NUREG/CR-1246 (1 of 4)
SAND79-2247/1
RS

SAFE Users Manual

Volume 1: Introduction to SAFE

Leon D. Chapman, Dennis Engi, Louann M. Grady, Constantine Pavlakos

Printed August 1981

Sandia National Laboratories

2900-Q(3-80)

Prepared For

U.S. NUCLEAR REGULATORY COMMISSION

NOTICE

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1246 (1of4)
SAND79-2247/1
RS

SAFE USERS MANUAL
VOLUME I: INTRODUCTION TO SAFE

Leon D. Chapman, Dennis Engi,
Louann M. Grady, and Constantine Pavlakos

Date Published: August 1981

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

Prepared for
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1060

Contributors

Harold A. Bennett
Charlene P. Harlan
Bernie L. Hulme
Dallas W. Sasser
G. Bruce Varnado

ABSTRACT

An overview of the Safeguards Automated Facility Evaluation (SAFE) method and its application to nuclear facility safeguards is presented. The evolution of SAFE is described, and background information on early first- and second-generation safeguards evaluation models is provided. The ability of SAFE to function as a global safeguards effectiveness evaluation method is examined, and the roles which the individual phases of a physical protection evaluation (facility characterization, facility representation, component performance, adversary path analysis, and effectiveness evaluation) play in an application of SAFE to a nuclear facility are detailed.

PREFACE

This volume of the SAFE Users Manual presents a complete overview of the Safeguards Automated Facility Evaluation (SAFE) method and its application to nuclear facility safeguards. To provide the user with a better understanding of SAFE and the philosophical rationale behind its development, Section 2 of this volume contains a description of the evolution of SAFE. Two early, first-generation, scenario-based safeguards evaluation models, the Forcible Entry Safeguards Effectiveness Model (FESEM) and the Insider Safeguards Effectiveness Model (ISEM) as well as two second-generation, scenario-based models, the Fixed-Site Neutralization Model (FSNM) and the Safeguards Network Analysis Procedure (SNAP), are described. The ability of SAFE to surmount both the technical and philosophical limitations of scenario-based safeguards models with respect to modeling global safeguards effectiveness is examined.

Section 3 details the phases involved in the physical protection evaluation process: (1) facility characterization, (2) facility representation, (3) component performance, (4) adversary path analysis, and (5) effectiveness evaluation. The parameters required for each phase, the interrelationship of the phases, and the manner in which each contributes to the overall SAFE evaluation process are described. Finally, the role of SAFE as an aid in the decision-making process is briefly considered in Section 4.

This volume is the first in a series of four volumes which comprise the SAFE Users Manual. This manual provides sufficient information for the uninitiated physical protection system analyst to gain a working knowledge of SAFE. For further information on SAFE, the reader is referred to Volume II: Method Description, which presents a detailed description of the SAFE evaluation process, Volume III: Example Application, which presents an application of the SAFE method to an example facility, and Volume IV: Computer Programs, which presents simple program flowcharts, a brief description of each program, and a complete listing of the programs used in SAFE.

CONTENTS

Section		Page
1	INTRODUCTION	11
2	THE EVOLUTION OF SAFE	13
	2.1 Early Scenario-Based Models	13
	2.2 Second-Generation Scenario Models	14
	2.3 A Global Evaluation Technique	15
3	SAFE EVALUATION PHASES	19
	3.1 Facility Characterization	20
	3.2 Facility Representation	21
	3.3 Component Performance	24
	3.4 Adversary Path Analysis	26
	3.5 Effectiveness Evaluation	29
4	SUMMARY	33
	4.1 Overview of SAFE Computer Programs	33
	4.2 Commentary on the Use of Models	35
REFERENCES		37
INDEX		39

ILLUSTRATIONS

Figure		
1	Evolution of SAFE	13
2	Physical Protection Evaluation Process	19
3	Input/Output of the SAFE Facility Characterization Phase	20
4	Input/Output of the SAFE Facility Representation Phase	21
5	Facility Blueprint--Level 1	22
6	Facility Layout Digitization	23
7	Facility Layout--Level 1	24
8	Facility Layout--Level 2	24
9	Input/Output of the SAFE Component Performance Phase	25
10	Input/Output of the SAFE Adversary Path Analysis Phase	26

ILLUSTRATIONS (Continued)

Figure		Page
11	Exterior Adversary Path into Facility (Level 1)	28
12	Interior Adversary Path to Target (Level 2)	28
13	Input/Output of the SAFE Effectiveness Evaluation Phase	29
14	Three-Dimensional EASI Graphics Plot	31
15	SAFE Evaluation Procedure and Computer Programs	33

TABLE

Table		
1	Global Results for All Type I Targets (7-Minute Response)	30

SAFE USERS MANUAL
VOLUME I: INTRODUCTION TO SAFE

1. INTRODUCTION

The development of models to aid in the evaluation of physical protection systems at nuclear facilities was in progress at Sandia National Laboratories as early as 1974. This work has been sponsored principally by the U.S. Nuclear Regulatory Commission (NRC). These models were developed 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 existent facilities and for designing new facilities.

The Safeguards Au[illegible] Facility Evaluation (SAFE) method is an evaluation process con[illegible]ng of operational phases for facility representation, component performance, adversary path analysis, and effectiveness evaluation. SAFE combines these phases into a continuous stream of operations. The technique has been implemented on an interactive computer time-sharing system and makes use of computer graphics for the processing and presentation of information. Using this technique, a global evaluation of a safeguards system can be provided by systematically varying the parameters that characterize the physical protection components of a facility to reflect the perceived adversary attributes and strategies, environmental conditions, and site operational conditions.

2. THE EVOLUTION OF SAFE

2.1 EARLY SCENARIO-BASED MODELS

Figure 1 depicts the evolution of SAFE. Two of the first safeguards evaluation models which were developed are the Forcible Entry Safeguards Effectiveness Model (FESEM)[1] and the Insider Safeguards Effectiveness Model (ISEM).[2] FESEM and ISEM employ Monte Carlo techniques to simulate a group of adversaries attacking a nuclear facility. The principal difference between these two models lies in the hypothesized threat they are structured to address. FESEM was structured to consider primarily adversaries who do not have authorized access to the facility (outsiders), while ISEM focuses on adversaries who do have authorized access (insiders).

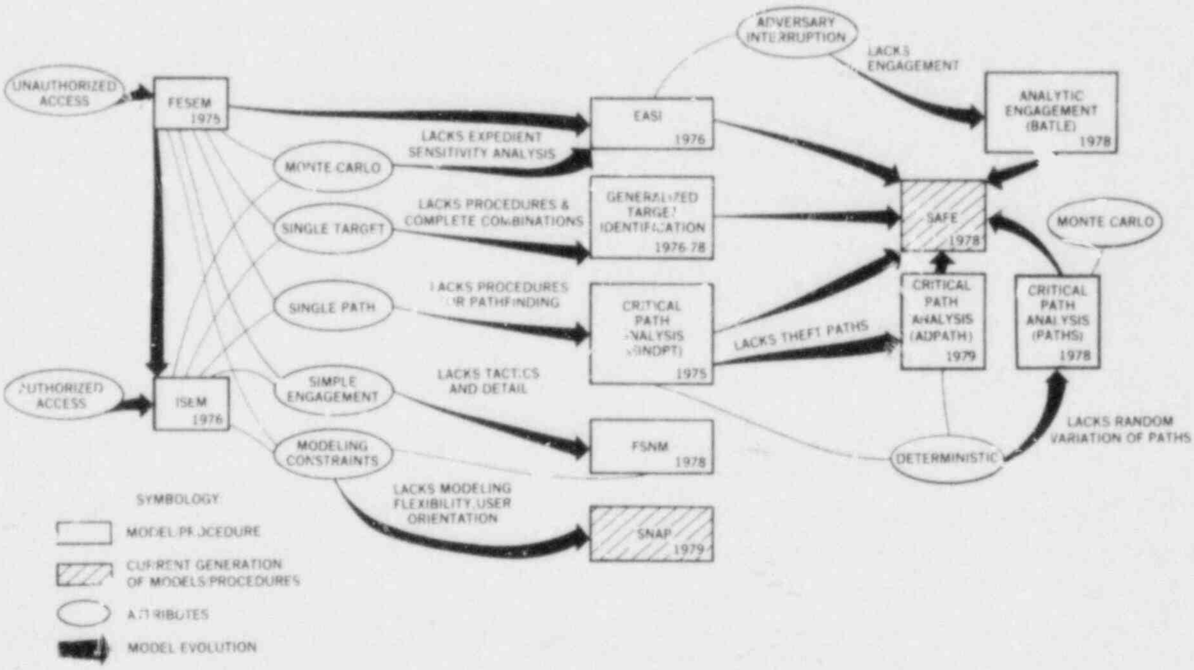

Figure 1. Evolution of SAFE

Experience gained through the application of FESEM and ISEM provided the impetus for further safeguards methodology development. There were essentially two schools of thought regarding the most fruitful direction for further developmental work in the 1975 to 1976 time frame. On the one hand, it was clear that the single-scenario orientation of FESEM and ISEM was not amenable to an evaluation of safeguards systems considered in their entirety. That is, an evaluation of the effectiveness of a safeguards system in countering individual adversary scenarios merely reflects the ability (or inability) of the system to deal with these scenarios--it is likely to imply little about the safeguards system as a whole. Consequently, a need for a global approach to the problem of evaluating safeguards system effectiveness was identified. At the other extreme, both FESEM and ISEM were criticized for not including a sufficient amount of detail in individual scenarios. This criticism was directed primarily toward the inability of these models to represent complex tactics that might be used by the adversaries as well as the security force.

In order to satisfy both of these concerns, developmental activities proceeded along two lines. One area of work centered on the development of detailed scenario models and resulted in a set of second-generation scenario models that can explicitly represent quite complex tactics. The other area of work focused on development of a global approach to safeguards effectiveness evaluation. The result of the global effort is an interlinked collection of analytical techniques which can be used to evaluate the effectiveness of the entire safeguards system. The following two subsections describe in greater detail the products of these two developmental activities.

2.2 SECOND-GENERATION SCENARIO MODELS

The primary concern in the development of the second-generation scenario models was enhancement of the capability to represent complex tactics. The goal of enhanced capability was pursued through the development of two separate scenario models. One of these models, the Fixed-Site Neutralization Model (FSNM),[3] utilizes tactical procedures which are internal to the model logic and require only a minimal amount of user input related to the tactics. The other scenario-based model, the Safeguards Network Analysis Procedure (SNAP),[4] is the antithesis of FSNM with respect to the representation of tactics. SNAP requires explicit user input to represent tactics. Both models employ Monte Carlo techniques to simulate randomness in the scenario. Output from the models includes estimates for a variety of system performance measures.

With the advent of SNAP, the majority of the criticism directed at the limitations pertaining to the representation of detail in the early scenario models (FESEM and ISEM) was answered. SNAP can be used to represent quite complex tactical situations and, as a consequence, lends credibility to the evaluation of individual scenarios. In the context of "vulnerability analyses," SNAP is a valuable tool in that it can provide insights into the strengths (or weaknesses) of the safeguards system's ability to defend against a predefined adversary scenario. However, as previously observed, the analysis of a single scenario is likely to offer little in the way of global insights with respect to the safeguards system. Moreover, even without considering analyst time, a detailed analysis of a sufficient number of scenarios (by any scenario model) in order to gain these global insights is unlikely to be computationally tractable. In addition, it is not obvious just what is implied by "a sufficient number of scenarios." To address these inherent limitations, which are inexorably linked to any scenario-based technique, a global approach to the evaluation of safeguards effectiveness was developed.

2.3 A GLOBAL EVALUATION TECHNIQUE

The principal limitations of the scenario-based models with respect to their applicability to a global safeguards effectiveness evaluation were observed to be of a philosophical as well as a technical nature. First, on the technical level, the scenario-based models involved relatively complex Monte Carlo simulation techniques. In addition to the significant amount of computer time necessary to replicate a sufficient number of times to obtain statistical stability, the analyst time required for preparation of the input for a single scenario can be excessive. The input data requirements normally increase with model detail. Perhaps more importantly, the modeling philosophy of the scenario-based models does not include the creation or generation of adversary scenarios. It is difficult to determine which and how many scenarios are necessary for evaluation to assure a comprehensive analysis of the physical protection system.

The SAFE method evolved as a result of efforts to overcome the limitations described above. The technical limitations were addressed by developing a set of analytical techniques that is computer-time efficient and by structuring a highly user-oriented approach that is analyst-time efficient. On the philosophical level, techniques for generating "optimal" adversary scenarios were developed.

The generation of adversary scenarios is based on selecting optimal adversary paths into the facility, to a target,* and (in the event of theft) exiting the facility. Currently, SAFE uses one of three measures for adversary pathfinding: (1) minimum adversary task time, (2) minimum adversary detection probability, and (3) minimum probability of interruption (sometimes called timely detection) of the adversary. Within SAFE, these measures can be either deterministic[5] or stochastic.[6] In effect, the interruption measure generates paths which minimize the probability that the security force can confront (or interrupt) the adversary. This implies that the system must detect the adversary with sufficient time remaining in the adversary's path for the security force to respond and confront him prior to the completion of the scenario. The output of the adversary path analysis is a collection of ordered sets of node identifiers that represent physical paths in the facility which are "critical" in terms of the pathfinding measure being used. This information is a portion of the input to the effectiveness evaluation phase in SAFE.

Effectiveness evaluation for a given path can be decomposed into two major parts: interruption and neutralization. The path is "evaluated" by first determining the probability that the adversary will be interrupted and then determining the probability that the adversary will be neutralized or defeated by the security force. These two probabilities can be multipled together to yield the total probability that the physical protection system will be successful in defending against the adversary along the path under consideration.

The Estimate of Adversary Sequence Interruption (EASI)[7] model is an analytical technique which is used in the effectiveness evaluation phase to compute the probability that the adversary will be interrupted. EASI focuses on the adversary path and requires information related to the probability of detecting the adversary, the probability of communication with the security force, the delays along the adversary path, and the response time of the security force. The output of

---

*Target--For sabotage, a target may be defined as a source of special nuclear material (SNM) that could be released off-site to endanger the public or a vital component(s) which, if compromised, would result in radioactive release of SNM beyond the facility boundaries. For theft, a target will normally be defined as a source from which SNM can be obtained.

EASI is an estimate of the probability of adversary interruption along the specified path, i.e., the probability that the security force arrives at a point along the adversary's path prior to the time at which the adversary passes through that point.

The Brief Adversary Threat Loss Estimator (BATLE)[8] model is an analytical technique that is used to estimate the probability that the adversary is neutralized by the security force. The information required by BATLE includes the number of combatants in each force, characteristics describing each combatant, the distance between forces, environmental conditions, and reinforcements for both the adversaries and the security force. A primary output of BATLE is the probability that the adversary is neutralized by the security force. This "neutralization probability" is then multipled by the "interruption probability" to yield the total probability of system win of the physical protection system for the path in question.

Capabilities for effectiveness evaluation can be utilized in either a single- or multi-path mode. During a single-path evaluation using EASI, the probability of interruption is calculated and the user may request two- or three-dimensional plots which show the probability of adversary interruption or the probability of system win as a function of one or two of the other input variables.[9] Based on the probability of interruption, these graphs illustrate sensitivities related to upgrading the facility. The multi-path option displays, in tabular form, the probability of interruption, the traversal time of each path, and the frequency at which nodes appear in the set of critical paths. The multi-path evaluation identifies paths that are particularly vulnerable and, thus, are candidates for study by the single-path mode or by elaborate scenario-based models such as those previously described.

The global approach used in SAFE to estimate probability of interruption and probability of neutralization provides the analyst with three valuable capabilities. First, SAFE can be used to obtain a global lower bound on probability of interruption that is a figure of merit, not just for a path or a set of paths, but for the whole facility. Second, SAFE can be used to evaluate sensitivities to a range of parameter values so that facility upgrades can be suggested and evaluated. Finally, SAFE can develop critical paths (scenarios) to be studied in more detail with scenario-based models.

3. SAFE EVALUATION PHASES

Any physical protection evaluation process should include a set of functions to provide the capability to account for facility characterization, facility representation, component performance, adversary path analysis, and effectiveness evaluation, as shown in Figure 2. SAFE combines the latter four of these phases into a continuous stream of highly automated operations. SAFE has been implemented on an interactive computer time-sharing system and makes use of computer graphics for the processing and presentation of information. Using SAFE, a global evaluation of a safeguards system can be provided by systematically varying the parameters that characterize the physical protection components of a facility to reflect the perceived adversary attributes and strategies, environmental conditions, and site operational conditions. Several alternative paths to all targets in the facility should be examined under different environmental and adversary conditions or threats. As noted in Figure 2, a different set of targets could result from various operational conditions, such as full power or cold standby. Then, an analysis for the various operational conditions and target

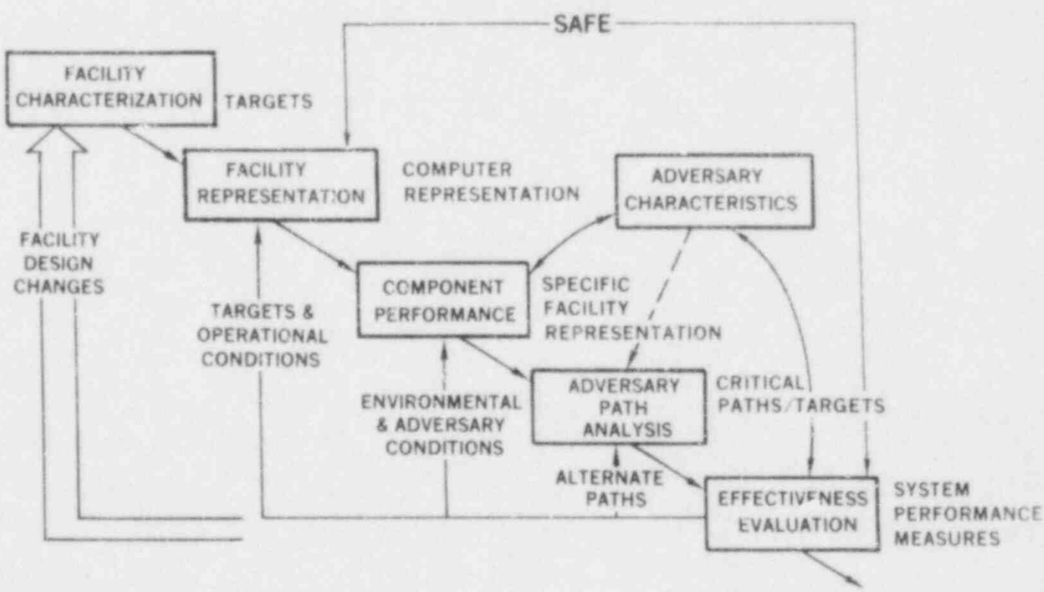

Figure 2. Physical Protection Evaluation Process

combinations over sets of environmental and adversary conditions for alternative adversary paths to each target would have to be performed for a comprehensive evaluation of the facility.

3.1 FACILITY CHARACTERIZATION

The first step in the evaluation process is the facility characterization phase, which is illustrated in Figure 3. The objective of this phase is to determine six essential facility characteristics: (1) the facility layout characteristics, (2) the targets and vital areas,* (3) the operational conditions, which include such items as maintenance conditions, normal operation, and emergency conditions, (4) the environmental conditions that are relevant to the specific site, i.e., heavy rain, snow, or extreme cold, (5) identification of the components of the physical protection system and their location, and (6) the characteristics of the security force, which include number of guards, types of weapons, routing of patrols, and other specific characteristics. All of this input information for SAFE will make possible a thorough analysis.

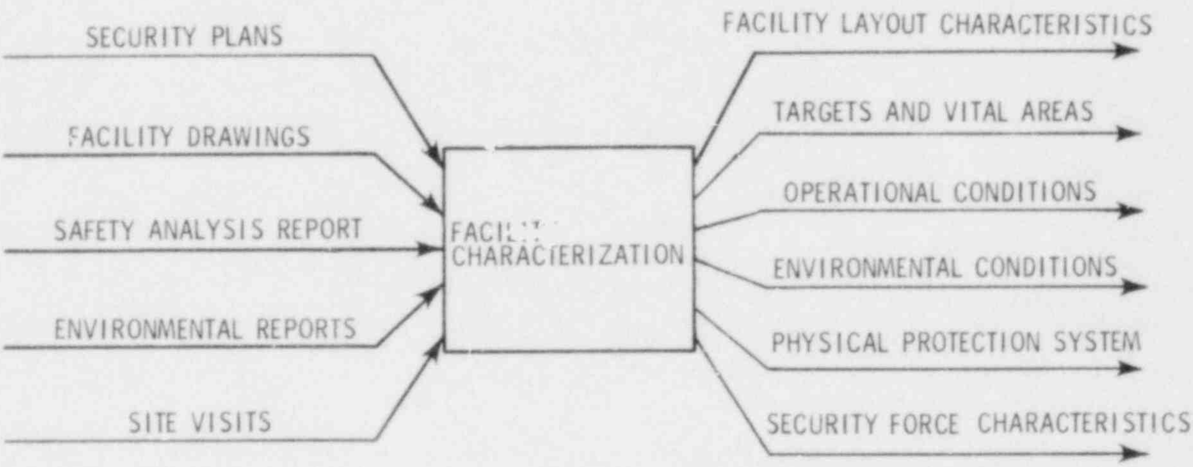

Figure 3. Input/Output of the SAFE Facility Characterization Phase

The input to the facility characterization phase includes the various security plans that have been developed for the facility, the facility drawings, the safety analysis report, and the environmental reports for the facility. This information should be supplemented with information gained from site visits, as required.

*Vital area--A vital area is a location in a nuclear facility at which a sabotage or theft event can be accomplished.

Essential output of the facility characterization phase includes the various facility layout characteristics, e.g., barriers and access points. The targets and vital areas are identified for specific operational conditions. Three additional sets of information can be obtained from this process: (1) specific site-relevant environmental conditions from the environmental reports, (2) the description and location of the physical protection system components, and (3) the particular security force characteristics which are available from the security plans.

The output of this phase is obtained through careful study of the available resources. It is a step which essentially requires the analyst to acquire the necessary information for the analysis and make clear the input data and assumptions used. For complex nuclear power plants, fault tree techniques are available to assist the analyst in locating the targets and vital areas.[10,11]

3.2 FACILITY REPRESENTATION

The second phase in the evaluation process is facility representation. The objective of this phase is to provide a basis for the evaluation procedure through a computer representation of the facility layout. This phase provides an explicit record of the analyst's assumptions regarding the facility representation. As shown in Figure 4, the input to this phase is a subset of the output from the facility characterization phase: the facility layout characteristics and the targets and vital areas for specific operational conditions. The output of the facility representation phase is a computer representation of the facility to be used in the analysis. For example, a facility layout or blueprint, as shown in Figure 5, shows a chain-link fence around the outside of the facility and main reactor building. In addition, there are several ancillary buildings around the area. It is

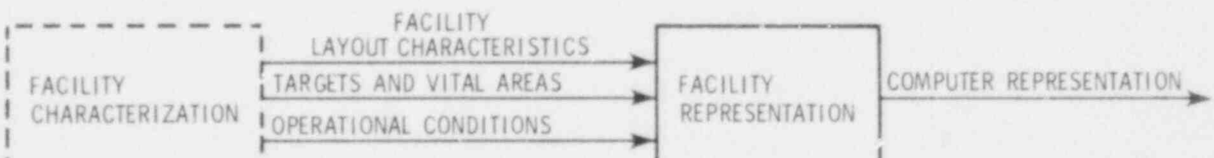

Figure 4. Input/Output of the SAFE Facility Representation Phase

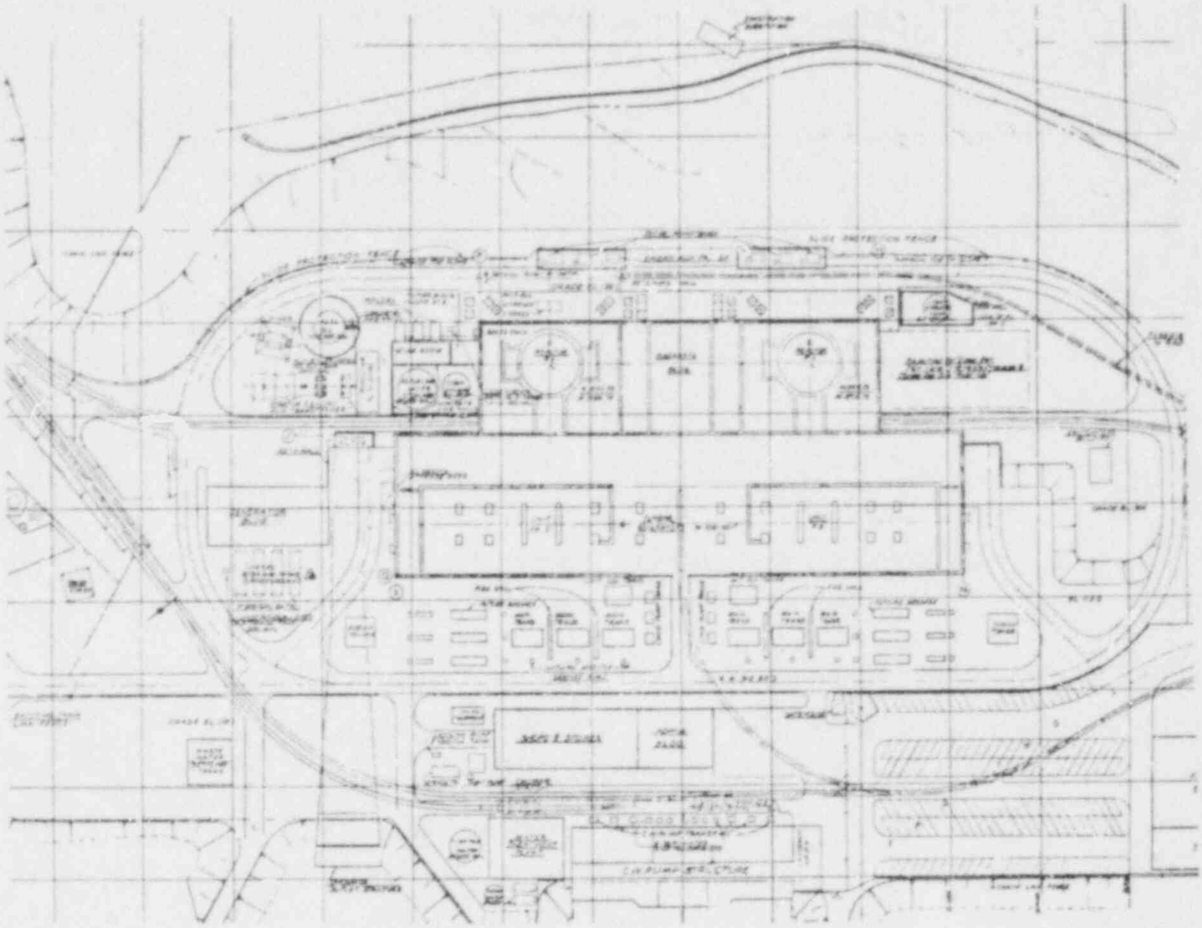

Figure 5. Facility Blueprint--Level 1

not essential that all of this information be translated into the computer representation of the facility, but the key elements which affect adversary or guard movement must be included.

More specifically, the input required for this procedure includes (1) the facility layout characteristics that comprise the principal barriers and obstructions to any adversary movement, (2) all points of potential ingress and egress by the adversary (this might include such items as windows, doors, potential adversary penetration points of boundaries, barriers, fences, walls of the buildings, etc.), and (3) floor levels and their interconnection through stairwells and ventilation ducts. The specific targets and vital areas for a set of operational conditions are also required.

The facility representation phase is accomplished through a digitizing process, illustrated in Figure 6, in which the analyst uses a

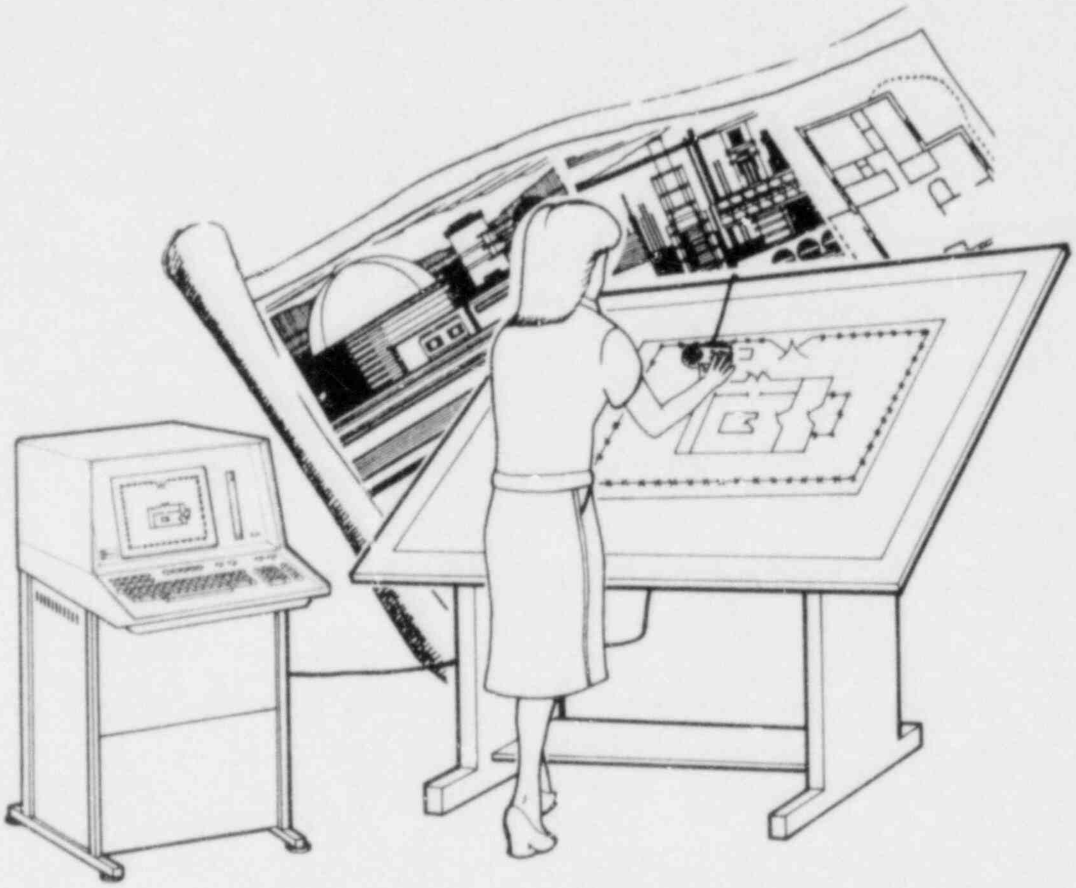

Figure 6. Facility Layout Digitization

digitizing table and a cross-hair cursor to send x,y-coordinates of the required locations from the blueprints to the computer. The analyst simply traces over the essential or key features of the blueprints and obtains a corresponding one-to-one computer graphics representation. The result of the process is a simplified facility drawing for the overall facility. Figure 7 illustrates the result of digitizing the blueprint shown in Figure 5. This drawing represents the first (ground) level of the facility, i.e., the chain-link fence and the major buildings inside the fence. Figure 8, which represents part of the interior of the building (Unit 2), is designated as Facility Layout--Level 2. The diamonds represent potential sabotage targets, and the triangles represent stairwells that join one floor to another.

Once the facility has been digitized in order to represent the important features, the facility data are put into the form of an undirected graph, which is a network of nodes and arcs. In the graph, nodes represent barrier penetrations and targets, and arcs represent

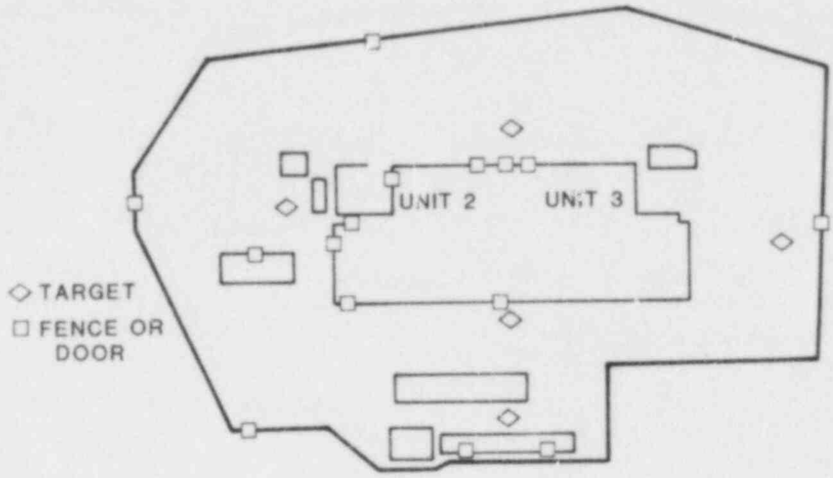

Figure 7. Facility Layout--Level 1

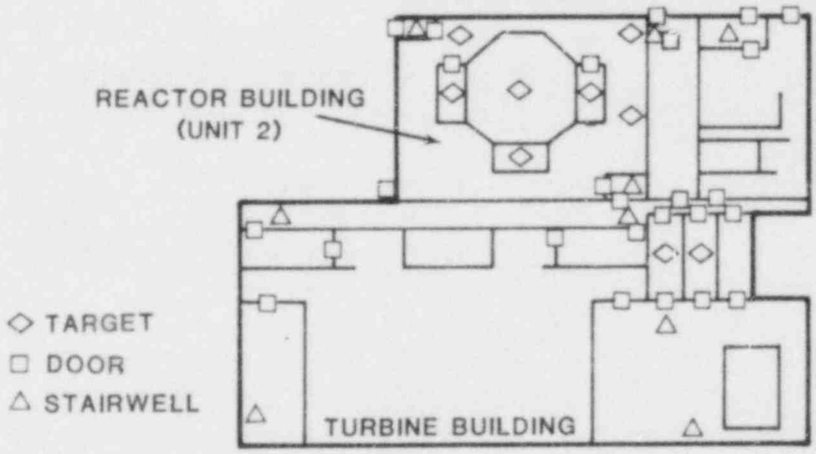

Figure 8. Facility Layout--Level 2

crossing times between barriers. The graph will be the actual model of the facility to be used as input to the pathfinding codes. The transformation from the digitized representation to the graph (except for the description of how stairwells on different levels are connected) is performed by a computer program.

3.3 COMPONENT PERFORMANCE

The next step in the SAFE process involves setting the component performance of each of the physical protection system components. The objective of this phase is to base performance of both hardware and personnel upon relevant sets of environmental and adversary conditions for the specific site being evaluated. As illustrated in Figure 9, the input required for this phase is the computer representation that was produced by the facility representation phase. In addition, the facility characterization phase provides a description of the physical protection system components and the site-relevant environmental conditions. This information is coupled with specific adversary characteristics so that a specific component performance that is relevant to the environment and the threat being considered can be determined.

The component performance characteristics that must be provided include penetration time delays for barriers, probabilities of detection for sensors, adversary and security force travel velocities, times to travel between levels of the facility, time required for the security force to respond to an alarm, and the probability that the security force can be alerted when an alarm occurs (the reliability of a facility's communication system). These values can vary for different environmental and site conditions and for different adversary attributes.

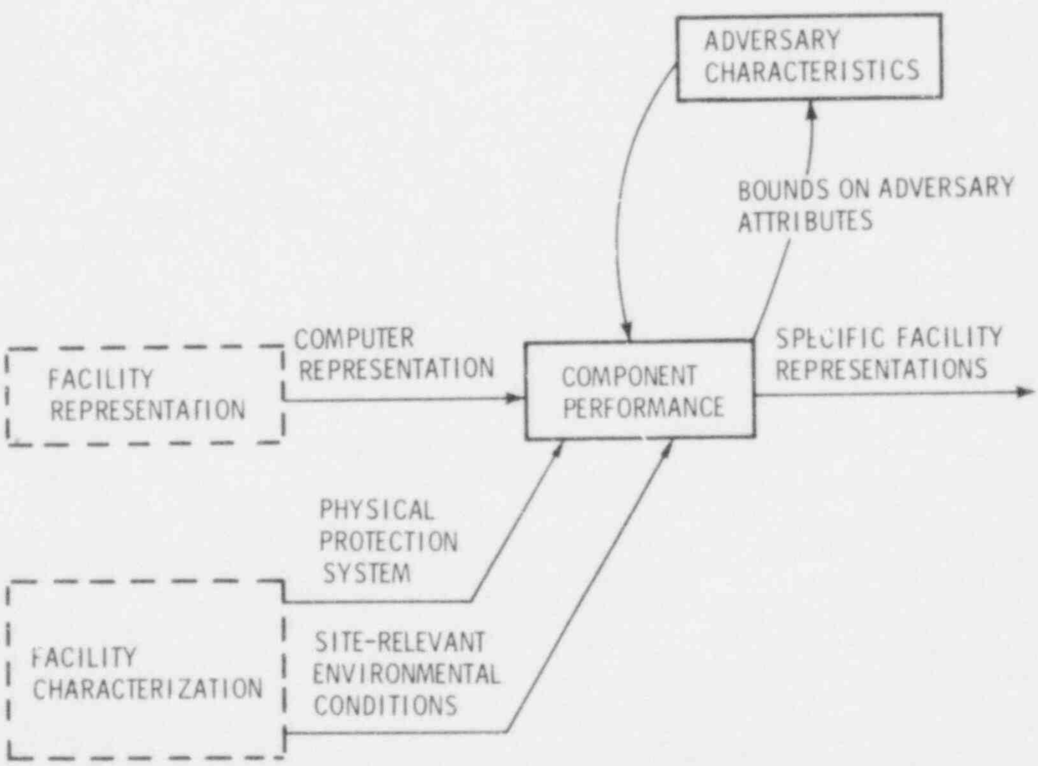

Figure 9. Input/Output of the SAFE Component Performance Phase

Through the use of these types of component performance assignments, the analyst can set specific bounds on component performance, while directly coupling this information to adversary attributes and environmental conditions. A worst-case component performance can be considered in terms of how the adversary could defeat the system and, from this information, bounds on adversary attributes can be set.

In summary, the component performance phase provides a method of documenting and communicating the analyst's input data assumptions. It also provides the basis for the effectiveness evaluation since component performance is based on a specific set of operational, environmental, and adversary conditions. By providing bounds on specific adversary attributes, the analyst is not required to consider every scenario, but, in a more global sense, a bound for the worst-case adversary scenarios is determined.

3.4 ADVERSARY PATH ANALYSIS

The next phase in SAFE is the adversary path analysis. The objective of this phase is to provide a systematic procedure for generating meaningful adversary paths for subsequent evaluation.

In the adversary path analysis process shown in Figure 10, the input from the component performance phase is a specific facility representation in terms of the digitized facility. The facility and physical protection system are represented by a graph of nodes and

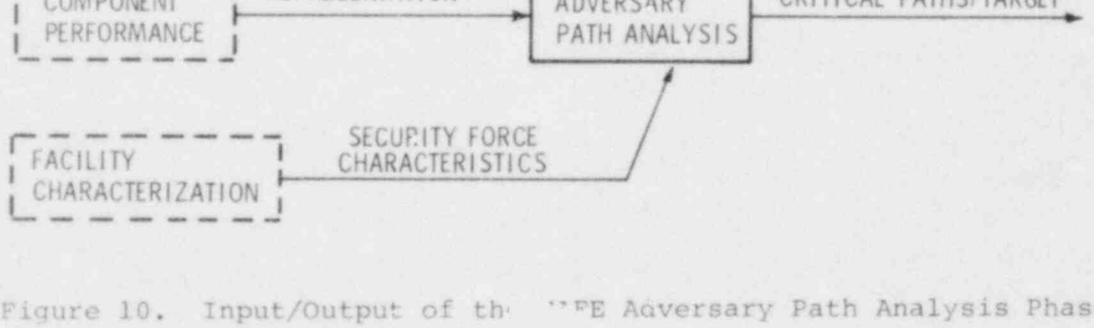

Figure 10. Input/Output of th ''FE Adversary Path Analysis Phase

arcs. The security force characteristics that are available for the interruption capability are obtained from the facility characterization phase. Interruption necessitates detecting the adversary with sufficient time to respond with a security force to confront the adversary prior to completion of his mission.

Critical adversary paths are automatically generated by SAFE to each potential target based on certain adversary characteristics. The output is a critical set of paths for each designated target within the facility. Figures 11 and 12 illustrate this output on the digitized facility layout. The nodes (squares) on the chain-link fence at the perimeter of the facility represent possible points where the adversary could penetrate the fence. The nodes (squares) on the building represent points where the adversary could enter through a door or penetrate a wall barrier. The target nodes are represented by diamonds. Each of the nodes is assigned a time for penetration and a detection probability in the component performance phase. Based on this information, the most critical paths to each target within the facility are found.

Figures 11 and 12 illustrate one path in which the adversary comes through the chain-link fence, traverses the open area, and enters a building door. The adversary then goes inside the building, through a stair door, and down the hall through two more doorways to a target. This path represents the route which the adversary could traverse to sabotage the facility, minimizing the likelihood of his being interrupted by the security force.

The various pathfinding algorithms used to identify critical paths provide a capability for examination of several alternative adversary strategies. For instance, the analyst can consider a scenario in which the adversary tries to minimize his total time by using force to penetrate barriers as rapidly as possible in order to strike the target. The analyst can also choose to determine the most critical paths to each target in terms of smallest probability of detection for the adversary. This would represent a scenario in which the adversary employs a stealth or deceit tactic. The combination of these two measures in terms of minimum interruption probability provides a more complete measure. In this case, the concern is to detect the adversary and to couple that detection with sufficient delay time to permit the security force to respond and confront the adversary before he has accomplished his mission. Use of this pathfinding measure produces a

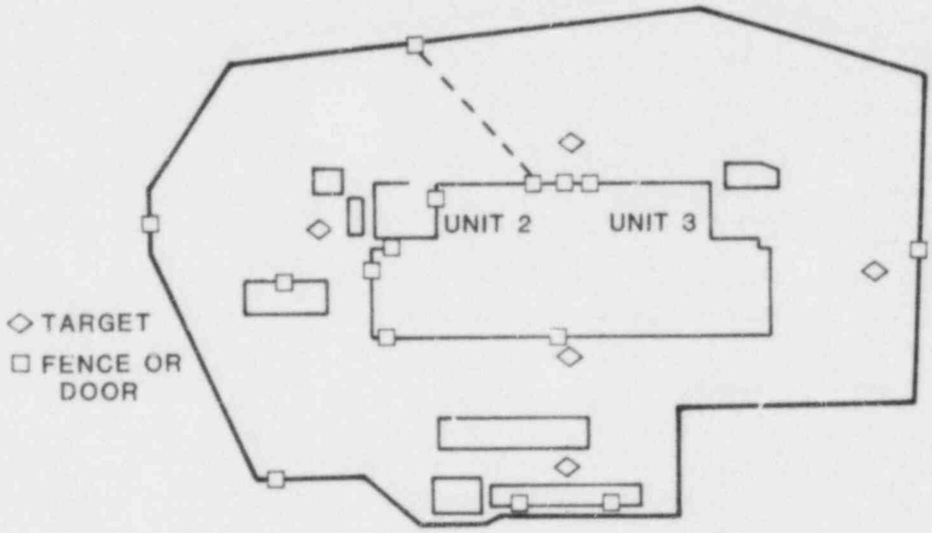

Figure 11. Exterior Adversary Path into Facility (Level 1)

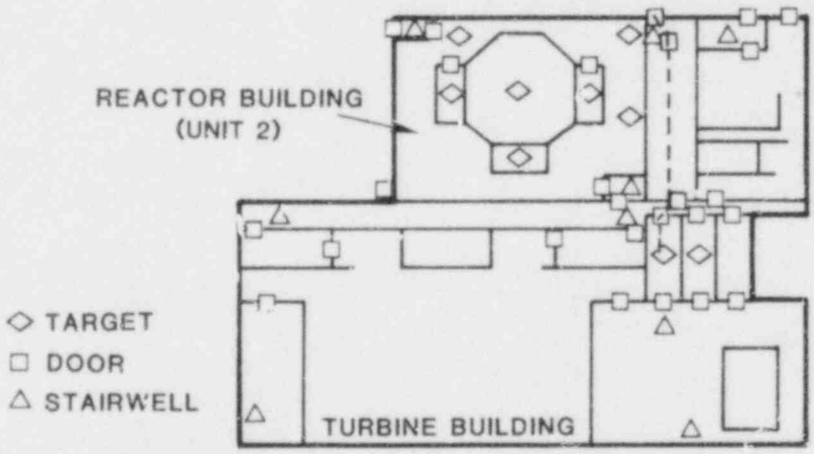

Figure 12. Interior Adversary Path to Target (Level 2)

critical path which combines adversary tactics of force, stealth, and deceit--the most stressful situation.

In summary, the adversary path analysis forms a basis for bounding the adversary strategies, attributes, and actions. It reduces, to a manageable set, the enormous number of adversary paths in a complex, multilevel facility. Only the "critical paths" to each target are generated. Typically, if every possible path to a target in the facility being considered were generated, the number of distinct paths could exceed the ability of current generation computers to exhaustively enumerate the paths; therefore, efficient, comprehensive, mathematical algorithms have been developed to find only the critical paths to each of the identified targets. In a matter of a few seconds of computer time, critical paths can be generated to 30 or 40 targets within a complex facility.

3.5 EFFECTIVENESS EVALUATION

The last phase of the SAFE evaluation process is the effectiveness evaluation. The objective in this phase is to provide meaningful aggregate measures of physical protection performance for various critical paths. Inputs to the effectiveness evaluation are obtained primarily from the adversary path analysis phase and involve at least one critical path to each target within the facility. As noted in Figure 13, the characteristics of the security force which involve the neutralization capabilities (the specific types of weapons, number of

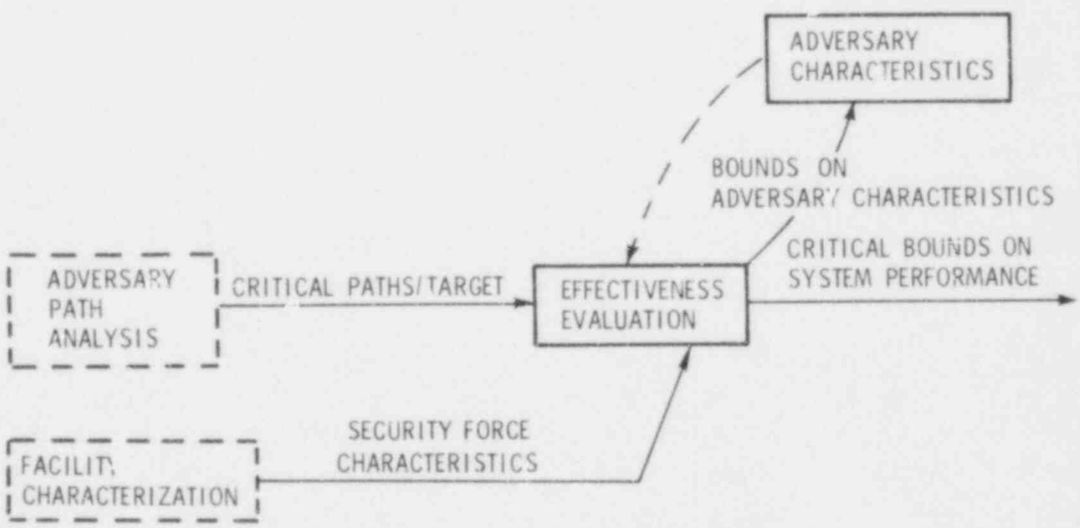

Figure 13. Input/Output of the SAFE Effectiveness Evaluation Phase

guards, their training, whether or not they have cover, etc.) are obtained from the facility characterization phase.

As an illustrative output of this process, part of the global results that were obtained from a facility is shown in Table 1. A response time of 7 minutes to each target has been assumed for three guards, and the targets have been designated in Column 1 by the node identification labels, 221, 440, etc. A ranking index has also been calculated that indicates which of these targets is the most attractive in terms of the adversary's attempts to reach each of the targets, as conditioned by the performance measure being used in the critical path analysis. For example, in terms of minimum interruption probability performance, Target 221 was generated 68% of the time by the PATHfinding Simulation (PATHS) code.[6] The interruption lower bound, as determined by PATHS, is shown to be 0.87 and is strongly correlated with the ranking index. The minimum neutralization probabilities required to achieve at least a 0.9 probability of system win are recorded in Column 4 of Table 1. Note that for the most vulnerable target (No. 221), even if the security force wins the engagement with certainty, a system win probability of 0.9 cannot be achieved because of the low interruption probability (0.87). Procedures also exist for the evaluation of all combinations of targets within a nuclear facility which must be compromised in order to achieve a radiological release. Although the output of SAFE is shown as two significant digits, the limited accuracy of the input data would indicate only one significant digit of accuracy on the output to be justifiable.

Table 1

Global Results for All Type I Targets
(7-Minute Response)

Node Labels of Targets	Ranking Index	Interruption Lower Bound	Neutralization	System Win
221	.68	.87	1.00	.87
440	.12	.95	.95	.90
438	.08	.97	.93	.90
224	.07	.97	.93	.90
439	.03	.98	.92	.90
703	.02	.98	.92	.90
523	0.00	.99	.91	.90
441	0.00	1.00	.90	.90

Figure 14 is a three-dimensional picture of the probability of interruption (plotted vertically) versus the response time of the security force versus the probability of detection of Sensor 4. (Sensor 4 is the door sensor located at the entrance to the reactor building, as noted in Figures 11 and 12.) If the sensor fails or does not work properly, the probability of interruption deteriorates significantly to about 0.5; whereas, if the sensor is effective, a high probability of interruption is obtained, provided the security force responds to the door alarm and to the appropriate target within 5 or 6 minutes.

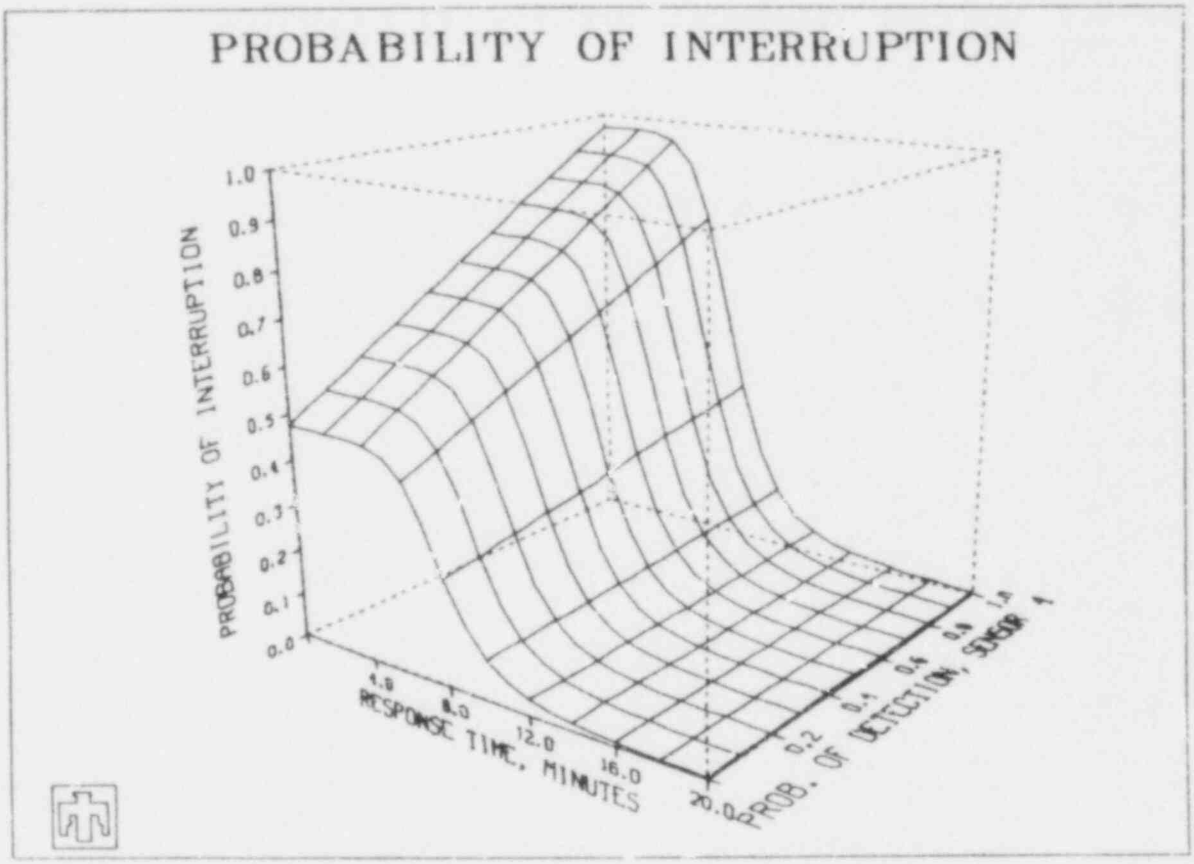

Figure 14. Three-Dimensional EASI Graphics Plot

4. SUMMARY

4.1 OVERVIEW OF SAFE COMPUTER PROGRAMS

The SAFE physical protection system evaluation procedure is illustrated in Figure 15; the computer techniques or programs are shown on the left and the general output from each phase of the process is shown on the right. Under facility characterization, a primary output is target identification. Computer programs, such as the Set Equation Transformation System (SETS)[12] and Generic Sabotage Fault Trees (GSFTs), have been used to perform this analysis for light water reactors. To digitize the facility and prepare it for evaluation, several computer programs, labeled here as Graphical Representation through Interactive Digitization (GRID) and Automated Region Extraction Algorithm (AREA),

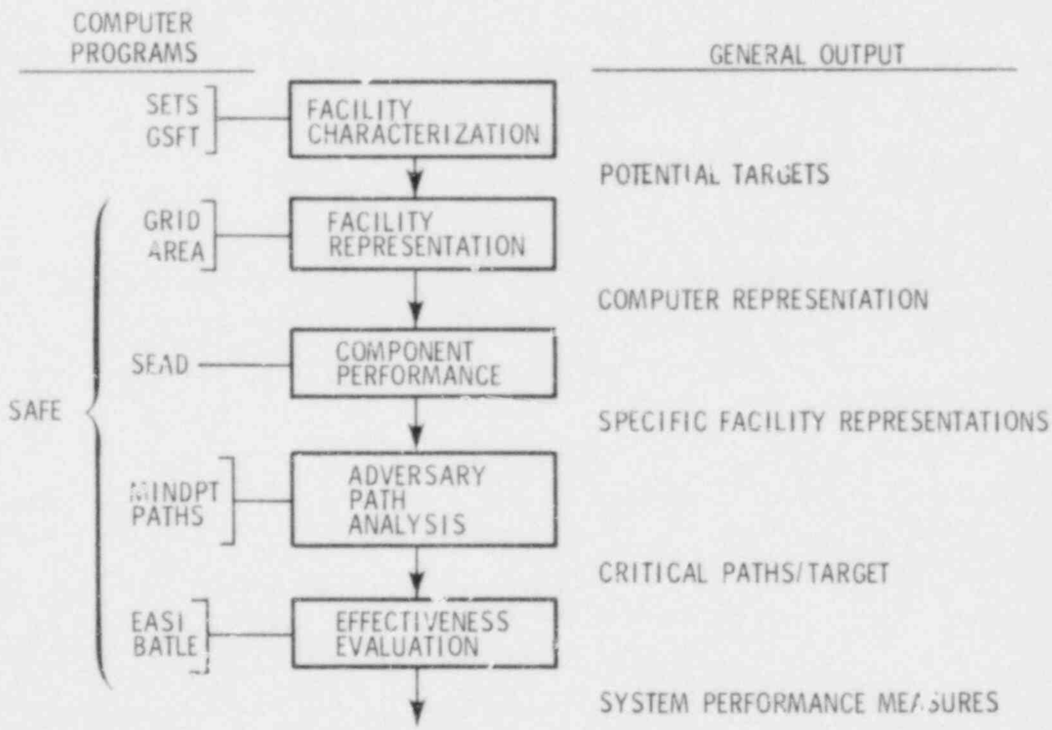

Figure 15. SAFE Evaluation Procedure and Computer Programs

are utilized. A digitized representation of the facility and a facility graph are obtained as output. Component performance characteristics are then supplied either from data obtained from the Safeguards Engineering and Analysis Data-Base (SEAD)[13] or directly by the user. The result is a specific facility representation in terms of specific environmental and operational conditions. The analyst then uses an adversary path analysis technique [MINimum Detection Probability and Time (MINDPT)[5] or PATHfinding Simulation (PATHS)[6]] to minimize detection probability, time, or interruption probability and to generate critical paths for each target. EASI (Estimate of Adversary Sequence Interruption)[7] and BATLE (Brief Adversary Threat Loss Estimator)[8] are utilized for an effectiveness evaluation along the critical path that would provide the overall system performance measures. Ultimately, the more critical adversary paths would require a more detailed evaluation using a technique such as SNAP[4] to look at specific scenarios. This would provide additional model detail in evaluating the overall system performance measure.

The SAFE process can be accomplished in a matter of a few days to a few weeks. The vital area analysis using SETS and GSFT is now being utilized by the NRC to identify vital areas for all the operating power reactors in the United States. Currently, the time required to perform the analysis for a typical operating facility averages from 2 to 4 weeks.

SAFE is an automated procedure for evaluating the effectiveness of physical protection systems. It provides an explicit record of the analyst's assumptions through the facility representation. Critical adversary paths can be determined, and overall global lower bounds on paths can be obtained. Sensitivities of the probability of interruption for a path to variations of path parameters can be generated and displayed using computer graphics. Within SAFE, estimates can be made for the probability that the security force neutralizes the adversary.

SAFE presents a broad range of evaluation capabilities to an analyst. It has potential uses in the areas of design, evaluation, and system improvement. To date, SAFE has been applied to a variety of existing and conceptual facilities. Besides land-based facilities, SAFE has been applied to a generic ship which has six decks and one target. These applications have shown SAFE to be a useful technique for analyzing physical protection systems.

4.2 COMMENTARY ON THE USE OF MODELS

It should be emphasized that SAFE cannot, nor was it meant to, replace the analyst or decision maker. A common misconception about the purpose of models is the belief that they are supposed to provide complete optimal solutions, free of human subjectivity and error. Implicit in this notion is the concept that the decision-making process can be automated once all the appropriate considerations have been properly defined. On the contrary, there are virtually always some neglected or intangible aspects to be considered, along with the output produced by the model, before a commitment can be made to any course of action. In the model formulation itself, many decisions must be made with respect to what aspects of the problem are important and what assumptions are reasonable.

All of these decisions are subjective and call for decision-making capabilities of a uniquely human nature. However, it would be going too far to say that models make the job of the decision maker any easier. If anything, the challenges are greater because of the expanded technical capabilities and other resources required to make good use of the modeling approach. Certainly, the role of experience, intuition, and judgment in the decision-making process remains undiminished. The models, in simplest terms, provide the analyst with a consistent structured approach which aids in the evaluation of safeguards systems. In this respect, models of physical protection systems can assist decision makers and allow for better decisions to be made, but they certainly are not a replacement for the decision maker.

Comment should also be made concerning model accuracy. Accuracy can refer to two aspects of models--the inherent numerical accuracy of model output and the precision of detail used to represent the real facility. The numerical results, in general, are represented to two decimal places. One decimal place would more realistically represent the confidence that may be placed in the result. Two digits have been used mainly due to user preference.

As the level of detail represented in a model increases, the accuracy of the representation does not necessarily improve. If superfluous detail is included, overhead cost increases with little or no improvement in results. Therefore, considerable care should be taken when deciding on the level of detail to be included in a SAFE effectiveness evaluation.

REFERENCES

[1]L. D. Chapman et al, Users Guide for Evaluating Alternative Fixed-Site Physical Protection Systems Using "FESEM," SAND77-1367 (Albuquerque: Sandia Laboratories, November 1977).

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

[3]D. Engi et al, Fixed Site Neutralization Model User's Manual, SAND79-2241, NUREG/CR-1307 (Albuquerque: Sandia Laboratories, December 1979).

[4]D. Engi et al, User's Guide for SNAP, SAND80-0315, NUREG/CR-1245 (Albuquerque: Sandia National Laboratories, July 1981).

[5]B. L. Hulme, MINDPT: A Code for Minimizing Detection Probability Up to a Given Time Away From a Sabotage Target, SAND77-2039 (Albuquerque: Sandia Laboratories, December 1977).

[6]D. Engi, J. S. Shanken, and P. W. Moore, "Pathfinding Simulation (PATHS) User's Guide," SAND80-1626, NUREG/CR-1589 (Albuquerque: Sandia National Laboratories, to be published).

[7]H. A. Bennett, User's Guide for Evaluating Physical Security Capabilities of Nuclear Facilities by the EASI Method, SAND77-0082, NUREG-0184 (Albuquerque: Sandia Laboratories, June 1977).

[8]D. Engi and C. P. Harlan, Brief Adversary Threat Loss Estimator (BATLE) User's Guide, SAND80-0952, NUREG/CR-1432 (Albuquerque: Sandia National Laboratories, May 1981).

[9]D. W. Sasser, Users Guide for EASI Graphics, SAND78-0112 (Albuquerque: Sandia Laboratories, March 1978).

[10]G. B. Varnado et al, Reactor Safeguards System Assessment and Design, Volume I, SAND77-0644, NUREG/CR-0313 (Albuquerque: Sandia Laboratories, June 1977).

[11]Safety and Security of Nuclear Power Reactors to Acts of Sabotage, SAND75-0504 (Albuquerque: Sandia Laboratories, March 1976).

[12]R. B. Worrell and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, NUREG/CR-0465 (Albuquerque: Sandia Laboratories, November 1978).

[13]R. C. Hall and R. D. Jones, A Scientific Data Base for Safeguards Components, SAND78-1766, NUREG/CR-0459 (Albuquerque: Sandia Laboratories, December 1978).

INDEX

This index references Volumes I, II, and III of the SAFE Users Manual. Volume IV, which contains a complete listing of the computer programs used in SAFE, is not referenced. References are to volume number and page. Footnotes are designated by an n following the page number.

Adversary attributes, bounds on, I.26, II.58
Adversary path(s), realistic, II.16, II.16n, II.28, III.16, III.16n
Adversary path analysis, I.26-29, II.14, II.16, II.61-75, III.16
  algorithms used, I.27, I.29, II.65, II.67, II.71
  criteria used, I.16, II.16, III.16, III.53
  critical paths generated, I.26-29, III.59
  input to, I.26-27
  interactive input procedure, III.53-59, III.73-81
  objective of, I.26, II.61
  optimal paths generated, II.61-65
  output of, I.16, I.27-28, II.16, III.16
  path selection example. II.73-75
  pathfinding criterion chosen, III.53-55, III.71, III.73
  problem complexity, II.63
  redimensioning of arrays in, III.56-58
Adversary scenarios, generation of, I.15-16
Analysis options. See path evaluation
Analyst
  input data assumptions, I.21, I.26, I.34, II.27, III.19
  input to facility graph, II.44
  resources available to, II.15, II.19, III.14
  role of, I.35, II.20-21, III.14
  use of facility layout drawing, II.26
Arc,
  in facility graph, I.23-24, II.16, II.43-44, II.52, II.63
  in stairwells, II.51-52
  traversal time, II.52
AREA (Automated Region Extraction Algorithm), I.33, II.45-52
  addition of stairwell regions in, II.45, II.51-52, III.39-40
  capabilities of, II.45, III.34
  constraints imposed by, II.45
  deletion of regions by, II.50-51, III.36
  editing of region data with, II.51, III.39
  generation of region data using, II.48-50, III.34-42.
  input to, III.34
  interactive input procedure, III.36-42
  output of, III.34
  termination of, II.52, III.39-42
  See also RFPREP, NSPLIT, BREGNS, POSTPR, UAREA
Arrays, redimensioning of, III.56-58
AUTREG, III.42

Barrier, to movement, II.20, II.43
  See also node, barrier
BATLE (Brief Adversary Threat Loss Estimator), I.17, I.34, II.17, II.79, II.83-87, III.17, III.59-60, III.81-90, III.187-211
  attrition rates in, II.83-85, III.187-188
  "BATLE Input and Status Reports," II.86, III.86-87, III.190, III.197-199
  "BATLE Termination Time Information," II.87, III.86, III.88, III.190, III.199-200
  combat parameters, II.85-86, III.188-190
  combat parameters, example facility, III.84-85, III.190-196
  definition of events, III.82-83
  editor, III.202
  in effectiveness evaluation phase, I.17, II.17, II.77-79, II.83-87, III.17, III.59-60
  engagement defined, II.83, III.187
  engagements simulated by, II.79, II.83-86, III.187
  "Guard Delay Time Information," II.86, III.86-87, III.190, III.197, III.199
  input to, I.17, II.85-86, III.188-190
  input to, example facility, III.83-86, III.191-196
  interactive input procedure, III.82-90, III.191-196
  Markov process, II.84
  measure of effectiveness, II.78
  output of, I.17, II.17, II.86-87, III.190, III.197

output of, example facility,
III.86-90, III.198-201
"Probability Distributions," II.87,
III.86, III.88-89, III.197,
III.199-201
probability mass table, III.197n
quit-criteria, III.202-203
reinforcements, II.17, II.84,
III.188
Safeguards System Effectiveness
Measures, III.90
sensitivity studies using, III.202,
III.204-211
state descriptor, III.187
steady-state status, II.86, III.197
transition diagram, II.83-85,
III.187-188
transition rates, II.83-85,
III.187-188
See also engagement
Battle. See engagement
Blueprints, facility, I.21-23, II.13,
II.20, II.26, III.19
BREGNS, II.48-50. See also AREA

Communication, probability of, I.16,
II.55, II.78-79
Communication system, II.25
Component performance, I.24-26,
II.14, II.16, II.55-59,
III.15, III.47-51
bounds on, I.26, II.58
characteristics, I.25, II.55-56
conditions affecting, I.25-26,
II.55-58
data editing, III.49, III.99
data selection, II.55-58
default values, III.47
generic data base, II.58-59
input to, I.25, II.55-56, III.47
interactive input procedure,
III.47-51
objective of, I.24-25, II.55
output of, II.56, III.15
probability of detection, I.25,
II.33n, III.15, III.23
specific facility representations,
II.56
time delay, I.25, II.16, II.33n,
III.15, III.23, III.47
travel velocities, I.25
values assigned using GRID, II.33,
II.33n
Conditions, environmental,
operational, and adversary,
I.11, I.19-21, I.24-25,
II.14-15, II.19-20, II.20n,
II.25, II.56-57, III.17, III.91
Coordinate system, II.15-16, II.28,
II.33, III.22-23
Critical paths, I.16, I.27, I.29,
II.62-63
criteria for, I.16, II.16,
II.62-63, III.151, III.159
determined by MINDPT, II.67-70,
III.151
determined by PATHS, II.71-72,
III.159
input to MINDPT for, II.68-70,
III.151
input to PATHS for, II.72,
III.159-160
listing, example facility,
III.59, III.80
Cursor, 12-button, I.23, II.31-35,
III.20-21, III.23-24

Data communication interface,
III.28-29
Data transfer to NOS, III.28-34
Default values, specified in GRID,
III.23, III.47
Delay time. See time delay
Design tool, SAFE used as, III.99-104
Detection. See probability of
detection
Deterministic pathfinder, I.16,
III.151-152.
arrays, redimensioning of,
III.56-58
criteria for determining critical
paths, III.151
input to, III.151
interactive input procedure,
example facility, III.153-158
output of, III.151-152
output of, example facility,
III.153-158
See also MINDPT
Digitization. See facility
digitization
Dijkstra, shortest-path algorithm
in MINDPT, II.67
in PATHS, II.71
Distribution types for time delays in
PATHS, II.72, III.75

EASI (Estimate of Adversary Sequence
Interruption), I.16-17, I.34,
II.17, II.77-79, III.16,
III.59-60
advantages of, II.78
central limit theorem, II.79
in effectiveness evaluation phase,
I.16-17, II.17, II.78-79,
III.16, III.59-68
graphics capability in. See EASI
Graphics
input to, II.78-79
measure of success, II.78-79
output of, I.16-17
EASI Graphics, I.17, I.31, II.79-80,
III.16
analysis of paths using, III.16,
III.60, III.68-71, III.107,
III.111-114

copy capability, III.71
plot options available, II.80, II.82
plots, example, II.81, II.89-90
plots, example facility, III.69-72, III.112-122
plots, user-scale, III.69, III.71
Effectiveness evaluation, I.16, I.29-31, II.14, II.17, II.77-90, III.16-17, III.59-71
BATLE used in, I.17, II.17, II.77-79, II.81-87, III.17, III.59-60
EASI used in, I.16-17, II.17, II.77-79, III.16, III.59-68
EASI Graphics used in, III.68-71
global results, example, II.87
input to, I.16, I.29-30, II.77, III.16
interactive input procedure, III.60-71
multi-path option, I.17, II.17, III.16-17
objective of, I.29, II.77
output of, I.30-31, II.77
single-path option, I.17, II.17, III.16, III.111
Engagement(s) in BATLE, II.79, II.83-87
commencement of, II.84, III.190
defined, II.83, III.187
quit-criteria, III.202-203
state descriptor, III.187
states in, II.83-85, III.187-188
termination of, II.84, III.202
transition diagram for, II.83-85, III.187-188
transition rates, II.83-85, III.187-188
See also BATLE
Equipment used in SAFE. See SAFE
Evaluation of specific facility representation, III.91-99
Evaluation tree used for component performance, II.57
Example facility, III.19, III.123
adversary path analysis phase for, III.53-59
analysis of, simplified, III.97-99
AREA used to generate regions for, III.36-42
arrays, redimensioning of, III.56-58
BATLE run for, III.81-90, III.190-202
component performance phase, III.47-51
coordinates registered, III.22-23, III.26-27
critical paths listed, III.59, III.80-81
data, III.137-144
data transfer to NOS, III.28-34
default values for III.23-24,
description of, III.19, III.123
digitization of using GRID, III.20-28
EASI used to analyze, III.60-68, III.111
EASI Graphics used to analyze, III.68-71, III.111-122
editing facility data, III.49-51, III.49n
effectivensss evaluation phase for, III.59-71
facility characterization phase for, III.19n
facility representation phase for, III.19-46
global sensitivity analysis of, III.108-111
guard facility model, III.105, III.142
histograms for, III.66-67, III.81-82
layout drawings, III.19-20, III.51-53, III.123-136
levels in, III.19, III.123
list (dump) of regions in, III.145-149
lower bound for, III.97-99, III.104
MINDPT used to analyze, III.53-59, III.97-99, III.152-158
node types and symbols for, III.20-21, III.123
nodes in critical paths, III.66
nodes listed, III.42-45
NOS sign-on procedure, III.29-32
output using deterministic pathfinder (MINDPT), III.153-158
output using stochastic pathfinder (PATHS), III.161-172
pathfinding option chosen, III.53-54, III.71, III.73
PATHS used to analyze, III.73-80, III.97-99, III.160-172
probability of detection for, III.23-24, III.137-138
probability of interruption for critical paths, III.66, III.81
rate of travel selected, III.51
response time, security force, III.55-56, III.142-143
security force characteristics, III.105-106, III.142
sensitivity analysis of, using EASI Graphics, III.68-72
specific facility representation evaluation of, III.97-99
stairwell data, III.139-141
start nodes, III.55, III.106
targets, III.97-99, III.144
terminal nodes chosen, III.55
threshold, III.97-99
time delay values for nodes, III.23-24, III.105, III.137-138

UPREP executed for, III.42-46
USAFE run for, III.47-49

Facility characterization, I.20-21, II.13, II.15, II.19-26, III.14, III.19, III.19n, III.101
analyst's role in, II.20-21
facility layout drawing, II.26
facility operating states, I.20, II.20n, II.25
input to (data sources for), I.20, II.13, II.19, III.14
objective of, I.20
output of, I.21, II.19-20, II.26-27
Facility data, I.23
digitized, II.43-45
edited by user, II.51-52, III.47-51, III.105
for example facility, III.137-144
files, II.27, II.30-31, II.43-45, III.26
for guard model, III.142
input by user, III.47-51
physical characteristics, II.20
transfer to NOS, II.31, II.45, III.28-34
transformation to facility graph, I.23-24, II.52-53, III.34-46
Facility digitization, I.22-24, II.27-43, III.19-34
analyst's role in, I.22-23
cursor used in, I.23, II.31-35, III.20-21, III.23-24
data communication interface, III.28-29
data transfer to NOS, III.28-34
equipment used in, II.30-31. See also Tektronix 4051; cursor, 12-button
GRID used in, II.27-43, III.20-27
initialization for, III.22, III.28
input to, III.19
output of, II.30, II.43
restrictions on, II.30
steps in, II.33-36
user-definable keys (UDKs), II.36-43, III.25-32
Facility evaluation, II.13, III.91-99
iterative procedure for, II.14, II.17, III.14, III.17
using MINDPT, III.95-99
using PATHS, III.92-99
Facility graph, I.23-24, II.15-16, II.43, II.63-64, III.15
analyst's input to, II.44
construction of, II.43-45, II.52
nodes and arcs in, I.23-24, II.16, II.43-44, II.63-64, III.15
region data generated using AREA, II.45-52, III.34-42
regions in, II.16, II.43-45
transformation of data to, I.23-24, II.52-53, III.34-46
Facility layout, I.20-21, III.15
characteristics, I.20-22
computer representation of, I.21-24, III.19
data, III.34. See also LEVELS
digitization of, I.22-23, II.15-16, II.27-43, III.15, III.19
display, II.33, III.51-53
See also facility representation
Facility layout drawings, I.20, I.23, II.20-21, II.26, II.28, III.19
analyst's use of, II.26
copies made, III.51, III.60, III.62-65
for example facility, III.19-20, III.51-53, III.123-136
input to GRID, II.28
simplification of, II.20-21
Facility representation, I.21-24, II.13-16, II.27-53, III.15, III.19-46
AREA used in, II.45-52
computer representation, I.21, I.23, II.27
data transfer to NOS, III.28-34
digitizing process in, I.22-24, II.27-43, III.19-28. See also GRID
evaluation of specific, III.91-99
GRID used in, II.28-43, III.20-28
input to, I.21-22, II.26-27, III.19
objective of, I.21
output of, I.21, II.16, II.27, III.15
transformation to facility graph, II.43-53, III.34-46
See also facility layout
Fault tree analysis procedures, I.21, II.25, II.91-95
symbology used, II.94
usefulness of, II.95
FESEM (Forcible Entry Safeguards Effectiveness Model), I.13-14, III.17
FSNM (Fixed-Site Neutralization Model), I.14

Global evaluation, I.15-17
example results, I.30
using SAFE, I.11, I.17, I.19
GRID (Graphical Representation through Interactive Digitization), I.33, II.27-43
coordinate system used with, II.28, III.22-23
default values specified in, III.23, III.47
detection probabilities assigned using, II.33, II.33n
digitization using, III.20-28
equipment needed, II.30-33
how to load, III.20-21
input to, II.28

interactive input procedure,
III.21-28
template on Tektronix 4051,
II.36, III.25.
time delays assigned using, II.33,
II.33n
utility functions for Tektronix
4051, II.36-43
utility functions for Tektronix
4054, II.97-98
GSFT (Generic Sabotage Fault Trees),
I.33
Guard characteristics. See security
force, characteristics
Guard response time. See response
time, security force

Header, III.75
Histogram, III.66-67, III.81-82

Insider, I.13, III.92
ISEM (Insider Safeguards
Effectiveness Model), I.13-14,
III.17

LEVELS, III.33-34, III.36, III.42,
III.49n
Lines, II.28-30, II.43, II.45
cursor used to digitize, II.32-35
restrictions on, II.30
Locus point(s), II.65, II.67-68
Lower bound,
global, I.17
from PATHS, II.72, III.92-97
on performance for combinations of
targets, III.94-95
for theft paths, II.68

Measure(s)
deterministic, I.16
MIN-MAX, III.95, III.109-111
pathfinding, I.16, I.27-29
Safeguards System Effectiveness,
II.78, III.90
stochastic, I.16
See also minimum probability of
detection; minimum probability
of interruption; minimum time
MINDPT (MINimum Detection Probability
and Time), I.34, II.65,
II.67-71, III.151-152
input to, for critical paths,
II.68-70, III.151
interactive input procedure,
II.71, III.53-59, III.153-158
output of, II.70, III.101,
III.151-152
output of, example facility,
III.153-158

pathfinding criteria, II.67,
III.16, III.151
removal path determined by, II.68
for specific facility
representation evaluation,
III.95-99
See also deterministic pathfinder
Minimum probability of detection
criteria in adversary path
analysis, I.16, II.16, III.16,
III.53, III.151
for example facility, using MINDPT,
III.155-156
from MINDPT, II.67-68, III.151-152
for optimal path determination,
I.16, II.65-66
Minimum probability of interruption
criteria in adversary path
analysis, I.16, II.16, III.16,
III.16n, III.53, III.151,
III.159
for example facility, using MINDPT,
III.54-55, III.97-99,
III.157-158
for example facility, using PATHS,
III.73-81, III.97-99,
III.165-172
from MINDPT, II.69-71, III.95-97,
III.151-152
for optimal path determination,
I.16, II.62-63, II.65-66,
III.104
from PATHS, III.92-95, III.159-160
security force response times
generated for, III.104-107
threshold, III.92
Minimum time
criteria in adversary path
analysis, I.16, II.16, III.16,
III.53, III.151, III.159
for example facility, using MINDPT,
III.153-154
for example facility, using PATHS,
III.161-164
from MINDPT, II.67-68, III.151-152
for optimal path determination,
I.16, II.65-66
from PATHS, III.159-160
paths for security force,
III.105-106
MIN-MAX performance measure, III.95,
III.109-111
Model, evaluation,
accuracy of, I.35
FESEM, I.13-14, III.17
FSNM, I.14
global, I.14-17
ISEM, I.13-14, III.17
role of, I.35
scenario-based, I.13-15
second-generation, I.14-15
SNAP, I.14-15, III.17
Monte Carlo simulation techniques,
I.13-15, II.72

Node(s), II.28-30, II.43, II.63-64
  barrier, II.45, II.53, II.63
  boundary, II.53, II.63, III.42-45
  checked using UPREP, III.42-45
  cursor used to digitize, II.31-35, III.20-21
  default values specified for, III.23
  describing critical paths, III.80
  editing of, III.49-51
  examined using AREA, II.45-50, III.36-40
  example facility data, III.137-144
  in facility graph, I.23, II.16, II.43-44, II.63
  grouped for pathfinding routines, II.53
  label(s), II.30, III.20, III.77, III.123
  label(s) in list of critical paths, III.59, III.66, III.77, III.80
  listed in region dump, III.146-149
  locus, II.67
  POSTPR used to eliminate extra, II.50
  probability of detection for, III.23
  processed by RFPREP, II.45-47
  pseudo-, II.29-30, II.43, II.45, II.47, II.52, III.20, III.24
  restrictions on, II.30, II.43, II.45
  split by NSPLIT, II.47-48
  stairwell, II.43, II.51-52, III.139-141
  start, II.53, III.55
  symbols used in SAFE, II.32, III.20-21, III.123
  target, II.43, II.53, II.63, III.42-45, III.55
  terminal, II.67, II.70, III.16n, III.55, III.59
  time delays for, III.23, III.105
  types, II.30, II.32, III.20-21, III.123, III.137-138
  x,y-coordinates of, II.30
Node Update Option, III.49-51
NOS (Network Operating System), II.30-31, III.173-181
  accessing, III.173
  file commands, III.174-181
  file creation, III.32
  file types, III.174-175
  LEVELS file, III.33-34, III.49n
  local file, III.33, III.174
  local file commands, III.177-179
  permanent file, III.34, III.174
  permanent file commands, III.175-176
  primary file, III.33, III.175
  procedure files, III.178
  SAFE procedure on, III.47-90
  sign-on procedure, III.29-32, III.29n, III.173
  system procedures, III.178-179
  TAPE10, III.36
  TEXT mode, III.178
  transfer of data to, II.45, III.28-34
  XEDIT, III.32-33, III.45, III.49n, III.179-181
NSPLIT, II.47-48. See also AREA

Outsider, I.13, II.64, III.92

Path(s)
  access, II.61, II.64
  critical, I.16, II.62, II.68-72, III.59
  defined, II.61
  display of, III.60-65
  evaluation of, I.16
  optimal, I.16, II.61-65
  realistic, II.16n, II.28
  removal, II.61, II.68
  for sabotage, II.61, II.64
  sensitivity study of, III.111-112
  for theft, II.61, II.68
Path evaluation (analysis), II.77
  measure of effectiveness, II.78, III.90
  multi-path option, I.17, II.17, III.16-17, III.97
  selection criteria, I.16, II.16
  single-path option, I.17, II.17, III.16-17, III.111
Pathfinding
  algorithms, I.27, I.29, II.65-67, II.71, III.56-59. See also MINDPT; PATHS
  criteria, I.16, II.16, II.67, II.69, III.16, III.53
  options, III.16-17, III.53-55, III.71
PATHS (PATHfinding Simulation), I.34, II.65, II.71-73, III.73-81, III.92-95, III.159-172
  brief input mode, III.73
  critical paths listed, example facility, III.80-81
  header, III.75
  histogram for, III.81-82
  input to, II.72, III.159-160
  input to, example facility, III.161-172
  interactive input procedure, II.73, III.73-81, III.161-172
  interruption calculations, III.74-75
  lower bound on probability of interruption, II.72, III.92-95
  minimum interruption criterion, III.92, III.165-172
  minimum time criterion, III.161-164
  "Node Ranking Information," III.79-80, III.101, III.103, III.170-171

output of, II.72, III.92,
III.101-103, III.160
output of, example facility,
III.76-81, III.161-172
"Path Description," III.77,
III.102, III.168
"Path Ranking/Interruption
Information," III.78, III.103,
III.169
pathfinding criteria, II.67,
III.16, III.159
"PATHS Summary," III.76,
III.102, III.167
random number seed, III.74, III.74n
ranking index, II.71-72, II.87,
III.101
replications, II.71-72, III.74-75,
III.160
for specific facility
representation evaluation,
III.92-95
threshold, III.92-94, III.97
time delay distributions used,
II.72, III.75
See also stochastic pathfinder
Patrol, roving, III.105-106
Physical protection evaluation, I.11,
I.19, I.33, III.13-14
computer programs used in, I.33-34,
II.15, III.14-15
model development, I.11
phases of, I.11, II.13, III.13
Physical protection system,
configuration, II.25-26
modifications to, III.99-101
security plan, II.26
threats to, I.11, II.14
POSTPR, II.50. See also AREA
Probability of communication, I.16,
II.55, II.78-79
for example facility, III.60
Probability of detection, I.25,
II.16, II.33, II.33n, III.15,
III.23, III.47
cumulative, II.70
default values, III.23
for example facility nodes,
III.137-138
See also component performance
Probability of interruption, I.16-17,
II.16n, III.16n, III.104
for critical paths, example
facility, III.66
histogram of, III.67, III.81-82
measure in EASI, II.78-79,
III.59-60
for optimal path, II.62
Probability of neutralization,
I.17, II.77-78, III.17, III.90
measure in BATLE, II.78, III.60
Probability of system win, I.16-17,
II.78, II.87-88, III.17, III.90
Pseudo-node, II.29-30, II.43, II.45,
II.47, III.20, III.24

deletion of, II.52

Random number seed, III.74, III.74n
Ranking index, II.71-72, II.87,
III.101
REGDAT, III.42, III.45
Region(s), II.43-45
data file, III.42
deletion of using AREA, II.50-51,
III.36
in digitized facility layout, II.43
display of, III.29
edit of data by user, II.51-52,
III.39-40
in facility graph, II.63-64
generation by AREA, II.48-50,
III.34-42
input to, III.34
listing (dump) of, example
facility, III.145-149
with split nodes, II.50-51
stairwells in, II.45, II.51-52,
III.39-40
REGION, III.42, III.45. See also
UPREP
Region file, III.42. See also AUTREG
Replication(s), in PATHS, II.71-72,
III.74-75
Response time(s), security force,
I.16, I.25, II.65-69, III.47,
III.55-56, III.59, III.104-107
calculation of, III.106, III.142
estimated, III.55-56, III.104
for example facility, III,55-56,
III.142-143
generation of, III.104-107
locus, II.67-68
relationship to pathfinding
criterion, II.69
sensitivities to, III.107
special cases, III.105, III.107
to targets, III.106, III.143
RFPREP, II.45-47. See also AREA

Sabotage. See target(s), sabotage
SAFE (Safeguards Automated Facility
Evaluation), I.11, I.33-35,
II.13-18, III.14-17
accuracy of, I.30
application of, I.34, II.18, III.91
capabilities of, I.15-17, I.34,
II.18, III.17
computer programs used in, I.33-34,
II.15, III.14-15
as design tool, III.99-104
equipment used in, II.30-31
evolution of, I.13-17
facilities evaluated using,
III.91-99
for global evaluation of safeguards
systems, I.11, I.19, II.18
for global sensitivity studies,
I.17, III.108-111

iteration in, II.17, III.14,
III.17, III.68, III.99
on NOS, III.47
phases of, I.11, I.19-31, II.15-17,
III.14-17
for sensitivity studies,
III.108-122
site-specific analysis, III.42-46
time required for application of,
I.34
Safeguards effectiveness evaluation
fault trees used for, II.91-95
global approach to, I.15-17
need for, II.13
Safeguards methodology development,
I.13-14
global approach, I.14-17
second-generation scenario models,
I.14-15
single-scenario approach, I.13-14
Safeguards System Effectiveness
Measures, II.78, III.90
Safety analysis report (SAR), I.20,
II.15, II.19, II.26, III.14
Scenario-based models, I.13-15
limitations of, I.14-15
SEAD (Safeguards Engineering and
Analysis Data-Base), I.34, II.59
Security force
characteristics, I.20-21, I.29-30,
II.25-26, III.94-95,
III.104-105
characteristics, example facility,
III.105-106, III.142
neutralization of adversary,
I.16-17, II.17
response time. See response time,
security force
start nodes for, III.105
Sensitivity studies, I.17,
III.108-122
global, III.108-111
specific, III.111-112
value of, III.108
SETS (Set Equation Transformation
System), I.33
Site-specific analysis using SAFE,
III.42-46
SNAP (Safeguards Network Analysis
Procedure), I.14-15, I.34,
III.17
Stairwell, II.20, II.28, II.51-52,
III.34, III.39-40, III.139-141.
See also node(s), stairwell;
region(s), stairwells in
Stochastic pathfinder, I.16,
III.159-160
criteria for determining critical
paths, III.159
defined, III.159
input to, III.159-160
input to, example facility,
III.161-172
output of, III.160
output of, example facility,
III.161-172
See also PATHS

Tactics, adversary, I.29, II.65
Target(s), I.16n, I.19-21, II.20n,
II.21-25, III.14, III.92n
in example facility, III.97,
III.101-104, III.144
identification of, II.21-25
MINDPT run for, III.95-99
PATHS run for, III.92-95,
III.101-104
sabotage, II.20n, II.21, II.23-25,
II.64, III.55, III.92
security force response time to,
III.104-107
theft, II.20n, II.21-23, III.55,
III.92
See also vital areas, Type I; vital
areas, Type II
Tektronix 4012 emulator program,
III.28-29
Tektronix 4051, II.30-31
commands, III.183-185
data communication interface,
III.28-29
GRID executed on, II.31-43,
III.20-27
GRID template, II.36, III.25
GRID utility functions on, II.36-43
special keys, III.184-185
statements, III.183-184
transfer of data from, III.28-34
user-definable keys, II.36-43,
III.25-32
See also Tektronix 4054
Tektronix 4054, II.30, II.30n,
II.97-98, III.183
GRID utility functions for,
II.97-98
See also Tektronix 4051
Template
data communications interface,
III.28-29
GRID, II.36, III.25
Terminal, II.16n, III.16n, III.59
Theft. See target(s), theft
Threat, adversary, I.11, I.13, II.77,
III.92
Threshold, III.92-94, III.97
Time delay, II.33, II.33n, III.15,
III.23, III.74, III.105, III.151
for arcs in stairwells, II.51-52
distribution code for in PATHS,
II.72, III.75
for example facility nodes, III.24,
III.105, III.137-138
histograms for, III.67
weights for, II.71-72
See also component performance
Time limit, III.76
Timely detection. See minimum
probability of interruption

Transition diagram, II.83-85, III.187-188
  state descriptor, III.187
  transition rates, II.83-85, III.187-188
  See also BATLE
Travel, rate of, III.47, III.51, III.106
Traversal times. See arc, traversal time

UAREA, III.36
Upper bound on performance for combinations of targets, III.95
UPREP, III.42-46
  cross-checking nodes with, III.42-45
  files generated by, III.45-46
  site-specific information edited by, III.45
USAFE, III.105
  example run, III.47-49
User-definable keys (UDKs). See Tektronix 4051, user-definable keys

Vital areas, I.20n, I.22, II.20n, III.92n
  example analysis procedures for, II.91-94
Vital areas, Type I
  defined, II.91, III.92, III.92n
  for example facility, III.97, III.144
  MINDPT run for, III.95-99
  PATHS run for, III.92-95, III.101-103
  in specific facility evaluation, III.92-99
  targets, example facility, III.97, III.144
Vital areas, Type II
  combinations, III.144
  composite score for, III.94-95
  defined, II.91, III.92, III.92n
  for example facility, III.97, III.144
  MINDPT run for, III.95-99
  PATHS run for, III.92-95
  in specific facility evaluation, III.92-99
  targets, example facility, III.97, III.144
  worst-case combinations, III.94-95

Weight(s), random draws for time delays, II.71-72
Weighted graph, II.62, II.67, II.71
  for determining optimal path, II.64-65
  for minimum interruption, II.65

XEDIT. See NOS, XEDIT

Yen, bookkeeping scheme, II.67

DISTRIBUTION:

U. S. NRC Distribution Contractor (CDSI)
7300 Pearl Street
Bethesda, MD 20014
320 copies for RS
25 copies for NTIS

Author selected distribution - 39
(List available from author.)

400	C. Winter	
1000	G. A. Fowler	
1230	W. L. Stevens, Attn:	R. E. Smith, 1233
1233	M. D. Olman	
1700	W. C. Myre	
1710	V. E. Blake, Attn:	M. R. Madsen, 1714
1716	R. L. Wilde	
1720	C. H. Mauney, Attn:	J. W. Kane, 1721
1730	J. D. Kennedy, Attn:	W. N. Caudle, 1734
1750	T. A. Sellers, Attn:	M. J. Eaton, 1759
1751	J. J. Baremore, Attn:	A. E. Winblad, 1751
1752	V. K. Smith	
1754	I. G. Waddoups	
1760	J. Jacobs, Attn:	M. N. Cravens, 1761 J. M. deMontmollin, 1760A W. F. Hartman, 1760A J. D. Williams, 1769
1762	H. E. Hansen	
1762	R. W. Mottern	
1768	C. E. Olson, Attn:	G. A. Kinemond, 1768
1765	D. S. Miyoshi	
2644	C. Pavlakos	
4400	A. W. Snyder	
4410	D. J. McCloskey	
4413	N. R. Ortiz	
4414	G. B. Varnado	
4416	L. D. Chapman (10)	
4416	K. G. Adams	
4416	J. A. Allensworth	
4416	H. A. Bennett	
4416	L. M. Grady (15)	
4416	C. P. Harlan	
4416	R. D. Jones	
4416	M. T. Olascoaga	
4416	J. M. Richardson	
4416	S. L. K. Rountree	
4416	D. W. Sasser	
4756	D. Engi	
5000	J. K. Galt	
5600	D. B. Shuster, Attn:	A. A. Lieber, M. M. Newson, 5620, R. C. Maydew, 5630
5640	G. J. Simmons, Attn:	R. J. Thompson, 5641 L. F. Shampine, 5642
5642	B. L. Hulme	
8214	M. A. Pound	
3141	L. J. Erickson (5)	
3151	W. L. Garner (3) For: DOE/TIC (Unlimited Release)	

☆U.S. GOVERNMENT PRINTING OFFICE: 1981-0-777-023/616