APPROACH

At present, the SAFE and SNAP analyses must be performed independently. Each methodology has its own data input format. It is clear, however, that much of the information that is required is common to the two procedures. In particular, each must have a complete facility description. SAFE, especially, is facility oriented. A digitized description of the facility is produced by the SAFE analyst, and much of the effort is directed toward insuring that the facility model is correct and collecting data on sensor effectiveness, barrier penetration times, etc. Once this task is complete, the generation of vulnerable paths is automatic. Thus, it is quite easy to perform sensitivity analysis with SAFE once the initial data file is constructed.

SNAP, on the other hand, tends to be procedure oriented. Facility data are needed, of course, but not with the same level of detail required for SAFE. Substantial effort may stil. be required by the SNAP analyst to construct the facility model. Much of the analyst's time, however, is spent constructing symbolic models of guard and adversary tactics. In this sense, trying out many different scenarios requires more than adjustment of certain input parameters; the analyst must reconstruct part or all of a previous scenario to test a new one.

Current work is aimed at reducing the time needed to construct and modify SNAP models once a SAFE analysis has been performed. Two software systems will be developed to achieve this goal. The first is the SAFE/SNAP interface. Since the SAFE facility model is essentially adequate for use in SNAP, this interface will accept the digitized SAFE data and produce a SNAP-compatible facility description automatically. Also, because the guard and adversary paths produced by SAFE are relatively simple to model with SNAP, it is possible to automatically produce the symbolic SNAP models which represent the SAFE paths. Thus, at the conclusion of the SAFE analysis it will be possible in one step to automatically produce SNAP models which emulate the SAFE scenarios. These models will then be used as a point of departure to develop more complex scenarios with SNAP. The SNAP analyst will be spared the "set up cost" of reformulating the facility description and developing initial symbolic models.

The second set of programs will aid in developing and modifying SNAP symbolic models. An interactive, graphical editor is under development which will allow the analyst to quickly develop symbolic models and which will automatically produce the appropriate data card input to represent the symbolic model.

SUMMARY

The combined SAFE/SNAP approach to safeguards evaluation provides a method of addressing both the global and scenario aspects of physical protection systems evaluations. The high degree of flexibility that SNAP provides in the representation of detail can be used with the insight obtained from SAFE to construct detailed adversary scenarios that test facility protection systems and guard force tactics. Similarly, it is possible to test recommended improvements in guard procedures and physical protection systems to determine their efficiency against very sophisticated attack plans. The new capabilities provided by the future developmental activities will substantially enhance the usability of the combined SAFE/SNAP approach and should provide an effective tool for safeguards evaluation.

REFERENCES

1. L.D. Chapman, et al., Safeguards Methodology Development History, SAND79-0059, Sandia National Laboratories, Albuquerque, New Mexico, May 1979.

2. L. D. Chapman, et al., Safeguards Automated Facility Evaluaation (SAFE) Methodology, SAND78-0378, Sandia National Laboratories, Albuquerque, New Mexico, August 1978.

3. L. D. Chapman, et al., Safeguards Network Analysis Procedure (SNAP), SAND79-0617, Sandia National Laboratories, Albuquerque, New Mexico, March 1979.

4. D. Engi and C. P. Harlan, Brief Adversary Threat Loss Estimator (BATLE) User's Guide, SAND80-0952, Sandia National Laboratories, Albuquerque, NM, to be published.

DISTRIBUTION:

U.S. Nuclear Regulatory Commission (320 copies for RS)
Division of Document Control
Distribution Services Branch
7920 Norfolk Ave.
Bethesda, MD 20014

U.S. Nuclear Regulatory Commission
MS 881SS
Washington, DC 20555
Attn: M. Fadden

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: P. E. Ebel
P.O. Box 847
Barnwell, SC 29812

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

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

Pritsker and Associates, Inc.
P.O. Box 8345
Attn: J. Polito
Albuqurque, NM 87198

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

400	C. Winter
1000	G. A. Fowler
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
1720	C. H. Mauney, Attn: J. D. Williams, 1729
1727	V. K. Smith
1730	J. D. Kennedy, Attn: W. N. Caudle, 1734
1750	J. E. Stiegler, Attn: M. J. Eaton, 1759

DISTRIBUTTION (Cont.)

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
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 (10)
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. M. Richardson
4416	D. W. Sasser
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
5642	B. L. Hulme
8266	E. A. Aas
3141	T. L. Werner (5)
3151	W. L. Garner (3) For: DOE/TIC (Unlimited Release)
3154-3	R. P. Campbell (25) For: NRC Distribution to NTIS