PHYSICAL PROTECTION OF NUCLEAR FACILITIES

Progress Report

November-December 1978

Prepared by

Leon D. Chapman

Safeguards Methodology Development Division 4416

Sandia Laboratories

NRC Research and Technical Assistance Report

30 January 1979

7902280218

PHYSICAL PROTECTION OF NUCLEAR FACILITIES

Progress Report

SUMMARY

In-House Activities

Activities this month included completion of a major portion of the Standardized Nuclear Unit Power Plant System (SNUPPS) facility characterization. Vital area analysis of a boiling water reactor (BWR) and a benchmark calculation for a pressurized water reactor (PWR) were also completed. Work was initiated on a computer-based fault tree development program which will hopefully reduce the time and manpower required to translate facility and operational information into fault tree logic.

A new computer code, ADPATH, which finds both theft and sabotage paths in a facility digraph and takes into account adversary direction of travel has been developed and tested. A set of theft and sabotage problems has been devised to fully exercise the capabilities of ADPATH.

Considerable time was spent this reporting period in preparing for a demonstration of the Safeguards Automated Facility Evaluation (SAFE) methodology to the Nuclear Regulatory Commission (NRC) and documentation of the SAFE process and related computer codes. Efforts to develop a capability which provides for the automatic identification of regions within SAFE continued.

Work related to the Safeguards Network Analysis Procedure (SNAP) concentrated on (1) the implementation of the Guard Tactics Simulation (GTS) engagement model, a tamper alarm capability, and a 72-column output capability, (2) the incorporation of new force-based stati tics, (3) an investigation of the question of detail in SNAP facility models,

and (4) the application of SNAP to a GTS scenario. Initial work has also been completed on the development of a SNAP short course.

FACILITY CHARACTERIZATION

In-House Activities

During November and December, the major part of the characterization of the Standardized Nuclear Unit Power Plant System (SNUPPS) plant design was completed. This characterization includes system descriptions for five important safety systems (auxiliary feedwater, residual heat removal, emergency electric power, reactor protection and primary coolant system boundary), development of the sabotage fault trees, and identification of the areas where basic sabotage actions can be accomplished. The fault trees and location information have been computerized for ease of future modification and analysis.

The SNUPPS characterization information will be used in several areas: (1) demonstration of the Safeguards Automated Facility Evaluation (SAFE) methodology, (2) the Nuclear Power Plant Design Concepts for Sabotage Protection program, (3) the Hazards to Nuclear Reactors from Nearby Transportation Accidents program, and (4) a fire protection study.

The vital area analyses of operating power reactors continued with the completion of a boiling water reactor (BWR) facility and a benchmark calculation for a pressurized water reactor (PWR) facility. Analyses were also performed for alternate configurations of two previously completed PWR plants. This work is part of a joint effort with Los Alamos Scientific Laboratory (LASL) for the Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation.

The transfer of the computer code, Set Equation Transformation System (SETS), and accompanying analysis capabilities to LASL is a continuing effort. One PWR facility was used as a benchmark case; the

computer analysis for this case was performed satisfactorily at both LASL and Sandia.

Assistance was given to Lawrence Livermore Laboratory in the use of SETS to solve large digraph problems which were developed in their material control and accounting program. The digraphs led to very large equations involving complement events and hence represent a different class of problems from fault trees. This work indicates that there exists a need to extend and improve SETS to handle these types of problems.

Work was initiated on the computer-based fault-tree development program. The goal is to reduce the time and manpower required to translate the facility design and operation information into fault-tree logic. The initial criteria for the required computer code modules have been defined. It is anticipated that subcontractors will be used in various parts of the project, including development of the data-gathering system and adaptation of the generic sabotage fault trees for use in this code.

Contractual Support

During this period, Dikewood Industries completed their support activity for the facility characterization of the SNUPPS facility. A final report on their effort has been delivered to Sandia. This report contains systems descriptions, fault trees, location information, and miscellaneous information developed during the study.

Falcon R&D continued their work on generic fault trees for interconnected, multi-loop heat-removal systems. Trees for two- and three-loop closed systems with full interconnection have been developed. The SETS analysis to obtain the minimal cut sets has required the use of all available sophisticated solution techniques. The application of these new generic fault trees to the SNUPPS Auxiliary Feedwater System to verify their practical applicability will begin during January 1979.

PATH-GENERATION/SELECTION METHODOLOGY

In-House Activities

ADPATH Tests

Testing of a new code, ADPATH, for finding adversary paths (theft and/or sabotage) in a facility digraph was begun in November. ADPATH is designed to include facility digraphs in which the delay times and detection probabilities may depend on the adversary's direction of travel. This new code will supplement the code MINDPT, currently used in SAFE, to find sabotage paths in an undirected facility graph.

All of the facility graphs used to test MINDPT have been converted to facility digraphs, and the corresponding sabotage problems have been solved correctly by ADPATH. In addition, the initial design of ADPATH has been altered to shorten the call list and to make it easier to use. A set of theft problems has been devised to supplement the sabotage test problems and thereby provide examples of each type of adversary path problem.

EVALUATION METHODOLOGY

In-House Activities

Automation of System Evaluation

SAFE Demonstrations -- A demonstration of the SAFE methodology was presented to Jay Durst, NRC Office of Regulatory Research, during October. This demonstration covered the SAFE procedure from the digitization phase to path analysis. In addition, assistance was also given to B. Hatter and J. Bartlett, NRC Office of Nuclear Material Safety and Safeguards, in their preparation of a demonstration of SAFE to NRC staff members. Discussions concerning the equipment required by SAFE, the input data, and the organization and content of the presentation were held, and the facility digitization process and the SAFE analysis procedure were thoroughly reviewed. Also, a demonstration of the

possible use of a video camera and monitor system to be used during presentations of SAFE to a group was arranged. A visit was made to the Advanced Research Projects Agency (ARPA) to examine their Demonstration and Development Facility. The purpose of this visit was to determine what modifications would be required in order to use the ARPA facility for a live demonstration of SAFE to NRC personnel. A later visit was made to present the live demonstration of SAFE.

Various line printers that are compatible with the Tektronix 4051 have been examined in order to provide a recommendation to NRC as to what type of line printer would be useful at the Applications and Development Facility (ADF). One requirement for the line printer is that it have the capability to print from the Tektronix 4051 as well as from the Sandia NOS time-sharing system. The line printer would be useful to print out large data files from SAFE, SNAP, or other models instead of printing them at the terminal. Equipment currently in use at Sandia Laboratories includes a Texas Instrument Model 810 printer and a Tektronix 4641 printer. Both of these printers require a Tektronix 4051 Option 10 printer interface/RS232 printer interface.

SAFE Documentation -- The SAFE modules for which general descriptions have been documented include facility characterization, target identification, pathfinding, path evaluation, adversary neutralization, general SAFE input and output, and an example of an application of SAFE to a generic facility. In the application example, emphasis is placed upon the use of SAFE to gain information and insights about the facility and the dependence of the facility security upon specific parameters (barrier delays, probability of detection of a sensor, guard response time, etc.).

A flowchart which illustrates the execution of SAFE from the user's point of view is shown in Figure 1. It also shows the flow of control and makes clear what options are available and what events occur once an option is chosen. A second flowchart, which is system oriented, has been constructed but, because of its complexity, is not included in this

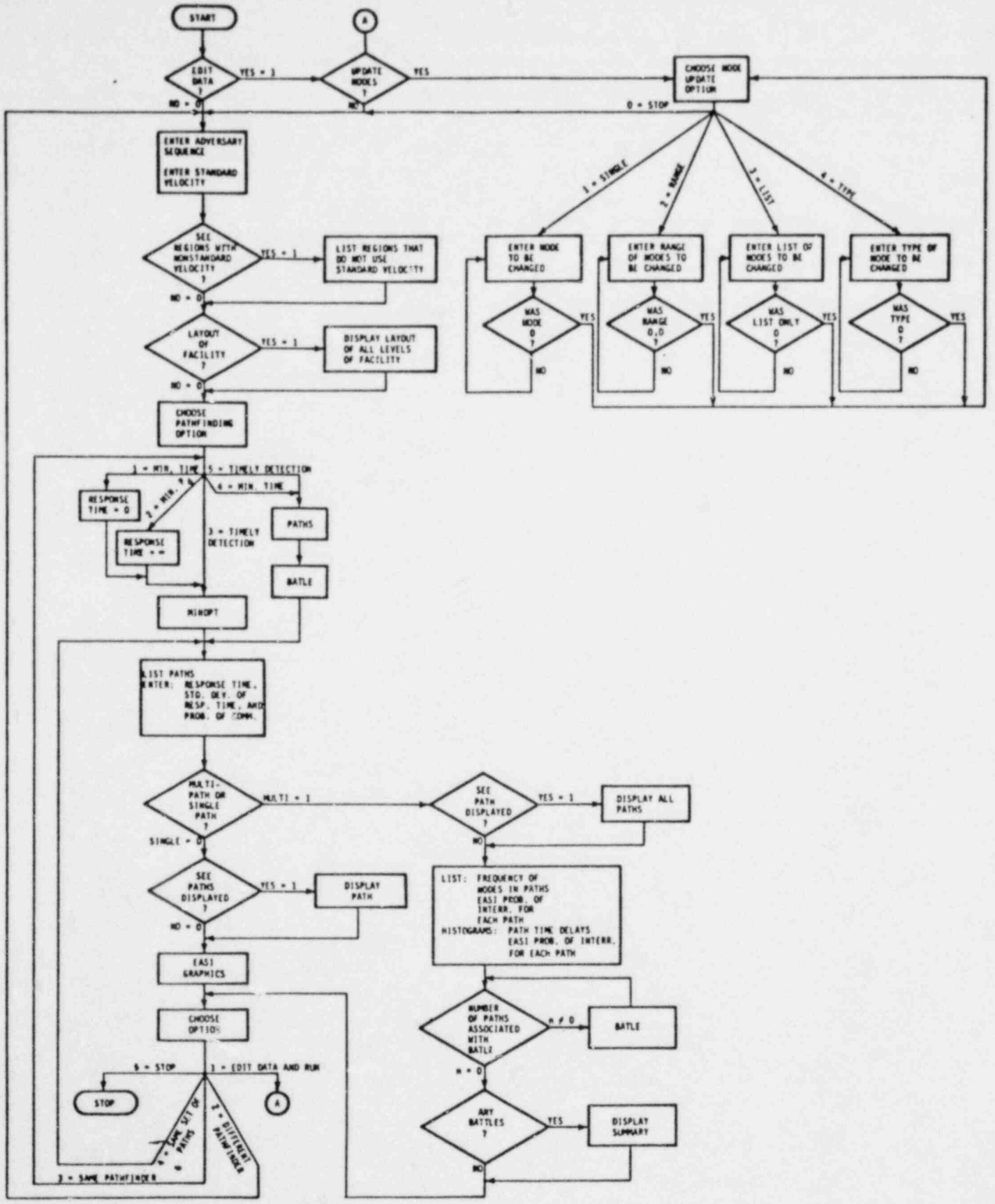

Figure 1. Flowchart of User's Options in SAFE

report. This flowchart shows the transfer of control from program to program, the use of data files, and the use of procedure file control variables.

Documentation of the SAFE computer codes continues. Comments have been added to these codes, and simplifying changes have been made. After changes are made to the code, it is necessary to verify that these changes have been made correctly.

SAFE Program Modifications -- The output of SAFE to a terminal was adjusted so that the output will fit within the 72 columns provided. This enhancement will allow output to be written on the Tektronix 4051 terminal without wraparound occurring. This change was made in anticipation of the demonstration to NRC staff members on a Tektronix 4051 terminal.

The pathfinding options of SAFE have been changed from computer subroutine names to descriptive names. For example, the interactive SAFE response

```
Choose Pathfinding Routine Wanted:
   1 = KSPTH
   2 = MINDPT
   3 = PATHS
```

has been changed to read

```
Choose Pathfinding Option Wanted:
Deterministic (MINDPT)
   1.  Minimum time over path
   2.  Minimum detection probability over path
   3.  Minimum timely detection
       (Detection with sufficient time for guard
       response)
Stochastic (PATHS)
   4.  Minimum time
   5.  Minimum timely detection
```

It was felt that these descriptive names were more understandable. To accomplish this change, program modifications were necessary in order to automatically perform the listed options.

Work related to the automation of region identification in SAFE is nearly completed. A network of computer codes has been written to perform this task, with minimal user assistance. At this time, the program offers the following capabilities:

1. Automatic transformation of data from the digitized facility into region data of the form required for interface with SAFE, and
2. User interaction to obtain a list of region information for verification, to delete superfluous regions, and to add stairwell-type regions where necessary to allow passage from one level to another (this is not performed automatically).

It is important to stress that the automation of this capability in SAFE makes the digitization phase all the more critical. Poor digitization can lead to improper formation of regions. The user must take care in digitizing and checking results after the region identification has been performed. If digitization errors result in incorrect formation of regions, it is the user's responsibility to recognize this deficiency, to correct the digitization errors, and to rerun the region identification program. Additional user capabilities will be added to SAFE to further assist the user.

The program has been tested on some example facilities and performs adequately. Tasks which once required hours of tedious work to accomplish can now be completed in minutes. This time saving may be especially helpful when SAFE is used in facility design. In this case, if the facility layout is modified, the region identification can be quickly redone. The sequence of events necessary for user implementation of the automatic identification of regions in SAFE is shown in Figure 2.

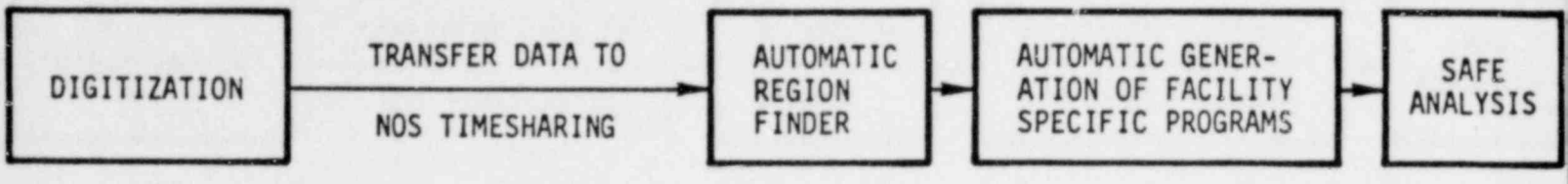

Figure 2. Block Diagram which Illustrates Automatic Region Finder in SAFE

Neutralization

Fixed-Site Neutralization Model -- A document which describes the performance data in the GTS example which was constructed for the Fixed-Site Neutralization Model (FSNM) has been completed. The guard force structure and tactics currently being used in SNAP are being modeled so that a comparison can be made between SNAP and FSNM.

Efforts to convert the FSNM code to the CDC 7600 computer continued during this reporting period. Previously, the FSNM files had been brought up on the NOS system and transferred to the 7600 system for compiling and attempted loading. During this period, modifications were made to use larger core memory and to load the two preprocessors and the FSNM Program on the 7600. As a result of these modifications, it appears almost certain that the code can be loaded onto the CDC 7600. In addition, the necessary data files and control sequences needed for testing the entire system have been completed, and testing on all phases of the system are underway.

Contractual Support

Neutralization

Safeguards Network Analysis Procedure -- Developments to the Safeguards Network Analysis Procedure (SNAP) focused on the following areas:

1. The implementation of the Guard Tactics Simulation (GTS) engagement model in SNAP,
2. The incorporation of new force-based statistics,

3. The implementation of tamper alarm capabilities,
4. An investigation of the question of detail in SNAP facility models,
5. The application of SNAP to a GTS scenario, and
6. The implementation of a 72-column output capability in SNAP.

A preliminary design for the implementation of the GTS engagement model in SNAP has been completed. This design required a definition of new data input fields as well as alternative processing schemes. The new model will be available as an alternative to the Sandia Brief Adversary-Threat Loss-Estimator (BATLE) engagement model currently available in SNAP. The data input modifications were designed to be incorporated in such a manner that the current engagement capability input is a subset of the new capabilities and will be selected by default.

Additional force-based statistics have been incorporated into SNAP. The following statistics are reported for both guard and adversary forces:

1. The probability that a particular force was the first casualty among all forces of the same type,
2. The probability that a particular force was the first casualty among all forces of the same type given the safeguards system fails, and
3. Given user specified combinations of forces, the probability that all forces within a particular combination were casualties (multiple combinations may be specified).

The additions of these statistics to SNAP will provide the user with force-specific information and allow a further evaluation of guard policy alternatives.

Tamper-alarms are defined as adversary detection devices which detect any attempt to modify or disable another adversary detection device. Tamper alarms have been incorporated in SNAP through an addition to the SENSOR element. The user may specify that a tamper alarm has

been placed on a sensor, logic point, or monitor. If the device is disabled, the tamper alarm will be triggered. The guard force may then make decisions based on the type of alarm triggered and respond accordingly.

The exploration of the question of detail in SNAP facility models continues. An analysis has been performed regarding the incorporation of various detail levels in SNAP models, and statistical information has been collected regarding the significance of the inclusion of these levels. The effects of detail appear to be manageable in SNAP if the user is willing to assume that the location of any particular force at a specific time is uniformly distributed across the area represented by a SNAP facility model component. This assumption is encompassed in the five-metre hex design in GTS.

In addition to the statistical analysis performed, the addition of detail was evaluated from an intuitive standpoint. Modeling procedures have been identified, and the process by which detail should be included in SNAP facility models will be described.

The implementation of the 72-column output capability in SNAP has been completed. With this addition, the outputs of SNAP are now available on all types of data terminals regardless of the width of the display screen.

Work plans for the coming month include

1. The implementation of the GTS engagement model,
2. The formalized specification of findings in the analysis of the detail question, and
3. The development of the GTS application.

Initial work has been completed on the development of a SNAP Short Course. Requirements for the course have been identified, and an initial course outline has been completed. Tentatively, the course is scheduled for 28 February to 2 March 1979. The course will be presented at Sandia Laboratories, Albuquerque.