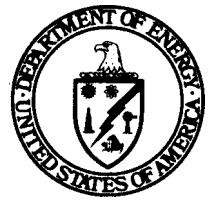
HCP/D0789-01
UC-15

A Systematic Approach to the Conceptual Design of Physical Protection Systems for Nuclear Facilities

May 1978



Prepared For
U.S. Department of Energy
Assistant Secretary for Defense Programs
Office of Safeguards and Security
Washington, D.C. 20545

Under Contract No. EY-76-C-04-0789

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock No. 061-000-00060-7

Available from:

National Technical Information Service (NTIS)
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161

Price: **Printed Copy:** $ 6.00
Microfiche: $ 3.00

TABLE OF CONTENTS

ILLUSTRATIONS

SUMMARY

This report describes a systematic approach that has been used by the Department of Energy's Sandia Laboratories in the course of developing physical protection system conceptual designs for nuclear facilities. A three-step approach is described which includes (1) facility characterization, (2) development and evaluation of hardware-based safeguards systems configurations, and (3) hardware and response force trade-off analysis. The purpose of the report is to establish a vehicle for initial examination and discussion by potential industry and government users of a formal sequence of activities for the conceptual design of physical protection systems and to identify currently available design tools, such as application reports, handbooks, and computer codes which might support these activities.

CHAPTER I

INTRODUCTION

Purpose

This report describes a systematic approach to the conceptual design of physical protection systems for nuclear facilities. Conceptual design of a physical protection system requires development of the system to a stage which is adequate for the demonstration of system feasibility and which has sufficient detail to allow commencement of detailed design and implementation. In this report the concept of a physical protection system is outlined and an approach to the evaluation of the relative effectiveness of physical protection system designs is described. A three-step approach is described which includes (1) facility characterization, (2) development and evaluation of hardware-based safeguards systems configurations, and (3) hardware and response force trade-off analysis. In addition, currently available design tools, such as application reports, handbooks, and computer codes, are identified.

The purpose of this report is to establish a vehicle for initial examination and discussion by potential industry and government users of a formal sequence of activities for the conceptual design of physical protection systems. This approach and some of the methods and models described continue to be developed and improved. The report is primarily a discussion of Sandia efforts sponsored by the Department of Energy; however, some of the evaluation models which are described were developed at Sandia under Nuclear

Regulatory Commission sponsorship. This report is an expansion of another Sandia report, SAND77-0119, "Physical Protection System Design Method."[1]

Physical Protection System Concept Description

The systematic approach discussed in this report is intended to aid the conceptual design of the physical protection portion of an Engineered Safeguards System (ESS). An effective safeguards system must provide four basic functions

- detection of unauthorized activities and material balance discrepancies,
- delay of unauthorized activities until appropriate response can be made,
- response to unauthorized activities and discrepancies in an adequate and timely manner, and
- deterrence of potential adversary actions through public awareness of the general capability of safeguards.

Deterrence, which may result from a potential adversary's perception of system effectiveness, will not be discussed in this report. The three remaining functions are provided by two major systems, physical protection and materials measurement and accounting, as shown in Figure 1-1.

The objective of the physical protection system is to prevent unauthorized removal of special nuclear material (SNM) or acts of sabotage by

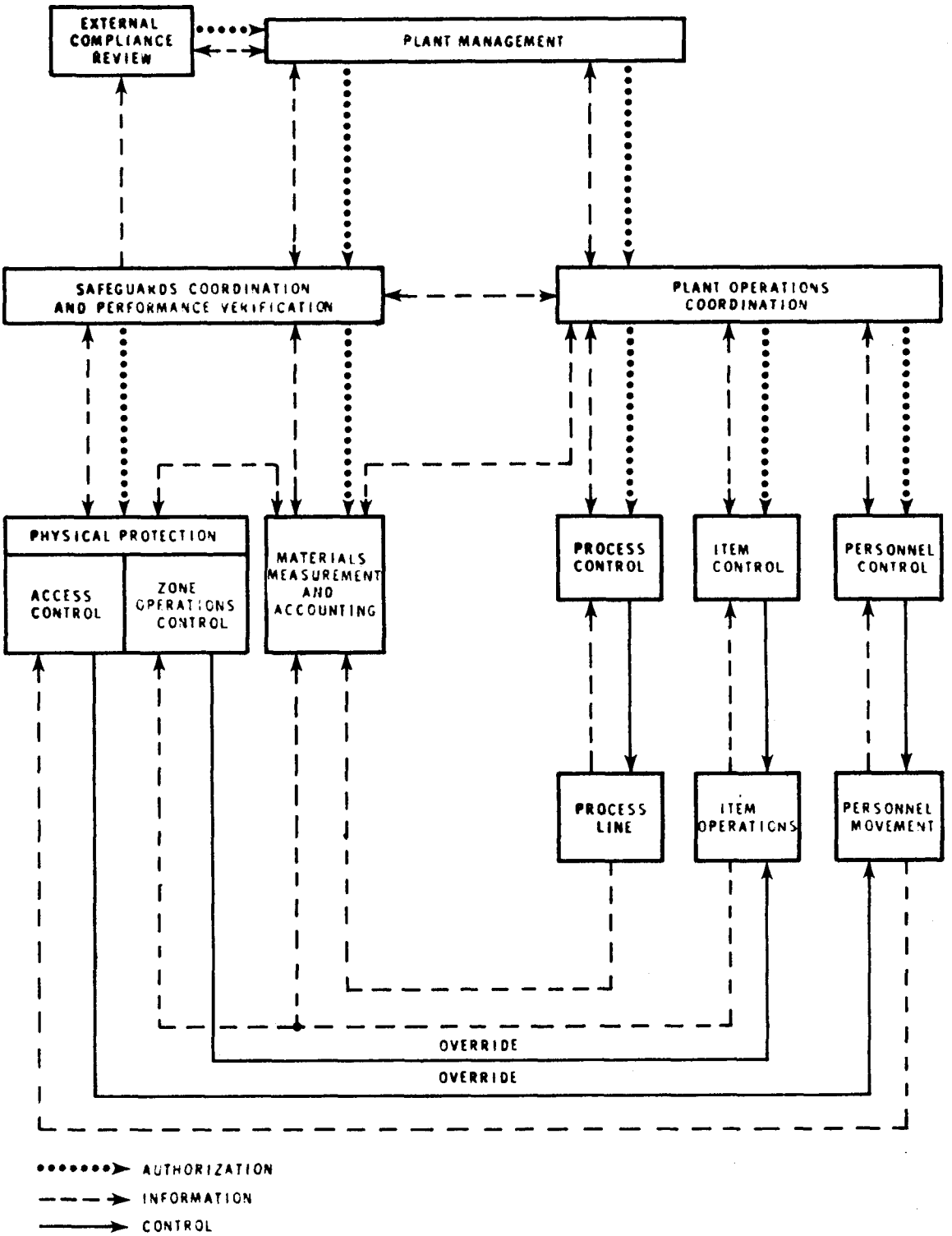


Figure 1-1. Safeguards System Overview

- excluding all unauthorized personnel and contraband from the facility,
- allowing only essential personnel to enter sensitive areas within the facility, and
- monitoring all significant activities and preventing those that are unauthorized.

The physical protection system is composed of two parts, access control, and zone operations control. Access control monitors and enables authorized movement of people and material across barriers and prevents unauthorized movement of people, SNM, and contraband. Zone operations control, which is concerned with the operational interfaces between people and vital equipment and SNM, monitors and enables authorized activities and delays unauthorized actions that could result in sabotage or theft.

The materials measurement and accounting system is used to obtain information on the quantity and location of SNM within the facility. In addition to providing information required for inventory and production control, it can provide the physical protection system with useful detection information related to both one-time theft and long-term diversion. Materials measurement and accounting technology is primarily being developed at the Los Alamos Scientific Laboratory and will not be discussed in this report.

These safeguards systems must be coordinated with normal plant operational systems to obtain a safeguards design which is effective and has minimal

cost and operational impact. The physical protection, materials measurement and accounting, and plant operations functions are coordinated using the authorization, information, and control channels shown in Figure 1-1. Safeguards responsibility is assigned to safeguards coordination just as operational responsibility is delegated to plant operations. Safeguards coordination supervises access control, zone operations control, and materials measurement and accounting. It also coordinates safeguards information flow among these elements, management, and plant operations. The three primary functions of safeguards coordination are data collection and processing, assessment of safeguards alarms, and determination and initiation of appropriate response. Wherever appropriate, safeguards coordination relies on automatic decision and control; however, human assessment, decision, and response initiation are used when necessary.

Although primary responsibility for safeguards assessment lies with safeguards coordination, direct control from lower levels can be used to reduce response times. For the physical protection system, direct control of area access and item handling is assigned to access control and zone operations control elements. Control of area access and of item handling involves a hierarchy of responses depending upon the discrepancy detected between the action authorized and the action performed. For minor discrepancies, control can be automated at the access and operations control level. Serious discrepancies requiring security force responses and/or plant shutdown may require coordination between safeguards and plant operation.

Since some plant processes must operate with continuous flow, direct interruption of the process line by the safeguards system may not be possible.

When process interruption is necessary for safeguards responses, safeguards coordination would initiate appropriate control measures through management or plant operation.

Design Approach

The systematic approach to conceptual design described in this report employs the following three steps:

1. facility characterization,

2. hardware-based safeguards systems configurations, and

3. hardware and response force trade-off analysis.

The level of detail to which each step of a design is defined will depend upon the stage of development of the facility. If the facility itself is in the concept stage, the physical protection system design is defined by major systems and operations. As the facility design becomes more detailed, safeguards system design can proceed at a more detailed level.

In addition, the stage of development of the facility will also affect the extent to which design changes in the facility can be considered in physical protection system design. For a facility which is in the conceptual design stage, simultaneous design of a safeguards system would allow modifications to be made to the overall facility design, probably significantly reducing the costs of the safeguards system. For a facility which already exists, changes in facility design which would reduce the

cost of the physical protection system would have to be evaluated in terms of the cost and feasibility of modifications to the existing facility.

The objective of the first step, facility characterization, is to assemble and process all of the technical information required to perform the physical protection system design and evaluation. The information required for this step includes the overall physical protection system performance requirements, the range of threat attributes to be considered in the design, and the descriptions of facility buildings, processes, and systems. This information is used to perform theft, diversion, and sabotage target analyses and to identify safeguards concerns for the facility. Alternative process and plant layouts can be considered in this step.

The objective of the second step, hardware-based safeguards systems configurations, is to develop and evaluate the portion of the physical protection system that provides detection and delay of the adversaries. This portion of the system is largely hardware-based and includes components such as barriers, detectors, and associated computers. Personnel that provide detection and delay, such as guards in fixed positions, are also included. A range of hardware configurations which address all of the safeguards concerns identified in the first step is developed for each alternative facility design. By using path-analysis techniques, each configuration is evaluated to obtain an estimate of its relative effectiveness. Those configurations that meet minimal performance and cost constraints are considered further in the third step.

In the third step, hardware and response force trade-off analysis, complete physical protection designs are developed by combining a range of

guard response options with the hardware-based configurations selected in the second step. In developing the guard response options, attributes such as numbers, armament, and protection are considered. Each design is evaluated to determine the relative level of protection provided by the particular combination of facility design, hardware design, and response force attributes. These designs are compared to select the most effective and economical design for detailed development and implementation.

The interrelationship of the three steps is shown in Figure 1-2. Not shown on the diagram are the iterative steps that may occur in the design process. For example, if during the comparison of hardware-based safeguards systems configurations with performance criteria, none are found to be adequate, then it may be desirable to develop and evaluate new options, or it may be desirable to return to the first step and make changes in the facility design and repeat the entire analysis.

Performance Measures

The methods and models described in this report provide a means of comparing the performances of various physical protection system designs. Three increasingly sensitive measures of physical protection system performance are used. Each measure is used to evaluate the ability of the system to counter a specific adversary action sequence; however, computer codes may be used to evaluate a number of adversary action sequences for each design. An adversary action sequence is an ordered set of specific

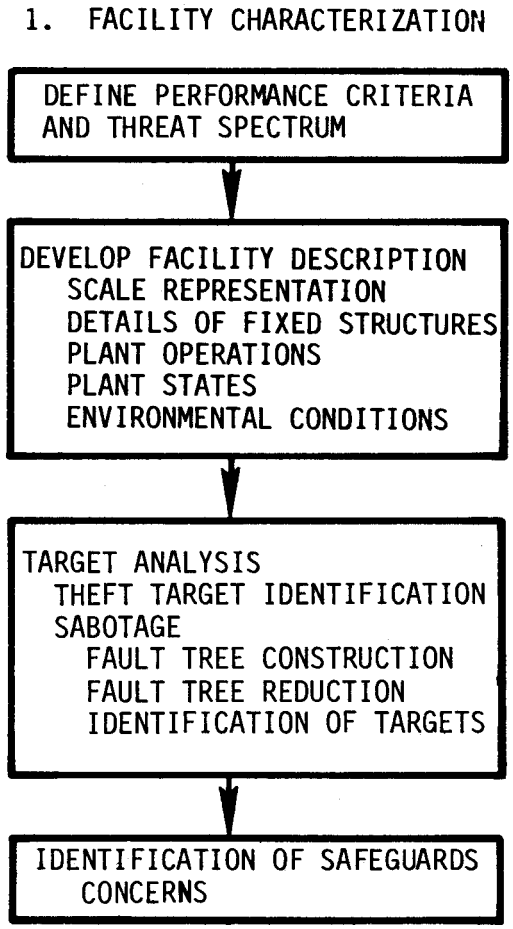


Figure 1-2. Design Approach

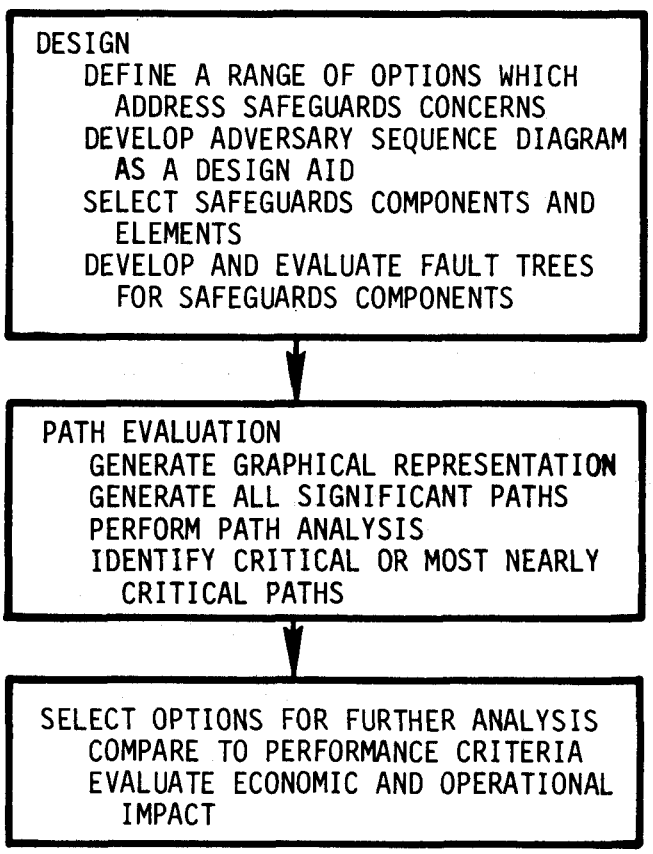


Figure 1-2. Design Approach (continued)

3. HARDWARE AND RESPONSE FORCE TRADE-OFF ANALYSIS

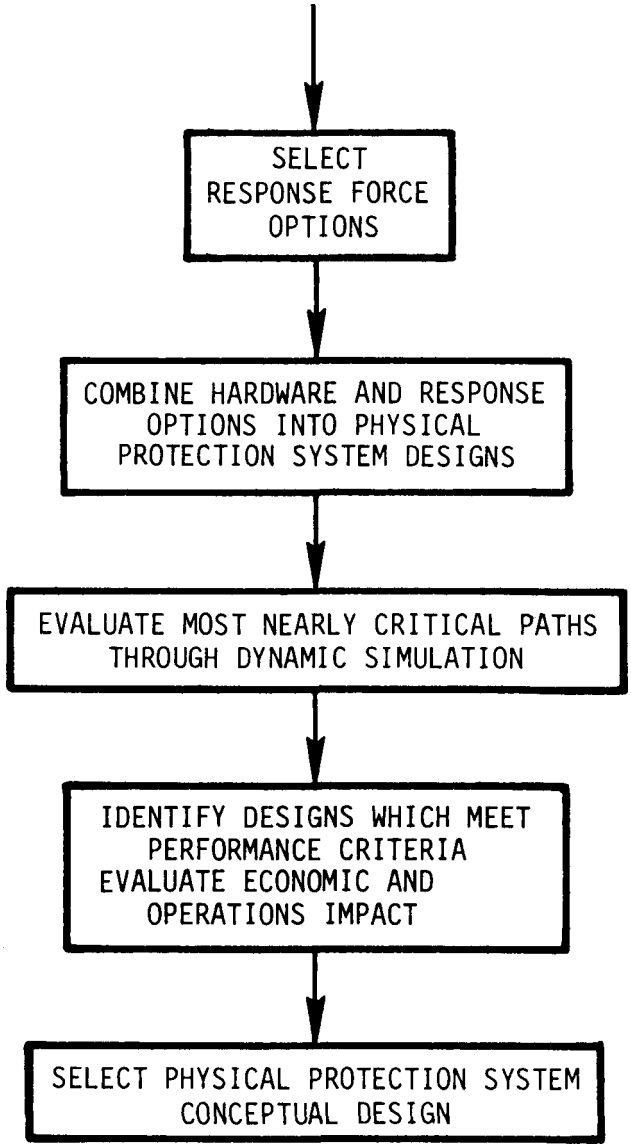


Figure 1-2. Design Approach (continued)

acts which, if completed, could result in successful sabotage or theft. Each act in the sequence is characterized, for the purpose of analysis, by the probability that the act may be detected and by the length of time required for the completion of the act.

The first measure of performance is an estimate of the detection and delay capabilities of the hardware-based portion of the physical protection system. By using path analysis techniques, the system is evaluated to determine the probability that an adversary will be detected during an adversary action sequence before the time remaining in the sequence becomes less than a postulated time for initial response. This measure can be rapidly calculated for a large number of adversary action sequences and thus can be used as a crude filter to determine which sequences are of the most concern for a particular physical protection system design.

A second measure of the performance of the system is the estimate of adversary sequence interruption. This is an estimate of the probability that the system will detect an adversary action and communicate an alarm to the response force while there is still sufficient time remaining in the action sequence of the adversary for the force to respond and interrupt the sequence. The response force is characterized by a distribution of response times; since the results of an engagement are not evaluated, other response force attributes, such as armament, are not required. Distributions of times required for adversary tasks are also used in the calculation. The use of the distributions provides increased sensitivity to system performance; this performance measure may be used to further determine which adversary action sequences are of concern.

The third measure of performance is the conditional probability of adversary sequence completion. This is the probability that, given an attack, adversaries will be able to complete their action sequence. This measure requires an evaluation of the results of a confrontation between adversaries and the response forces, and thus more closely represents the effectiveness of the total physical protection system. The models currently in use allow evaluation of response by several groups of guards over a period of time, and thus allow evaluation of a number of response force options as well as hardware designs. These calculations are quite time consuming, however, so it is desirable to use the other performance measures to limit the number of adversary action sequences which must be investigated.

Technology Transfer

As areas of the safeguards technology are developed, they are transferred to industry through technical reports, handbooks, standards, journal papers, briefings, and training programs. Documents which will provide useful reference for physical protection system conceptual design are described briefly in appendix B.

CHAPTER II

FACILITY CHARACTERIZATION

The objective of this step is to develop a facility characterization which will include all of the technical information necessary for physical protection system design. The information required for this step includes the overall physical protection system performance requirements, the range of threat attributes to be considered in the design, and the descriptions of facility buildings, processes, and systems. This information is used to perform theft and sabotage target analyses and to identify safeguards concerns for the facility. Facility characterizations which include alternative process and facility layouts can also be developed in this step.

Overall System Performance Criteria

To perform the conceptual design, the performance criteria for the facility must be specified. The source of the performance criteria may be government requirements, such as NRC regulations or DOE manual chapter requirements, and the level of protection desired by the owner. The basic requirements for the physical protection system will be defined by the performance criteria.

Threat Spectrum

To make an informed choice among possible safeguards options, the relative effectiveness of each option must be evaluated against a spectrum of threats. By investigating effectiveness against a range of threats

rather than a single threat, it is possible to show the sensitivity of conclusions to assumptions concerning threat attributes. Furthermore, if the threat spectrum is broad enough, the analyses will show the threats for which each option provides adequate protection and the deterioration of the system as threat levels increase. This approach is particularly relevant considering the presently evolving perception of the threat.

Due to the lack of applicable nuclear-related incidents, nonnuclear incidents, such as terrorist assaults, robberies, burglaries, and bombings, have been investigated to establish a data base for estimating the range of credible theft, diversion, and sabotage threats to nuclear facilities.[21-30] Additional investigations are in progress at this time.

The adversary attributes that should be considered include

- plant access (outsiders with no authorized access, employees or visitors with access, or outsiders in collusion with employees),
- number of adversaries,
- mode of transportation (foot, all-terrain vehicles, helicopters),
- weapons (side arms, automatic weapons, etc.),
- explosives,
- special equipment (self-contained breathing apparatus, etc.),
- technical and military skills,

- knowledge of plant operations and layout,
- knowledge of safeguards systems, and
- dedication (willingness to risk death or capture).

Facility Description

A facility description is required which includes information about facility buildings, processes, and systems. This information will be used both in the theft and sabotage analysis and in the development of physical protection system designs.

A representation of the facility must be prepared which shows all significant features of the facility site and buildings. Facility layouts must be obtained which show the site boundary, access points, building locations, and plan and elevation views of all significant buildings. All doors, gates, hatches, vents, and other openings in structural surfaces must be identified and classified according to the type of access allowed. Types of access include uncontrolled openings which allow free access, controlled openings which require identification for passage, and one-way emergency exits. Details of the construction of all fixed barriers and controlled openings should be provided to facilitate later estimates of barrier delay capability; however, internal walls and other fixed barriers which contain uncontrolled openings need not be investigated since access can occur through these openings.

In this step, a knowledge of facility operations is required for performing the target analysis. Considering subnational threats, the principal

safeguards concern for a light water reactor (LWR) is sabotage, whereas for a facility where SNM is present in easily handled forms, such as a fuel processing facility, both theft and sabotage are principal concerns. These facilities are considered separately in this report as examples of sabotage and theft targets, respectively.

For a light water reactor, information is required concerning the operation of systems such as

- the primary system,
- the shut-down system,
- the emergency core cooling system,
- the radioactive waste system, and
- the fuel storage and handling system.

Detailed information is required for these systems and their auxiliaries, such as instrumentation and control, power sources, and cooling. The information required includes operating procedures, system and component capacity and redundancy, system interconnections, and locations of system components and auxiliaries. In addition, the personnel interface with these systems and the access requirements to areas containing these systems must be understood.

For a fuel processing facility, the information required includes

- material input, location, output, and flow rates,
- process descriptions, item handling, and storage operations,
- personnel locations, flow, and access requirements, and

- normal, maintenance, and emergency procedures.

Information concerning the effect of various plant states on plant operation will be required both in target identification and in safeguards system design. Plant operation during different plant states may vary in areas such as personnel location and flow, plant system requirements, and SNM location. For example, during the refueling and maintenance period at a reactor, targets and access requirements would be different from those during normal operation. During refueling, the high pressure injection system would not be a target since the reactor would be depressurized, and access to this system for maintenance could be allowed. The primary system would, however, remain a target, and access control for the containment area would be affected by the large number of workers present during refueling. Many plant states can be identified, but usually only a few states will have significantly different safeguards requirements.

As an example, Figure 2-1 shows a hypothetical derivation of five plant states for an LWR. The derivation process excludes conditions that are either unlikely, impossible, or do not present a significant difference in safeguards concerns. These five plant states are combinations of reactor/reactor vessel states and plant general operation mode

1. Normal Operations

2. a. Limited Maintenance with reactor at power. In this condition, a few outside maintenance personnel can be in the operating areas of plant.

   b. Limited maintenance with reactor hot but not producing power. In addition to state 2a considerations, depending upon the duration of time since

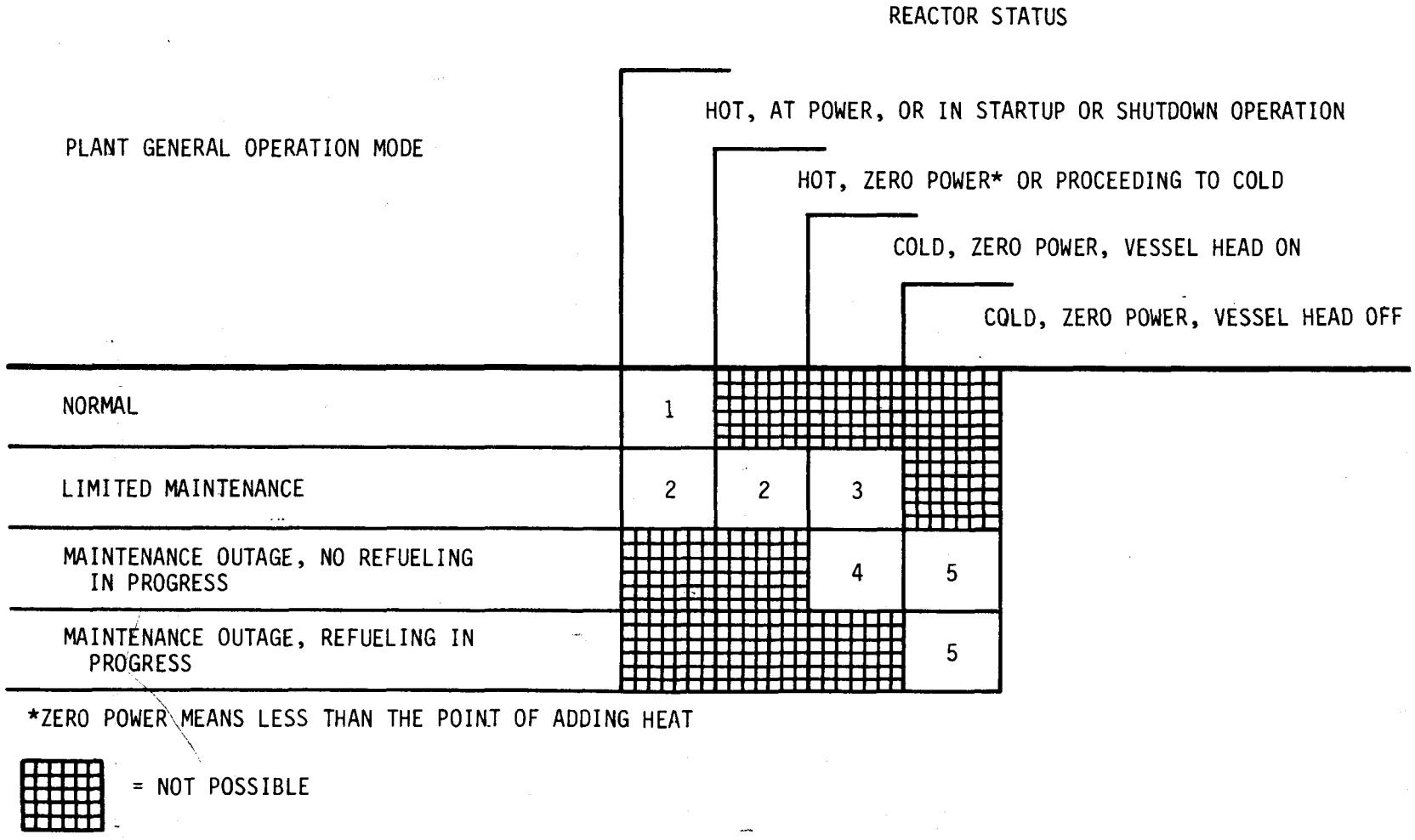


Figure 2-1. LWR Plant State Derivation Matrix

shutdown, the fission product inventory may be somewhat reduced. However, for analysis and ESS purposes a and b are essentially the same.

3. Limited maintenance with reactor cold and shut down. In addition to state 2 considerations, the consequences of a sabotage event are reduced.

4. General maintenance outage with reactor vessel head in place on the vessel. The difference between this state and state 3 is that a large outside construction labor force will be in the plant.

5. General maintenance outage with reactor vessel head removed. In addition to state 4 considerations, the fuel is in a more vulnerable state. Whether or not refueling is actually in progress does not affect safeguards requirements.

Information about environmental conditions in various areas of the facility must also be included in the facility description. Environmental conditions can determine the type of safeguards components selected, since weather conditions, electromagnetic interference, and interior noise, heat, and humidity may degrade performance. In addition, factors such as soil type can affect installation and maintenance costs. The effect of adversary-induced conditions may also have to be considered in the target analysis and safeguards system design. For example, plant or safeguards

equipment might fail if exposed to extreme conditions caused by adversary-induced steam release. The range of environmental conditions should be ident fied for all significant interior and exterior areas. Some extreme conditions such as a hurricane, may be identified as being outside the range of conditions to be considered in the design. These conditions would require the adoption of special security or operational procedures.

Target Analysis

The purpose of target analysis is to systematically identify the locations and characteristics of all potential targets in the facility and then to derive the list of targets which must be protected. All events or combinations of events that could lead to loss of SNM or dangerous release of radioactive material must be identified.

Theft targets are identified in the facility by determining all locations which may contain SNM. Each target is characterized by type of SNM, concentration, quantity, form, packaging, and handling or storage procedures. All areas which contain targets are identified as target zones.

A systematic method must be used for identifying all acts of sabotage which could lead to dangerous release of radioactive material. First the criteria that define dangerous release of radioactive materials must be determined. These criteria can be obtained from regulations or manual chapters. Then an analysis must be performed to determine whether sabotage of a particular component, possibly combined with sabotage of other components, can lead to radioactive release. One way of doing this is to analyze the facility on a functional basis using fault trees.

The top event of a sabotage fault tree is the significant release of radioactive material. The bottom of the tree contains all of the initiating events which might be performed by an adversary. The remainder of the tree indicates how an initiating event may, in combination with other events, cause the top event.

Figure 2-2 shows the top of a sabotage fault tree for a light water reactor. A systematic method for developing a sabotage fault tree for a light water reactor has been developed at Sandia under NRC sponsorship;[20] this method will be demonstrated in the report "Concept Definition for a Physical Protection System for a Typical Pressurized Water Reactor."[31] The fault tree is developed from the top down in terms of release under different plant operating conditions. Figure 2-3 shows the expansion of the tree for release during reactor operation. Under "release occurs due to fuel melt," the functional failures are indicated, mainly as failures that require mitigating systems and failure of the mitigating systems. The functions and systems that are required are identified through studies, such as the Reactor Safety Study[32] and the reactor safety analysis reports, and are coupled logically into the fault tree.

Once the tree is developed to a system level, previously developed generalized trees are used to complete the remainder of the tree. Each system that appears in the tree must be outlined logically with all system components and redundancies indicated. Each component is analyzed through a generalized tree, as shown in Figure 2-4. The generalized tree indicates all the ways a component could be sabotaged. Only the appropriate branches are included in the specific component tree; each specific tree that is developed can be used for other identical components. When the tree is fully developed,

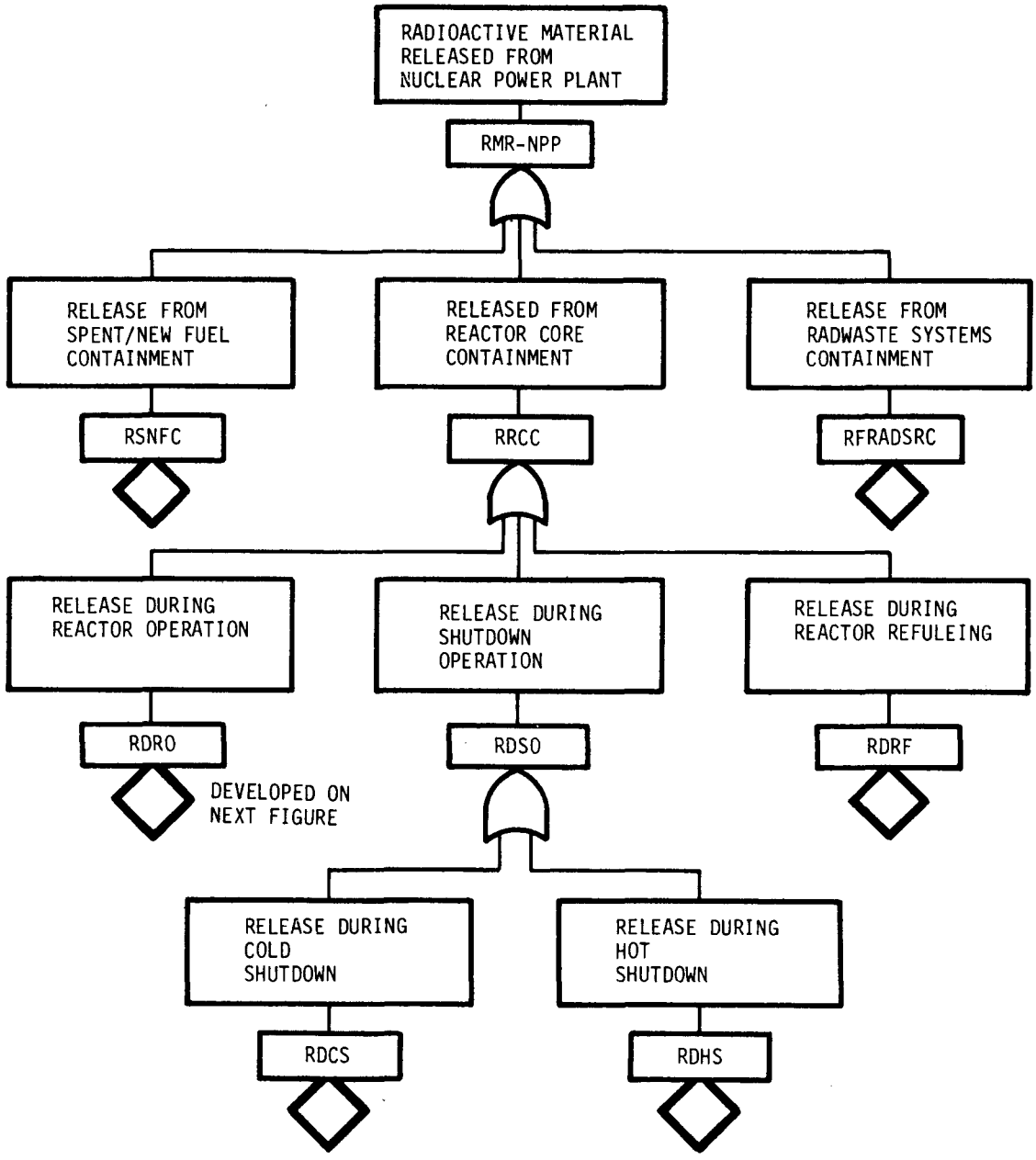


Figure 2-2. Fault Tree for Reactor Sabotage

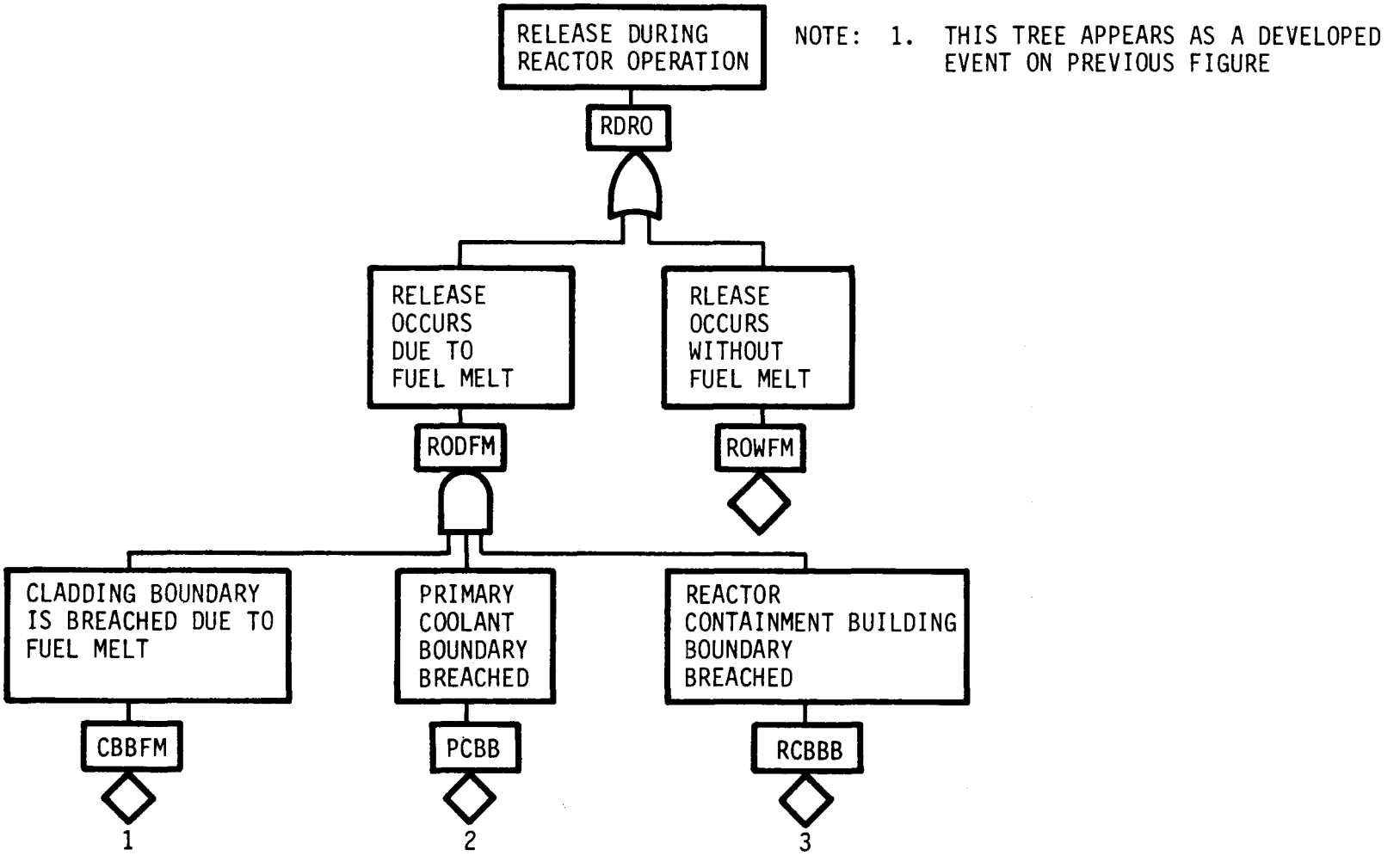


Figure 2-3. Fault Tree for Release During Reactor Operation

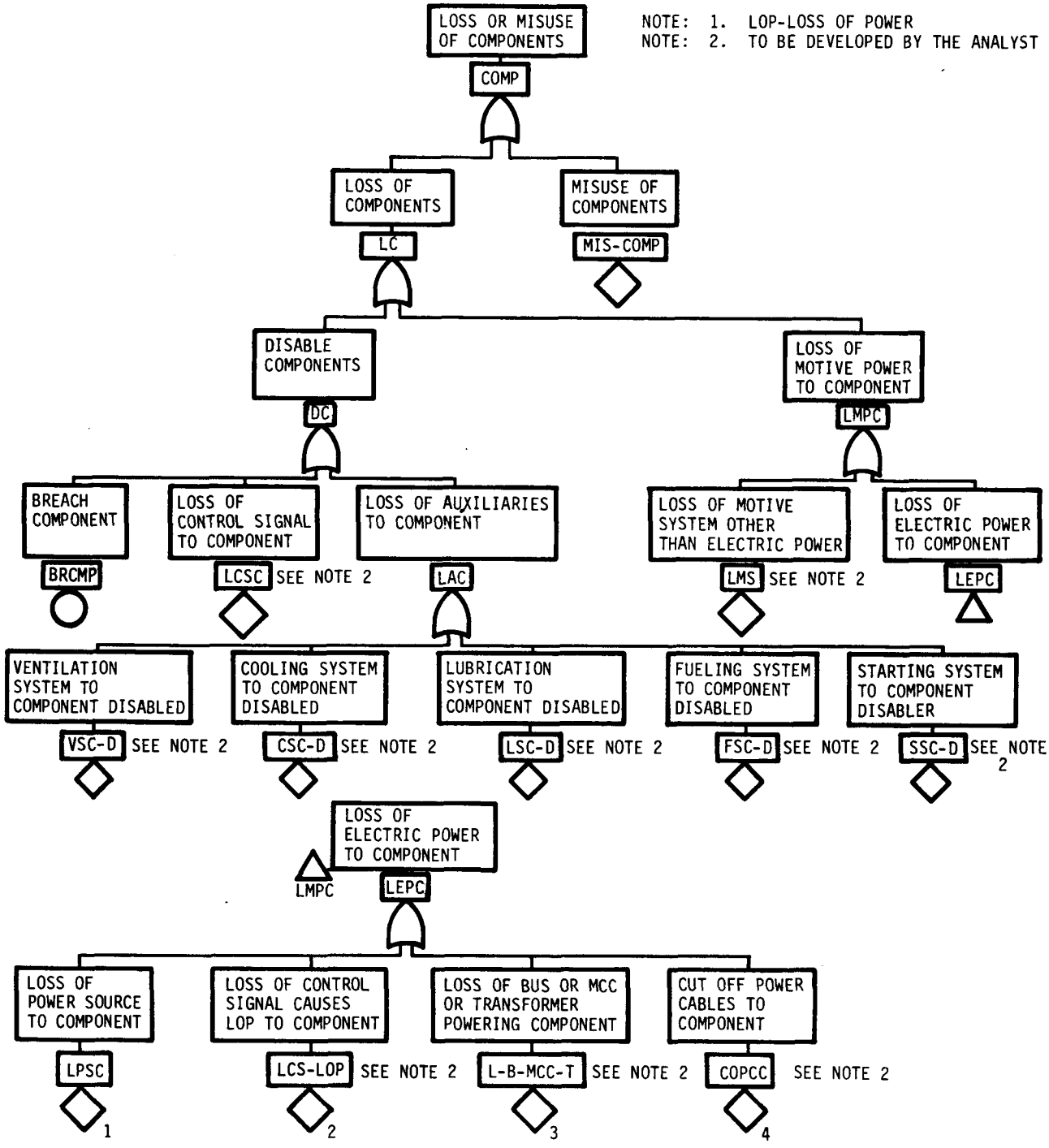


Figure 2-4. Fault Tree for Component Sabotage

the bottom of the tree will contain all the basic events which, if initiated, could possibly lead to radioactive release. Each event will correspond to a single component which is then identified as a possible target.

To minimize the size of a physical protection system, it is desirable to reduce to a minimum set the number of sabotage events to be prevented. The prevention of this set of events will assure that the top event, radioactive release, does not occur. Through the use of a computer code such as SETS[14 15] fault trees can be reduced. The fault tree must be complemented, so that the top event is no radioactive release and the basic events are prevention of some act of sabotage; for example, prevention of pipe severing. Then the cut sets for the complemented tree can be obtained. These cut sets are groups of basic events which can cause the top event. For the complemented tree, the sets of basic events will indicate sets of sabotage acts which, if prevented, will mean radioactive release is prevented. Each event which must be prevented is associated with a target to be protected, and each area that contains one or more targets is identified as a target zone. If it is not readily apparent which group of targets will be easier to protect, it may be desirable to analyze more than one set of targets during the physical protection system design stage.

Identification of Safeguards Concerns

The results of the target analysis are combined with the facility description to identify the safeguards concerns for the facility in terms of the threat spectrum being considered. Operational activities and personnel flow within each target zone are considered in developing general safeguards

concerns such as the following:

- unauthorized persons may attempt to disable vital equipment,
- unauthorized persons may attempt to enter a target zone to steal or disperse SNM,
- persons with authorized access may attempt to bring contraband (explosives, weapons, etc.) into a target zone to facilitate theft or sabotage,
- employees may attempt to falsify records in a computer to facilitate theft or diversion,
- SNM may be stolen during manual repair operations,
- handling equipment may be used to facilitate theft or diversion, and
- SNM may be hidden in transport vehicles or containers and removed from the facility with an authorized shipment.

Specific concerns for each target will identify the type of protection necessary. For example, if the safeguards concern for a particular valve is that its opening might release radioactive material, then the physical protection system must prevent unauthorized opening of the valve.

For a facility which is under design, safeguards concerns can be identified which could be met, at least in part, through modifications in the

plant design. In these cases, alternative facility layouts and processes can be developed. New facility descriptions and target analysis may also be necessary for these alternatives.

CHAPTER III

HARDWARE-BASED SAFEGUARDS SYSTEMS CONFIGURATIONS

In this step, hardware-based safeguards systems configurations which address all of the safeguards concerns identified in the previous step, "Facility Characterization," are defined and evaluated. The purpose of the hardware-based portion of the physical protection system is to detect all unauthorized activities and to provide delay of adversary actions until an appropriate response can be made. This portion of the system is largely hardware based and includes components such as barriers, detectors, and associated control and display systems. Personnel that provide detection and delay, such as guards in fixed positions, are also included.

Various levels of protection are obtained by placing detection and delay components at different locations and/or by increasing the quantity and quality of these components. By using path-analysis techniques, each configuration is evaluated to obtain estimates of its relative effectiveness and to identify its most vulnerable paths. Preliminary cost estimates are made for each configuration; those that meet minimal performance and cost constraints are considered in the next step, "Hardware and Response Force Trade-Off Analysis."

Design

A physical protection system provides protection through access control and operations control. Access control monitors and enables authorized movement of people and material through portals and other controlled access points, and prevents unauthorized movement of people, SNM, and contraband.

Operations control, which is concerned with the operational interfaces between people, vital equipment, and SNM, monitors and enables authorized plant activities within target zones and delays unauthorized actions that could result in sabotage or theft.

Both access control and operations control are forms of closed-loop control; both use monitor, control, and data processing components as shown in Figure 3-1. Monitor components measure appropriate events occurring in a given access or operational sequence. Monitored information is compared with an authorized event sequence stored in the computers of the safeguards central control system. If no discrepancy occurs, the sequence is allowed to continue; essentially, the safeguards control does not affect normal operations. If a discrepancy is detected, a decision is made to initiate a response action which is appropriate to the severity of the discrepancy. Safeguards-related problems range in severity from trivial procedural errors to serious safeguards alarms. The former can be handled by automatically informing an employee of the problem and halting further action until correction occurs. At the other extreme, an alarm indicating that theft of a canister containing SNM is in progress would require immediate response by security personnel. Initiation of response to as many situations as possible should be automatic; however, no automatic system can be so comprehensive that it covers all situations, and personnel must be available to monitor and assess complex, special situations or to request special action from management and plant operations.

Safeguards components must be selected and implemented in a way that will provide a high probability of detection of unauthorized actions and will

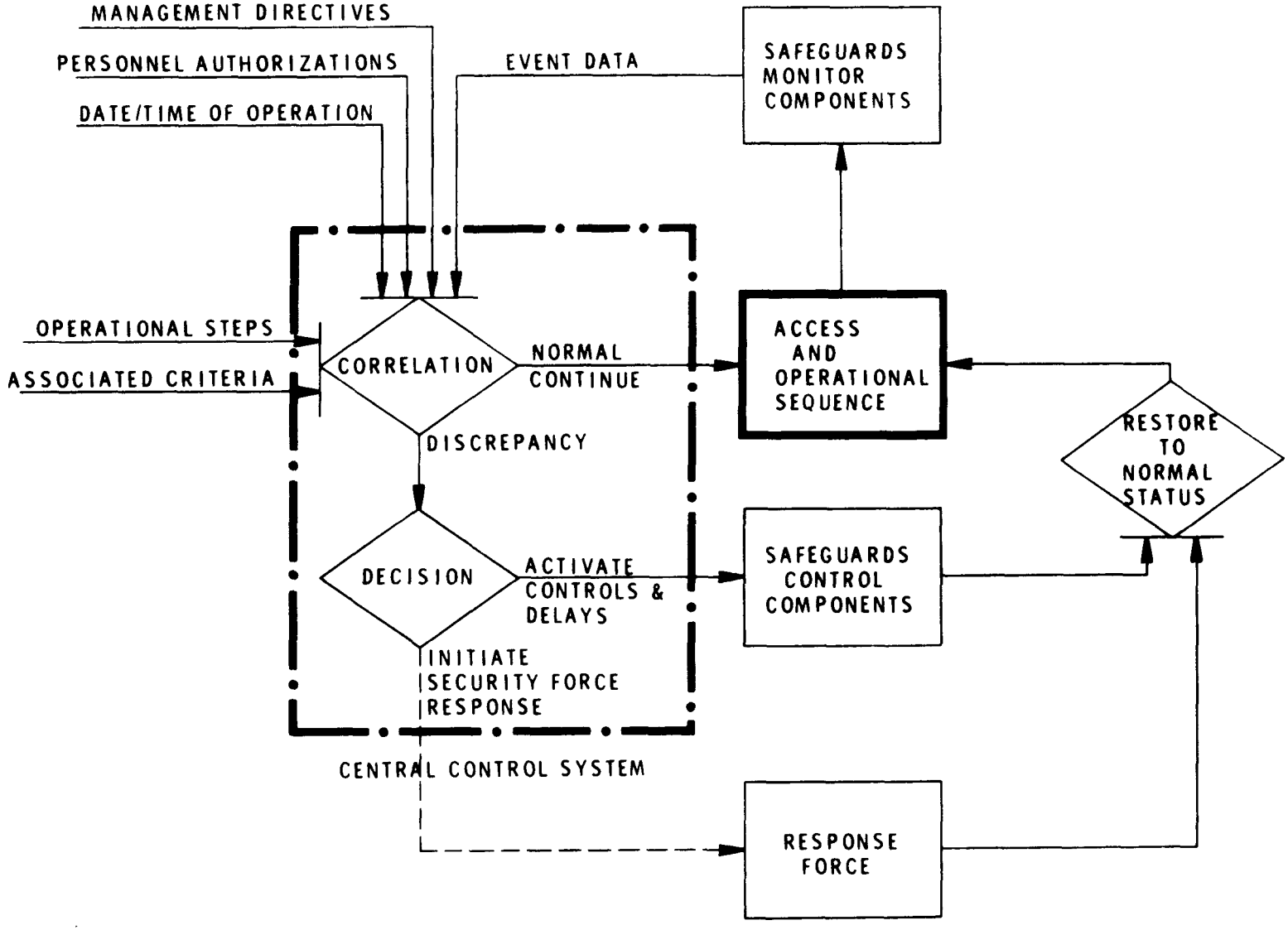


Figure 3-1. Safeguards Closed-Loop Control

provide sufficient delay after detection so that guards can respond. In addition, it is desirable to develop a physical protection system that has minimal cost and minimal operational impact. As the hardware-based systems are developed, the operational impact of safeguards components must be reviewed to assure compatibility with line process controls and flow rates, item-handling operations, health and safety considerations, maintenance procedures, and material and personnel flow rates. The relationship among materials information required for quality assurance, management reporting, materials measurement and accounting, and physical protection is also studied to avoid duplication. Information on safeguards components such as interior and exterior intrusion detectors, various types of barriers, and entry control systems is available from the handbooks described in appendix B.

Two design principles should be considered in physical protection system conceptual design. The first, protection in depth, is used to protect against single point failure. To achieve protection in depth, the physical protection system design should require an adversary to pass through several detectors and barriers to reach vital equipment or SNM. Thus, even if the adversary circumvents a detector or barrier, the system will still provide sufficient detection and delay capabilities. The second principle, balanced protection, is used to achieve maximum protection at minimum cost. Whenever possible, the system should be designed so that all similar areas in the facility are equally protected. For example, if an adversary can achieve the same result in either of two areas, it is pointless to provide a high degree of protection for just one of the areas.

For a complex facility, it is not readily apparent before evaluation what combination of safeguards components will provide adequate protection at the least cost and operational impact. Therefore, it is desirable to develop a number of hardware options using a variety of safeguards components. After evaluation, those that appear to meet minimum performance requirements can be compared in terms of cost and operational impact, and those that are the most attractive can be developed further.

An Adversary Sequence Diagram (ASD)[1] is a useful design tool that illustrates facility levels at which safeguards components and elements can be placed to provide protection in depth. In addition, by developing safeguards elements for each level in a uniform manner, a balanced protection system can be achieved. Figure 3-2 shows an illustrative facility with some safeguards components indicated. An ASD is given for this facility in Figure 3-3. In the ASD, rectangles represent areas or zones in the facility, lines represent barriers and associated detectors between areas, and triangles are used as transfer symbols to show line-segment connections without requiring line crossings. The rectangles may also represent detection and delay associated with intra-area travel and, in target zones, detection and delay associated with operations control elements.

An ASD shows the areas and safeguards elements through which an adversary must proceed. An adversary attempting to steal SNM would first have to proceed to a zone where SNM can be found and then must leave the facility; therefore, the ASD must include the areas through which the adversary exits. The ASD shown in Figure 3-3 is symmetric for this reason. A saboteur, however, may only have to reach a target zone to achieve his act of sabotage.

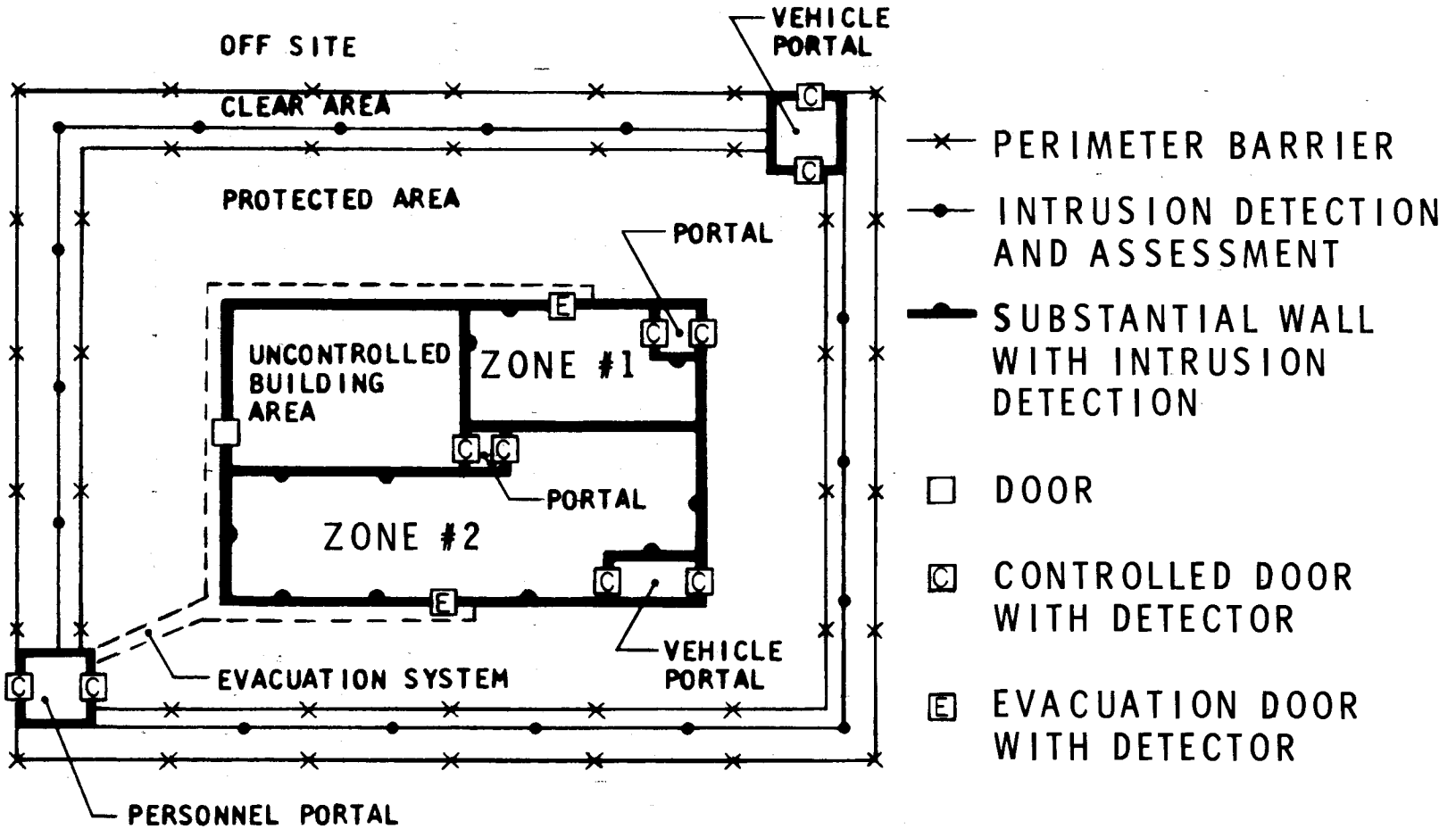


Figure 3-2. Illustrative Facility with Safeguards Components

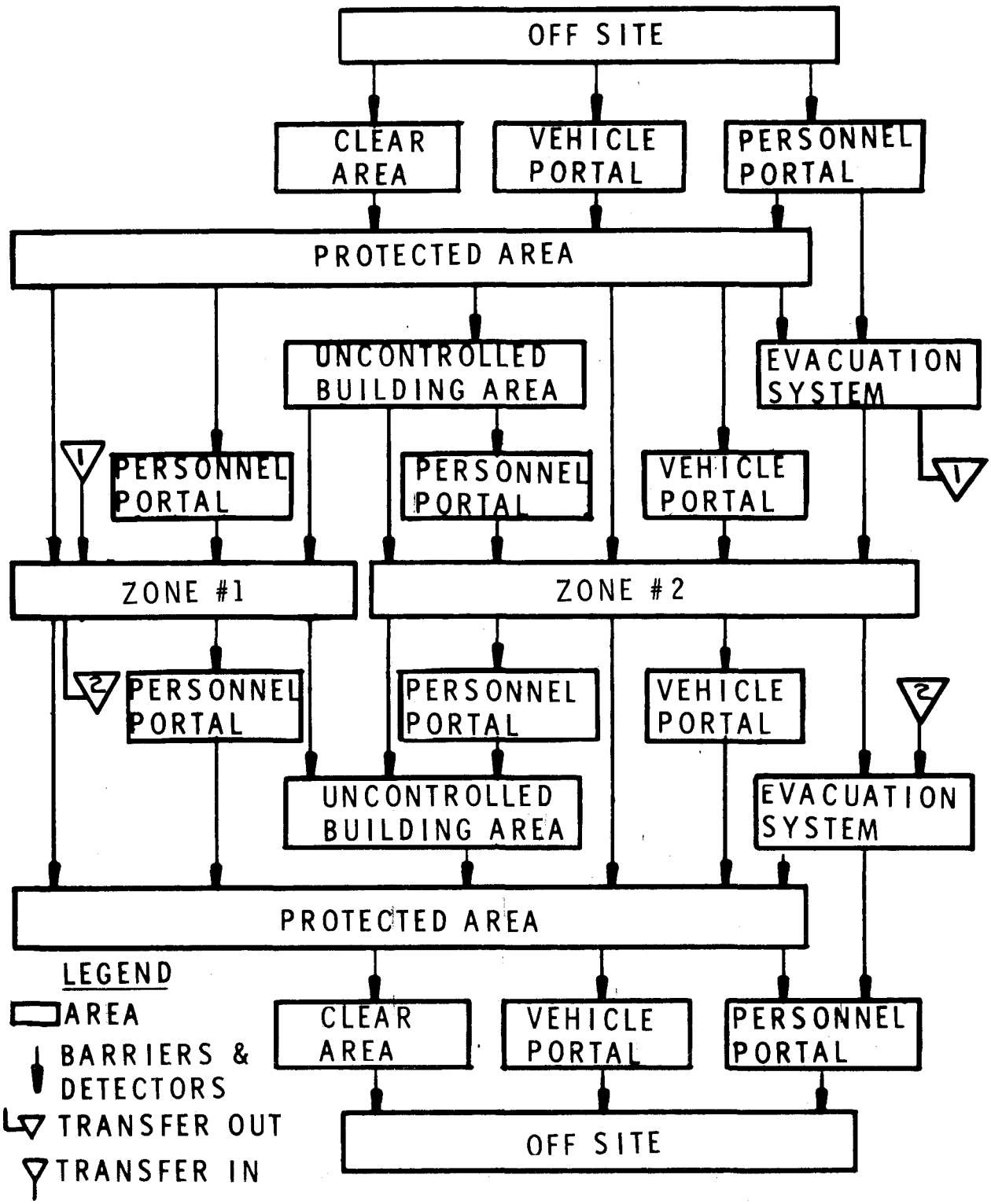


Figure 3-3. Illustrative Adversary Sequence Diagram

An ASD is similar to a region adjacency graph[18 19 33] in that two rectangles are connected by a line if the corresponding areas or zones have a common barrier or barriers between them; however, since it is the purpose of the analysis to identify the least difficult paths for an adversary, some connections which represent impractical adversary paths are eliminated from an ASD. For example, since it is reasonable to assume that it is easier for an adversary to penetrate one barrier rather than several of equivalent or greater difficulty, indirect routes among areas need not be included.

To evaluate the effectiveness of a physical protection system design, it is necessary to estimate the detection and delay capabilities of the safeguards elements used in the design. Examples of generalized fault trees developed for this purpose are shown in Figures 3-4, 3-5, and 3-6.[35] Each generalized tree indicates the various ways a particular type of safeguards element can be defeated. Only appropriate branches are included when these trees are applied to specific elements. Each tree is evaluated twice for each set of threat attributes. The tree is evaluated once to obtain the minimum probability of detection of an adversary. This is achieved by determining from the fault tree the particular combination of actions which are least likely to be detected. It is evaluated again to obtain the minimum delay time associated with the fastest means of penetrating the component. To do this, it is necessary to estimate the detection probability and delay time associated with the basic events, such as the probability of detection of and the time required to penetrate a wall for an adversary equipped with high explosives.

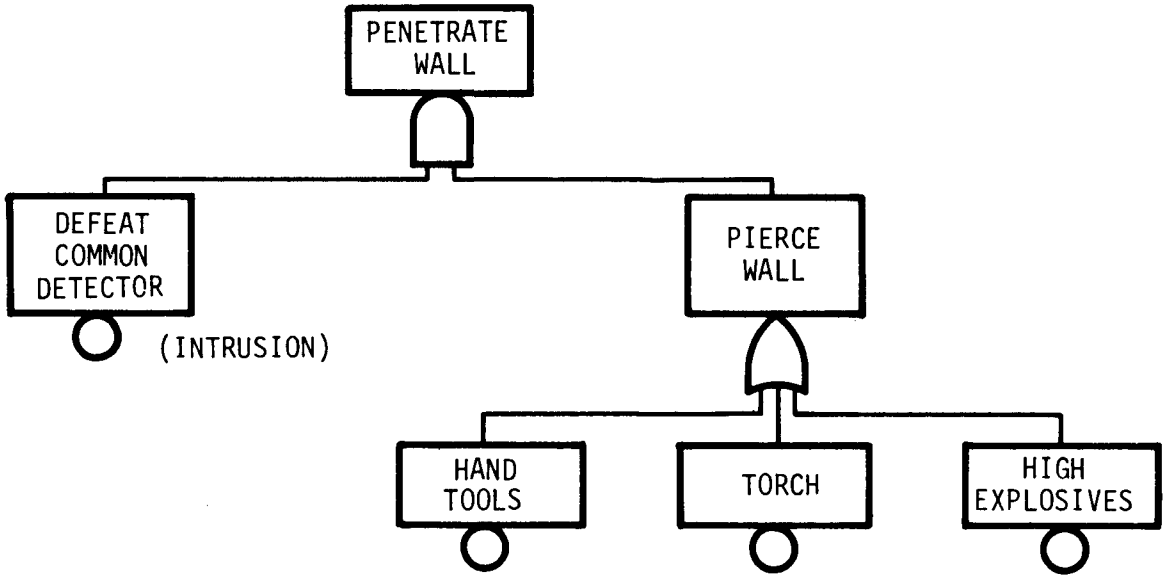


Figure 3-4. Fault Tree for a Wall

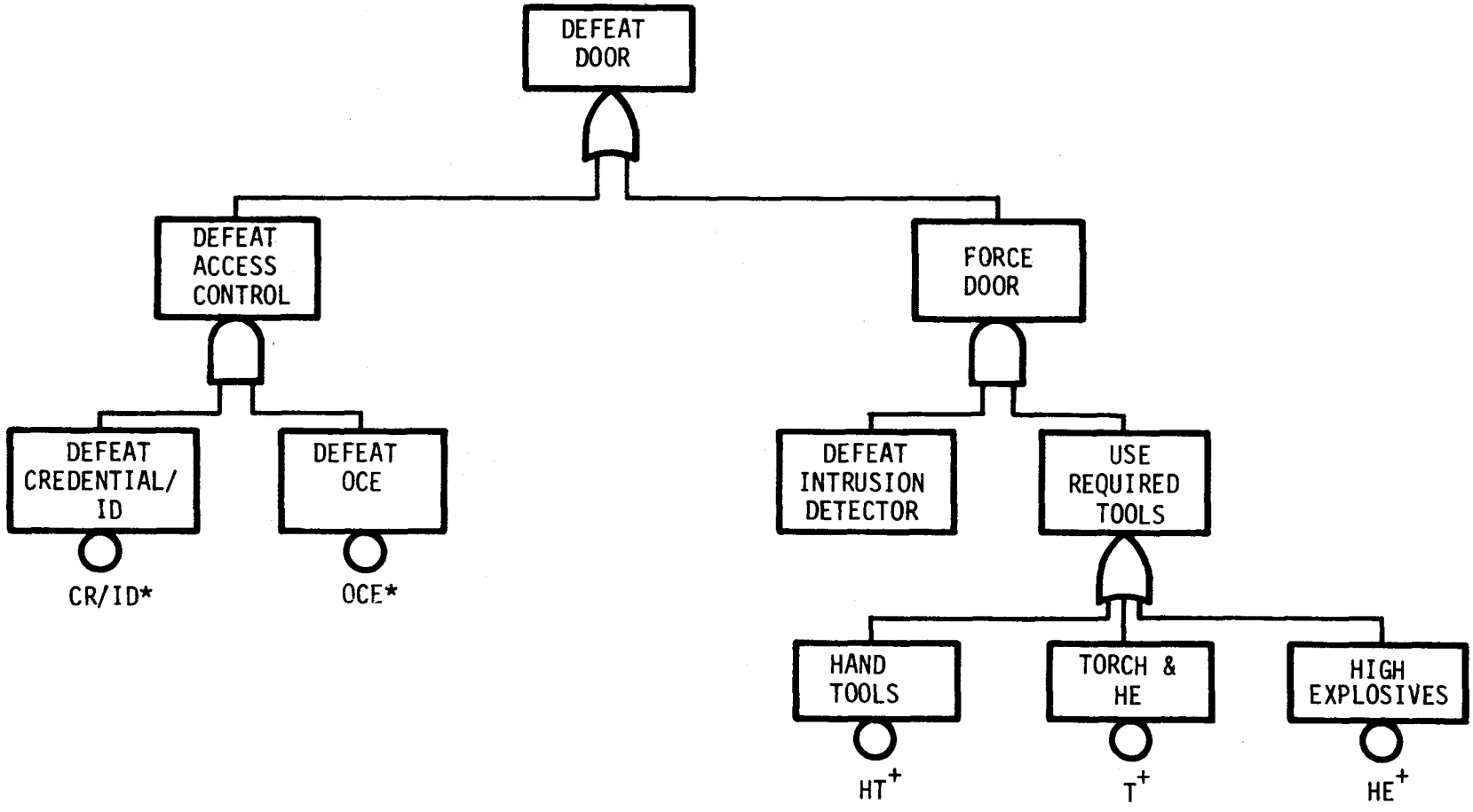


Figure 3-5. Fault Tree for a Door

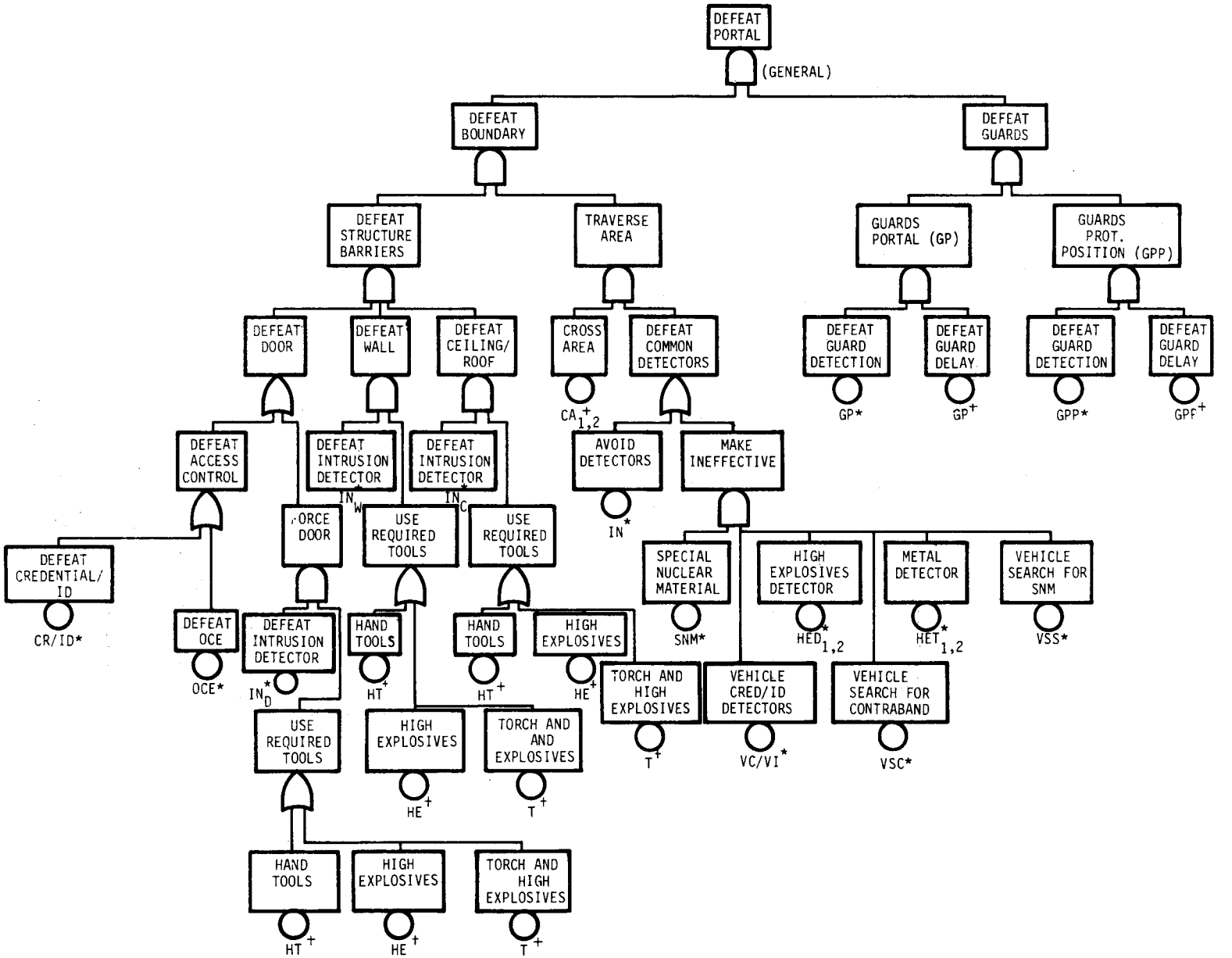


Figure 3-6. Fault Tree for a Portal

In the conceptual design stage, detailed descriptions of safeguards elements may not be available. In this case, detection probability and delay time can be estimated for general classes of components, and these estimates can be used as performance specifications when selecting specific components for implementation. The Intrusion Detection Systems Handbook, Entry-Control Systems Handbook, and Barrier Technology Handbook described in appendix B may aid in arriving at the estimates of the effectiveness of some types of safeguards components.

These fault trees can be evaluated manually or by a computer code such as SETS.[14,15] The use of SETS to analyze the effect of common-cause failures, such as the failure of three detectors due to the failure of a portion of the physical protection system common to all three, is discussed in Common-Cause Analysis Using SETS.[36]

Evaluation

After the hardware-based configurations have been defined and the fault trees have been evaluated, each configuration can be evaluated using path-analysis techniques to estimate the relative effectiveness as a function of the time required for initial response after detection of an adversary. The performance measure used is the probability that an adversary will be detected during an adversary action sequence before the time remaining in the sequence becomes less than a postulated time for initial response. This performance measure can be rapidly calculated for a large number of adversary action sequences and can be used to determine which sequences are of the most concern for a particular hardware-based design.

All of the significant paths for a facility are analyzed in this step. A path is a set of points into or through a facility. Associated with these points is a set of tasks which an adversary must perform in traversing these points. This set of tasks is known as an adversary action sequence. In Figure 3-7 a path is illustrated in terms of an ASD. The minimum probabilities of detection and minimum times of penetration obtained from the fault trees are indicated in the figure. Since probability of detection (P_D) and time of penetration (T_p) are minimized separately in the fault trees, they may not correspond to the same method of performing a task. For example, the fastest way to penetrate a fence may be to climb over it; however, an adversary trying to avoid detection by a fence sensor may choose a slower method of penetrating the fence. This does not affect the analysis, however, since probability of detection and time of penetration are never evaluated simultaneously for a single task.

As an adversary proceeds along a path, he encounters various detectors, as shown graphically in Figure 3-8. Each detector has some probability of detecting the adversary, so the adversary accumulates an increasing probability of detection as he proceeds along the path. Once an adversary has been detected, it is to his advantage to complete the sequence as rapidly as possible before a response can be made. A limiting sequence for a path is one for which the adversary attempts to minimize his probability of detection up to a point in the path, and then attempts to complete the path in the fastest way possible. Mathematically, this is described as follows:

Consider a path of n barriers and associated detectors where the detection system associated with the ith barrier will detect the

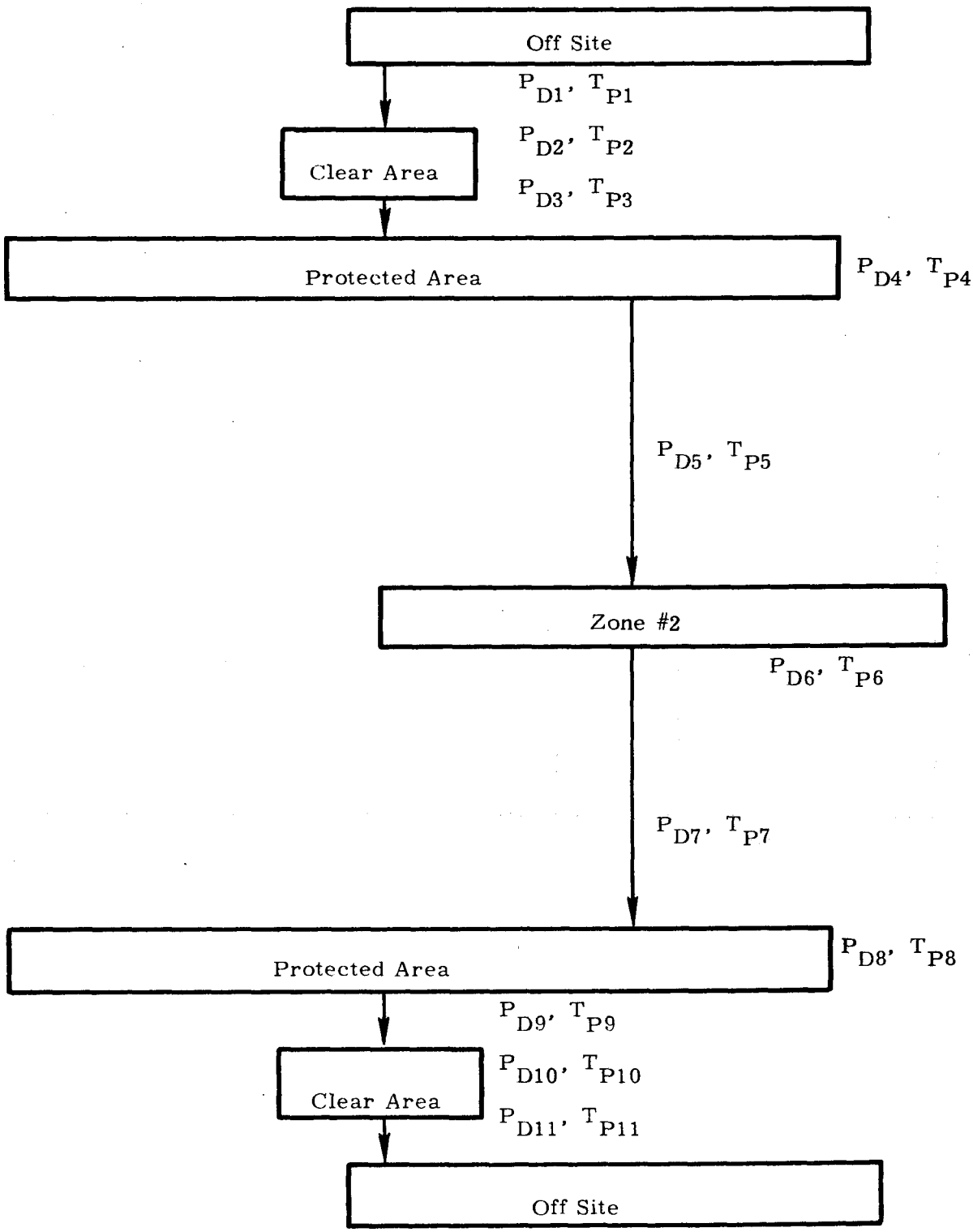


Figure 3-7. Illustrative Adversary Path

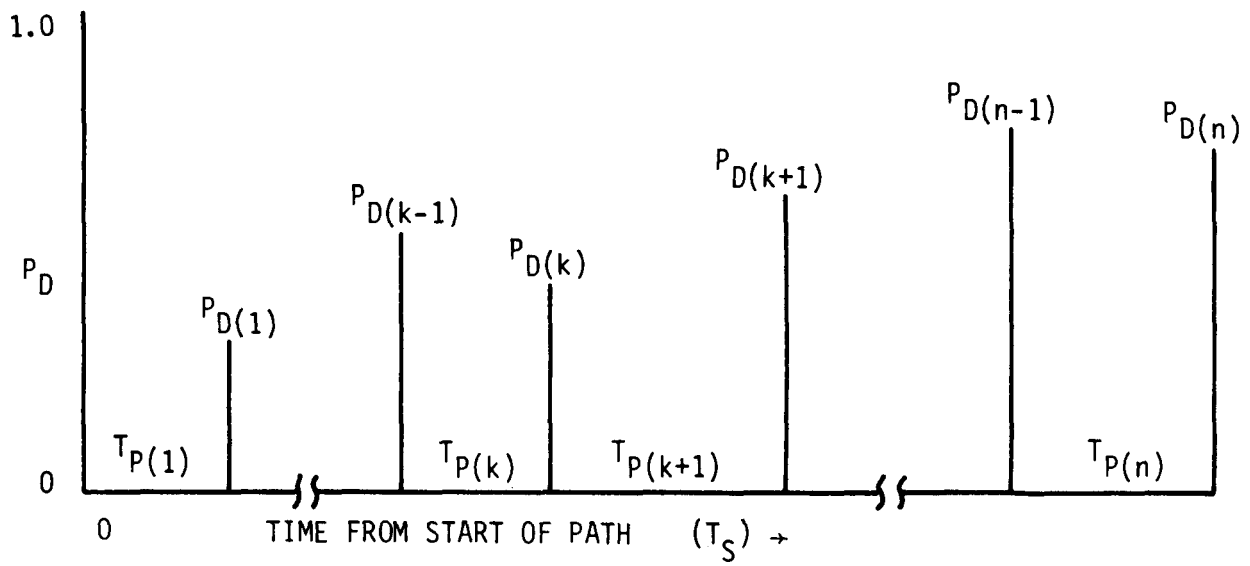


Figure 3-8. Data for an Adversary Action Sequence

adversary after the ith barrier is penetrated but before the (i+1)st barrier is reached, and where

P_{Di} is the probability of adversary detection by the ith detector, and

T_{Pi} is the time for the adversary to penetrate the ith barrier.

Figure 3-8 shows values of P_{Di} and T_{Pi} for one sequence in which an adversary with a particular set of attributes attempts to penetrate a path in a particular way under a particular set of operational and environmental circumstances. The cumulative probability of adversary detection $\left(P_{D(cum)}\right)$ at the ith detector is

$$P_{D(cum)k} = 1 - \prod_{i=1}^{k} \left(1-P_{Di}\right) = 1 - \prod_{i=1}^{k} \overline{P}_{Di} \qquad (1)$$

and the time remaining after the detector (T_{Rk}) is

$$T_{Rk} = \sum_{i=k+1}^{n} T_{Pi} \qquad (2)$$

The limiting sequence associated with the kth detector is one for which the adversary minimizes probability of detection through the kth detector and minimizes time in completing the remainder of

the path. Therefore, $P_{D(cum)k}$ and T_{Rk} are both minimum, and the values used for P_{Di} for $1 \leq i \leq k$ and T_{Pi} for $k+1 \leq i \leq n$ are the minimum values. As indicated earlier, when evaluating a sequence the minimum values for P_{Di} and T_{Pi} for a particular i are never used simultaneously.

Figure 3-9 is a plot of $P_{D(cum)}$ as a function of T_R for all limiting sequences associated with the path of Figure 3-8. If a criterion P is established as an acceptable level of detection while a criterion T is the postulated time for initial response following detection of an adversary, then an acceptable path can be defined as one which has at least one limiting sequence where

$$P_{D(cum)} \geq P \tag{3}$$

and

$$T_R \geq T \tag{4}$$

Alternatively, a critical path is defined as one that has no limiting sequence in which the above criteria are met. The path whose limiting sequences are plotted in Figure 3-9 is acceptable for criteria P_1T_1, P_1T_2, P_2T_1, and P_2T_2. The path would be critical for criteria P_1T_3, P_2T_3, P_3T_1, P_3T_2, and P_3T_3.

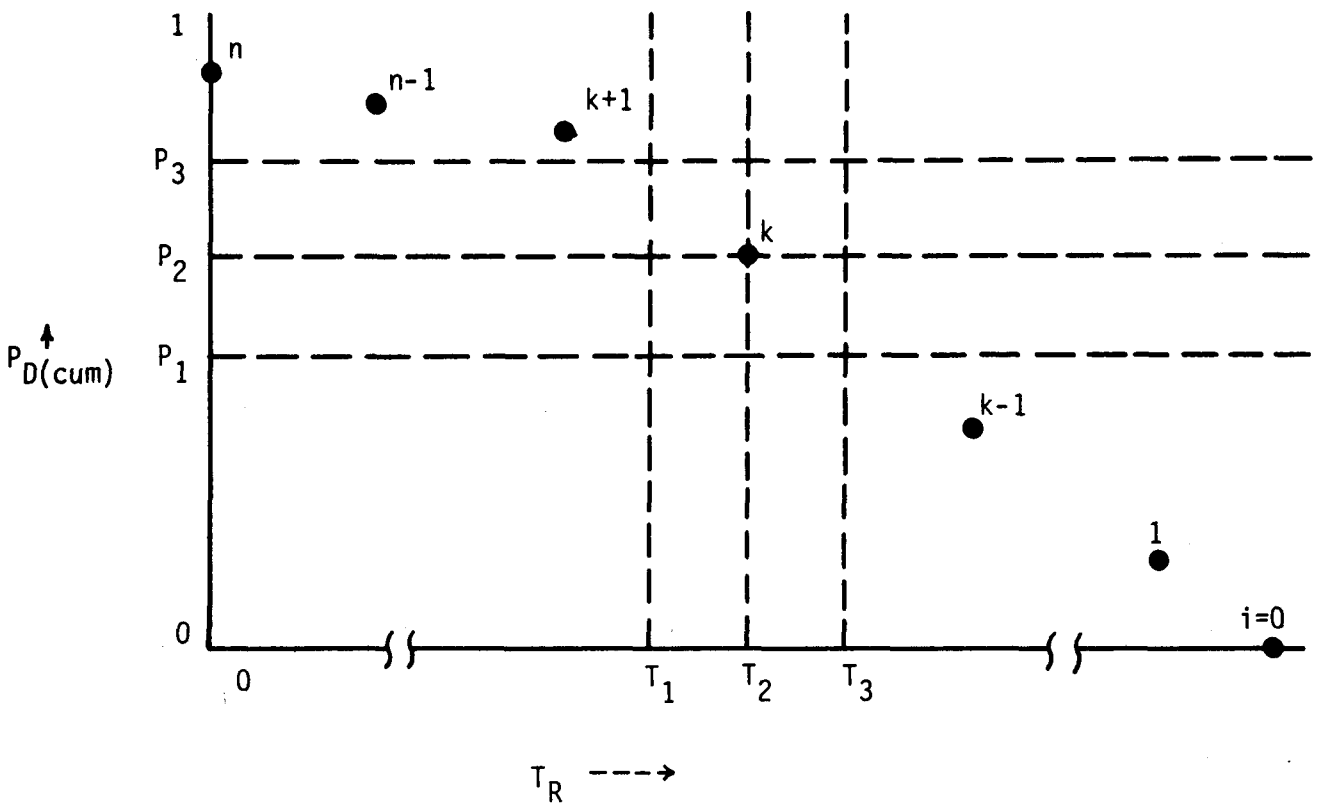


Figure 3-9. Plot of Limiting Sequences

Each path can be described by a characteristic limiting sequence for a particular time T. The characteristic limiting sequence is the limiting sequence associated with the kth detector and barrier, where

$$T_{Rk} \geq T \quad \text{and} \quad T_{Rk+1} < T \tag{5}$$

The sequences that are of the most concern are those with the lowest cumulative probability of detection, $P_{D(cum)k}$, associated with the characteristic limiting sequence. If the cumulative probability of detection is less than the criterion P, the path is critical. Conversely, if it is greater, the path is defined as acceptable for that time T.

All paths for a particular hardware configuration are analyzed simultaneously for a particular time. Those that are critical or most nearly critical are identified for further analysis. Each configuration should be analyzed for a range of times to obtain the sensitivity to the time.

Several computer codes are available for performing the path analysis; however, the codes differ somewhat in the method used to identify all the significant paths through the facility. The codes SAFE (Safeguards Automated Facility Evaulation), PANL (Path Analysis), and COPE (Critically Ordered Path Evaluation) are described in appendix B.

All methods initially utilize some type of graphical representation of the facility. If the code SAFE[17] is used for path evaluation, the graph may be in the form of a simplified facility layout, similar to that shown in Figure 3-2, upon which all safeguards elements and theft and sabotage targets

are shown. A node is associated with points of barrier penetration and associated detectors on the graph. When the graph is digitized, the code will identify all significant paths to or from all of the targets in the facility through the digitized nodes. These paths correspond directly to physical paths through the facility. This advanced technique, which is in the final stages of development, offers the potential for more rigorous identification of paths.

Other computer codes, such as PANL and COPE,[16] use an Adversary Sequence Diagram as a means of identifying all the generic paths the adversary may traverse. These paths are described as generic because the transit between any two areas in a path may represent several physical paths through a barrier, for example, entering through any one of four controlled openings in a barrier, or destroying the barrier. In addition, as described earlier, some connections between areas are systematically eliminated as being more difficult for the adversary. Although the ASD is not as complete a method of representing a facility as the graphical technique employed by SAFE, practical experience with the ASD has indicated it is adequate for concept evaluation.

Each of the three computer codes discussed performs the analysis described; however, care must be taken in specifying the input to the codes to assure that detection and delay are analyzed in the order intended by the user. The mathematical method described above specifies that penetration occurs before detection. For example, a "door open" detector will detect the opening of the door only after the door locking mechanism has been defeated. The delay for defeating the lock does not contribute to the time

remaining in the path unless the adversary has been detected previously. On the other hand, some safeguards elements which may be associated with an area in an ASD, such as an operations control element, may give detection before delay. These can be handled properly by attributing the detection to the barrier at the entrance to the area and by attributing the delay to the barrier at the exit from the area.

Care must also be taken in analyzing attacks, such as theft, in which the adversary may leave the facility through the same areas by which he entered. In this case, the path must be analyzed to determine if the detection probability and penetration time for an exit through an area is affected by previous passage through that area. For example, if an adversary destroys a barrier on the way into a facility, he will not have to destroy that same barrier again if he leaves through that same barrier. This is referred to as commonality. The user guide for the particular code to be used should be consulted to determine how the code accounts for commonality.

When the path-analysis has been completed for all hardware-based safeguards system configurations, the configurations can be compared and considered for further analysis, as shown in Figure 3-10. Those configurations that have critical paths can either be upgraded and reevaluated or can be discarded. Configurations that have acceptable performance, i.e., no critical paths, are reviewed to assess system costs and operational impact. Those that have acceptable performance as well as acceptable cost and minimal operational impact are selected for further consideration in the next step.

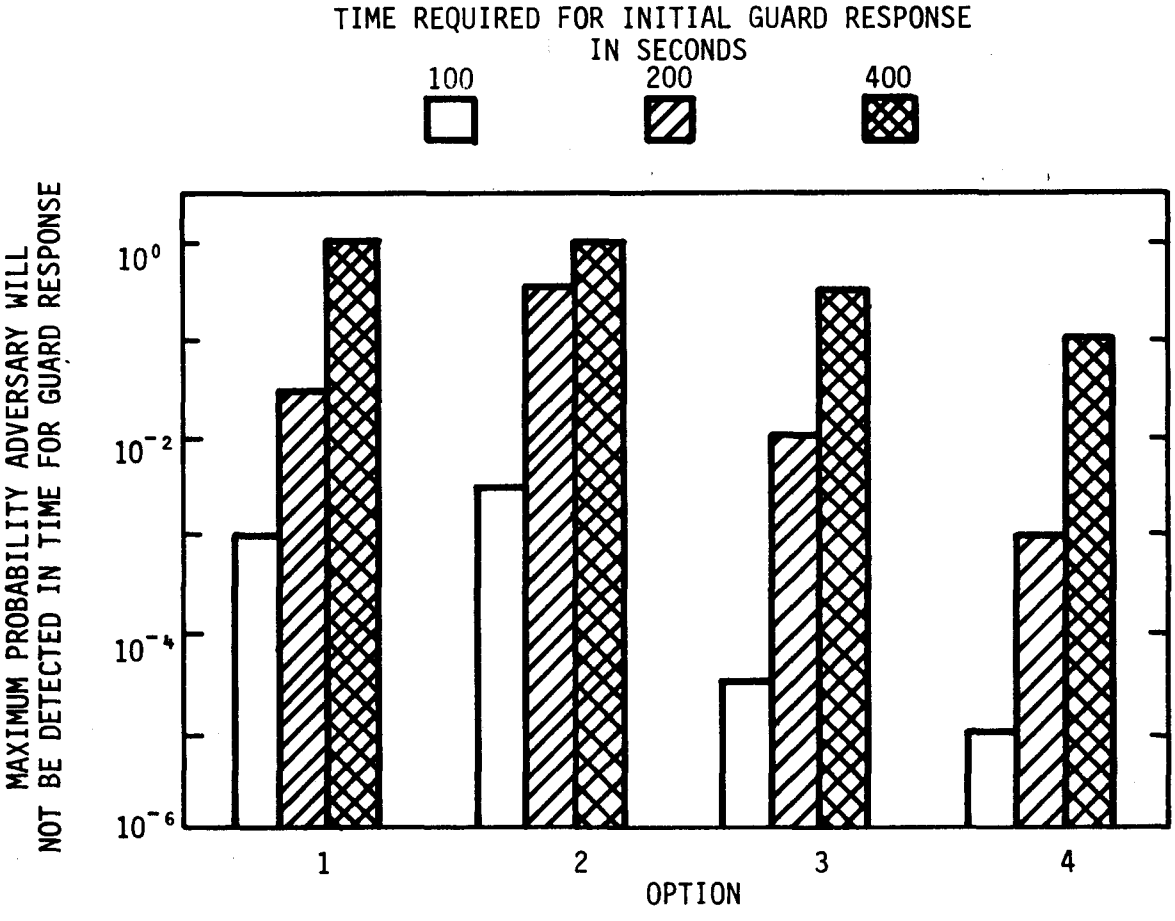


Figure 3-10. Comparison of Hardware-Based Safeguards Systems Configurations

CHAPTER IV

HARDWARE AND RESPONSE FORCE TRADE-OFF ANALYSIS

In this final step, physical protection system conceptual designs are developed by combining a range of guard response options with the hardware-based systems configurations selected in the previous step. Each design is then evaluated to determine the relative level of protection provided by the particular combination of facility design, hardware capabilities, and response force attributes. These designs are compared to select the most effective and economical design for detailed development and implementation.

Selection of Response Options

A range of response force options must be developed to complement the hardware-based configurations developed in the previous step. These options must include the guards which were associated with the hardware-based configurations, such as guards stationed in a personnel portal. In addition, the response force should be capable of providing initial response within the time criterion, T, for which the hardware-based configuration was shown to be effective. Time for initial response refers to the time between detection of an adversary and the arrival of the first group of guards to intercept the adversary. Other response groups which arrive later, such as an off-site force, may also be included in the response force options. Additional response force attributes which include number, armament, transportation, and deployment may also be considered.

Evaluation

Two performance measures are used to evaluate paths in detail: the estimate of adversary sequence interruption and the conditional probability of adversary sequence completion. The first may be calculated with the Estimate of Adversary Sequence Interruption (EASI) computer code.[67] This code estimates the probability that, given an attack, the system will detect an adversary action and communicate an alarm to the response force while there is still sufficient time remaining in the adversary action sequence for the response force to respond and interrupt the sequence. Only the probability that the guard force will arrive before the end of the sequence is calculated; the probability that guards will defeat the adversaries after they arrive is not calculated. This method uses distributions for the guard response time and the component time of penetration, so that system sensitivity to initial response time is better defined than with the performance measure used in the previous step.

EASI is particularly useful in further limiting the number of adversary action sequences which are of concern, since EASI can be rapidly run for a number of individual paths. In addition, since EASI only requires that the response force be described by initial response time, it can provide useful information in the initial selection of options for response force deployment. EASI can be run for any path; however, the computer code SAFE automatically uses EASI to evaluate the most critical or nearly critical paths in a facility.

Other computer models can be used to calculate the Conditional Probability of Adversary Sequence Completion P(ASC). This is the probability that, given an attack, adversaries will be able to successfully complete their objective

of theft, diversion, or sabotage. This calculation requires some type of engagement model to determine the result of confrontations between guards and adversaries. Dynamic simulation is used to evaluate the effects of guards arriving at different times, such as roving patrols and off-site response forces coming to the aid of a guard at a portal.

Two computer models that include confrontation simulations are currently in use at Sandia to evaluate relative physical protection system effectiveness, the Forcible Entry Safeguards Effectiveness Model (FESEM)[8-11] and the Insider Safeguards Effectiveness Model (ISEM).[12 13] A significant limitation of these models is the relatively long time required to evaluate a large number of paths in a facility. However, by analyzing only those paths identified as being of most concern in the previous step, or with EASI, this limitation can be overcome and both models can be used to explore the relative value of various response force configurations and other safeguards features.

Figure 4-1 illustrates the type of effectiveness information that is obtained from FESEM. One curve shows the conditional probability of adversary theft sequence completion for a specific adversary threat on a particular path for a baseline facility with a limited physical protection system. The other curves display results for various protection system options. Additional sets of curves would result for other adversary threats and paths. These would show sensitivity to transportation mode, level of plant access, and other adversary attributes.

The results of this effectiveness analysis are used along with estimated costs to aid in the selection of a physical protection system conceptual

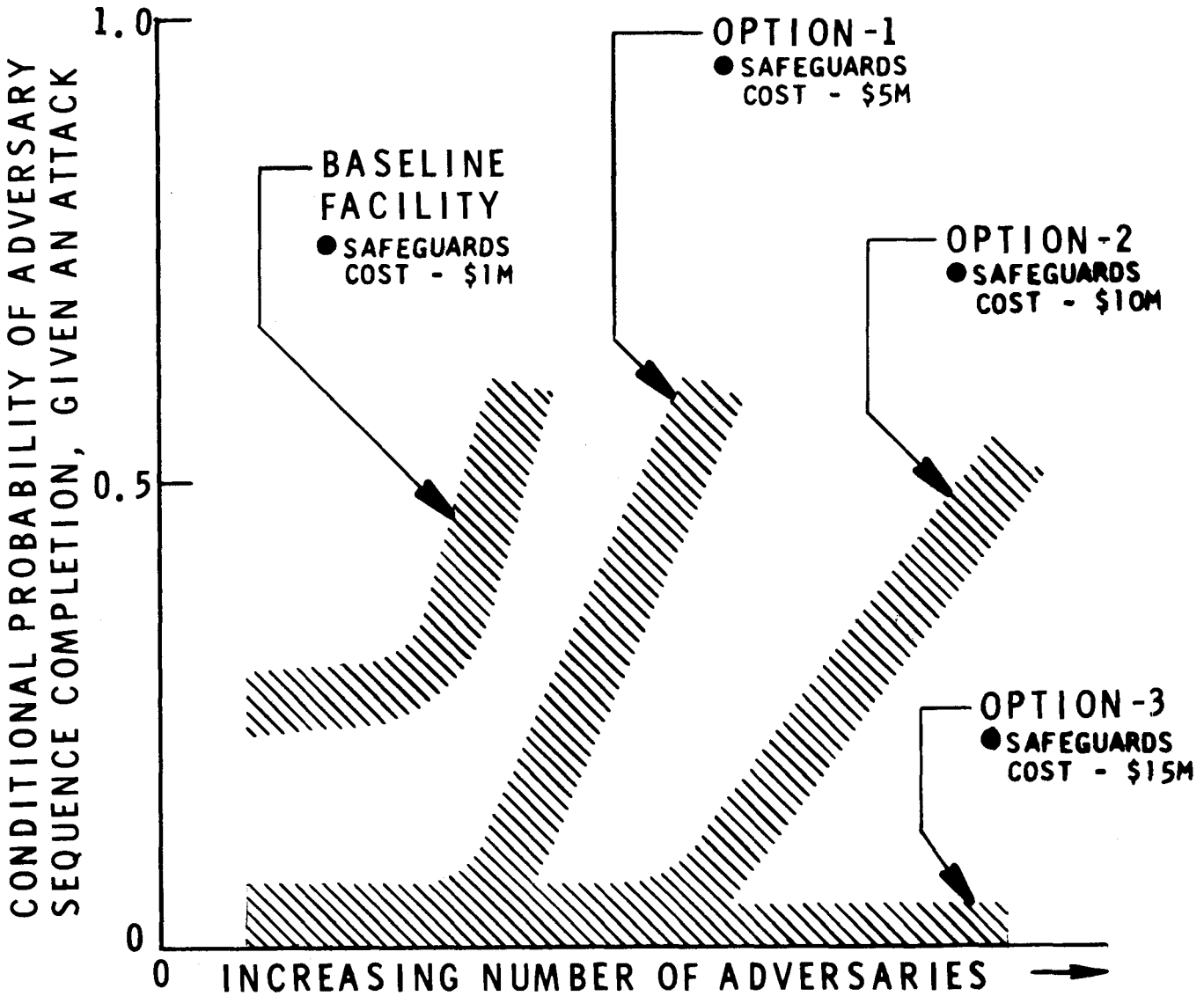


Figure 4-1. Effectiveness Analysis

design. Estimated costs must include the original system cost, including design, procurement, and installation, and the continuing costs of operation and maintenance. Data on component costs is available from the Intrusion Detection Systems Handbook, Entry-Control Systems Handbook, and Barrier Technology Handbook described in apendix B. In addition, less tangible factors such as operational impact must be considered. For a facility which is itself in the planning stage, the cost effectiveness of reducing safeguards system cost by making modifications in the facility design must also be considered. Figure 4-1 illustrates how systems can be compared on the basis of cost for relative levels of system performance against increasing numbers of adversaries. For example, if the design threat is thought to be a large number of adversaries, it would be desirable to pursue option 3 at an estimated cost of $15 million. If defense against fewer adversaries is required, options 1 or 2 might be adequate.

The various physical protection system designs can be compared in terms of performance, cost, and operational impact to determine the optimum combination of facility design, hardware capabilities, and response force attributes. If necessary, designs can be further modified until one or more designs is determined to be acceptable for more detailed design, evaluation, and implementation.

CHAPTER V

SUMMARY

This report has described a systematic approach to the conceptual design of physical protection systems for nuclear facilities. The primary emphasis of the report has been on evaluation of the relative effectiveness of physical protection system designs to allow comparison of various facility, hardware, and response force options. Models and calculations which may support design evaluation are identified. In addition, reference materials such as the handbooks described in appendix B are identified for use as aids in design and effectiveness evaluation as well as to support the assessment of costs and operational impact.

This approach can be applied to identify candidate physical protection system conceptual designs which meet overall system performance criteria. In the course of design and evaluation of conceptual design, performance criteria for specific portions of the physical protection system are identified. These criteria will guide the detailed design of the physical protection system for implementation in a facility.

This approach and some of the methods and models that are described in this report continue to be developed and improved. Appendix B lists the reports on conceptual designs for various nuclear facilities which have been developed using this approach. These reports give further insight into both the application and the evolving nature of the approach.

APPENDIX A

Glossary

Acceptable Path
: A path which has at least one limiting sequence which meets or exceeds the defined criteria P and T, where P is an acceptable level of detection and T is the time required for initial guard response following detection of the adversary.

Access Control
: A function which monitors and enables authorized movement of people and material through barriers and prevents unauthorized movement of people, special nuclear material, and contraband.

Adversary Sequence Diagram
: A graphical representation which, by indicating all significant connections between plant areas, represents all significant generic adversary paths through a facility.

Adversary Sequence Interruption
: The interception of an adversary by a response force before the adversary sequence is complete. Only a meeting of response force and adversary is implied. The results of an engagement are not considered.

Area
: A space enclosed by a connected set of barriers and controlled openings.

Balanced Protection
: A design principle which provides nearly equal protection of all similar areas to achieve maximum protection at minimum cost.

Barrier
: Any physical constraint to adversary or material movement. Operations classification of barriers is being developed based upon degree of resistance.

Characteristic Limiting Sequence
: The limiting sequence associated with the kth component where, for a particular time T associated with the time required for response force arrival,

$$T_{Rk} \geq T \text{ and } T_{Rk+1} < T \qquad \text{(A-1)}$$

The characteristic limiting sequence for a time T is described by the cumulative probability of detection $P_{D(cum)k}$ and the time remaining T_{Rk}.

Closed-Loop Control
A function which monitors specific access or operational sequences, compares the monitored sequence to a previously authorized sequence, and either permits the sequence to continue or, in case of a discrepancy, halts or corrects the sequence and/or initiates an alarm.

Commonality
The property associated with the change in detection probability and penetration time for a component that has been penetrated previously in an adversary action sequence.

Component
A discrete safeguards system part such as a sensor, barrier, computer or guard.

Conceptual Design
Development of a system at a concept level which is sufficient for demonstration of system feasibility and provides sufficient detail to allow commencement of detailed design and implementation.

Conditional Probability of Adversary Sequence Completion
The predicted probability that, given an attack, the adversary completes the adversary action sequence.

Contraband
Materials, such as SNM, explosives, and metal, which are not routinely permitted to pass into or out of an area.

Controlled Opening
A movable section of a barrier that permits controlled passage through the barrier.

Critical Path
A path for which the cumulative probability of detection does not reach an acceptable level before the time remaining for the adversary to complete the path is less than the time required for response force arrival and which, therefore, has no limiting sequence for which both the cumulative probability and the time remaining exceed the specified criteria.

Cumulative Probability of (Adversary) Detection ($P_{D(cum)k}$)
The detection probability accumulated by the adversary in passing through k safeguards components.

$$P_{D(cum)k} = 1 - \prod_{i=0}^{k} (1-P_{Di}) \qquad \text{(A-2)}$$

Cut Set
A group of basic events from the bottom of a fault tree which, if initiated, will cause the top event.

Diversion
: The removal of SNM from authorized locations, process lines, or transports for some unlawful use by persons who are authorized to possess the material.

Element
: A group of components combined to perform specific access-control or operations-control tasks.

Engineered Safeguards System (ESS)
: An integrated hardware and response force system designed to protect nuclear facilities against theft, diversion, or sabotage.

Facility Characterization
: A complete description of a facility and its safeguards requirements, including an outline of the threat spectrum to be considered; descriptions of buildings, processes, systems, and procedures; theft, diversion, and sabotage target analyses; and identification of safeguards concerns.

Hardware-Based Safeguards Systems Configuration
: The portion of the physical protection system which includes all safeguards components such as barriers, sensors, and computers, and all guards who are in fixed positions and may be characterized by a detection probability and a delay time (time of penetration).

Limiting Sequence
: The sequence associated with the kth component in which $P_{D(cum)k}$ and T_{Rk} are both minimum.

Material Measurement and Accounting System (MMA)
: A subsystem of an Engineered Safeguards System that provides information on the quantity and location of SNM within a facility for the purposes of inventory and production control as well as detection of theft or long-term diversion.

Most Nearly Critical Path(s)
: The path (or paths) through a facility which has the lowest cumulative probability of detection associated with its characteristic limiting sequence of all paths through the facility.

Operations Control
: A function which, through the operational interface between people, vital equipment, and SNM, monitors and enables authorized plant activities and delays unauthorized actions that could result in sabotage or theft.

Path
: A set of points into or through a facility and the associated tasks which an adversary must perform in traversing these points.

Physical Protection System
: A subsystem of an Engineered Safeguards System that utilizes detection, delay, and response capabilities to prevent theft, diversion, and sabotage.

Plant State

A specific operations state of the plant which may differ from other plant states in the items that may be targets, and the detection probabilities and penetration times which are associated with safeguards components.

Probability of (Adversary) Detection (P_D)

For a particular safeguards component, the probability that an adversary would be detected if he attempted to pass in a particular way through the detection field of the component. The minimum probability of detection is obtained by considering the way that provides the least probability of detection for a particular adversary.

Protection in Depth

The use of several detectors and barriers so that the failure of one does not result in the failure of the whole system.

Radiological Sabotage

A deliberate act directed against a transport, facility or a component of the facility that could directly or indirectly endanger the public health and safety by release of radiation.

Region Adjacency Diagram

A two dimensional graphical representation of a facility which shows all areas and all significant connections to adjacent areas.

Sabotage Sequence

A combination of specific sabotage acts which together could directly or indirectly endanger the public health and safety by release of radiation.

Sequence

An ordered set of adversary acts involving penetration of a particular set of components on a particular way, resulting in completion of a mission of sabotage, theft, or diversion, if the sequence is not stopped by response forces.

Special Nuclear Material

Plutonium, uranium-233, uranium-235, or any material artificially enriched with these materials or any other material pursuant to the provisions of Section 51 of the Atomic Energy Act of 1954, as amended, determined to be special nuclear material.

Target

Any quantity of SNM which may be subject to theft or diversion, or any quantity of radioactive material which, if dispersed, could endanger the public health and safety, or any vital equipment.

Target Analysis

The process of systematically identifying all targets and, then, determining which set or sets must be protected to prevent theft, diversion, or sabotage which could endanger the public health and safety.

Target Zone

Any area within a structure which contains a target which must be protected. The walls, roof, and floor of a zone constitute physical barriers with controlled access.

Theft

The unlawful removal of SNM from a facility or transport by persons who are not authorized to possess the material.

Time of Penetration (T_P)

The time required for an adversary to penetrate, pass through, or overcome a particular safeguards component. The minimum time of penetration is obtained by considering the fastest way for a particular adversary to penetrate a component.

Time Remaining (T_{Rk})

The minimum time required for an adversary to complete his sequence after penetrating the kth component. For a sequence with n components,

$$T_{Rk} = \sum_{i=k+1}^{n} T_{Pi} \qquad \text{(A-3)}$$

Vital Equipment

Any equipment, system, or device, the failure, destruction, or misuse of which could directly or indirectly endanger the public health and safety by release of radiation.

APPENDIX B

Abstracts of Reference Materials

Physical Protection System Conceptual Design

This appendix contains abstracts and descriptions of several documents and computer codes that may be useful references for physical protection system conceptual design. Also included is a list of documents which describes physical protection system concepts and candidate conceptual designs for nuclear facilities.

B.1 Intrusion Detection Systems Handbook*

B.2 Entry-Control Systems Handbook*

B.3 Barrier Technology Handbook*

B.4 Safeguards Central Control System Handbook*

B.5 Estimate of Adversary Sequence Interruption (EASI)†

B.6 Forcible Entry Safeguards Effectiveness Model (FESEM)†

B.7 Insider Safeguards Effectiveness Model (ISEM)*†

B.8 Set Equation Transformation System (SETS)*†

B.9 Path Analysis (PANL)*

B.10 Critically Ordered Path Evaluator (COPE)*

B.11 Safeguards Automated Facility Evaluation (SAFE)†

B.12 Generic Sabotage Fault Trees for Nuclear Power Plants†

B.13 Physical Protection System Concept and Candidate Conceptual Design Reports*

* Sponsored by the United States Department of Energy

† Sponsored by the United States Nuclear Regulatory Commission

B.1 Intrusion Detection Systems Handbook[2]

This handbook was based on data obtained from evaluation programs conducted by DOE, the Department of Defense, and other government agencies, on information provided by commercial security equipment suppliers, and actual field experiments.

The handbook was written primarily to provide recommendations for the selection, procurement, installation, testing, and maintenance of intrusion detection systems, both for interior and exterior use. It also provides guidelines for the assessment of alarms and guidance applicable to alarm communication and display systems. Its contents are the following:

B.2 Entry-Control Systems Handbook[3]

As a companion to the Intrusion Detection Systems Handbook, an Entry-Control Systems Handbook has been prepared. This handbook states the general entry-control systems concepts and provides a theoretical discussion of the operating principles of the various elements of an entry-control system. It also provides descriptions of entry-control elements and systems that are presently available or under development, including a discussion of operating characteristics and test results. Its contents are the following:

Chapter 1: Introduction

Chapter 2: Credentials

Chapter 3: Personnel Identity Verification Systems

Chapter 4: Special Nuclear Materials Monitors

Chapter 5: Metal Detectors

Chapter 6: Explosives Detectors

Chapter 7: Package Search Systems

Chapter 8: Criteria for Selection of Entry-Control Equipment

Chapter 9: Machine-Aided Manual Entry-Control Systems

Chapter 10: Automated Entry-Control Systems

Appendix A: System Example

B.3 Barrier Technology Handbook[4]

A barrier technology handbook has also been prepared to define the role of barriers in a total physical security system and to provide an overview and a tutorial background for barrier evaluation.

It is also intended to establish a central source of performance characteristics for use by designers, inspectors, and engineers and to outline the state-of-the-art advanced concepts.

The handbook establishes the scenario for barrier studies and discusses threat attributes and various adversary action sequences. It presents philosophical aspects of barrier-design trade-offs with detection and response systems and discusses delay concepts, attack tools, and penetration considerations. Further discussions include advanced concepts for upgrading existing facilities and cost considerations.

Details on penetration aspects of specific barrier categories and evaluation of vulnerability of current designs to attack modes are presented. Advanced concepts and upgrading suggestions are also included. Its contents are the following:

Chapter 1: Introduction

Chapter 2: Role of Barriers

Chapter 3: Perimeter Barriers

Chapter 4: Walls

Chapter 5: Roof and Floors

Chapter 6: Doors

Chapter 7: Locking Mechanisms

Chapter 8: Windows

Chapter 9: Utility Ports

Chapter 10: Vaults

Chapter 11: Igloos

Chapter 12: Earth Cover and Overburden

Chapter 13: Airborne Penetration Deterrents

Chapter 14: Armor

Chapter 15: Dispensable Barriers and Deterrents

Chapter 16: Penetration Times - Data Base

Chapter 17: Rates

B.4 Safeguards Central Control System Handbook[5]

This handbook is being prepared to assist facility designers in the selection of a computer based system that will best serve the safeguards requirements of their particular facility. The design approach is toward a modular system that is constructed from well-defined building blocks. It includes descriptions of hardware and software elements that are commercially available to support the Safeguards Central Control System (SCCS) concepts including operating system capabilities. Its intended contents are the following:

Chapter 1: Introduction

Chapter 2: Engineered Safeguards System Concepts

Chapter 3: Central Control System Elements and Configurations

Chapter 4: Typical Applications

Chapter 5: Design Criteria and Considerations

Chapter 6: Central Control

Chapter 7: Front-End processors

Chapter 8: Data Concentrators

Chapter 9: Transducer Interface Units

Chapter 10: Data Lines

Appendix A: LWR Example

Appendix B: Available Equipment

Appendix C: Technology Reports

Appendix D: Definition of Terms

B.5 Estimate of Adversary Sequence Interruption (EASI)

Purpose--The objective of EASI[67] is to provide a simple evaluation method for use as a physical protection system design aid. Due to its simplicity, the evaluation can be performed on a hand-held programmable calculator. The EASI evaluation method is a probabilistic approach which analytically evaluates basic functions of the physical security system (detection, assessment, communications, delay) with respect to response time and provides an estimate of adversary sequence interruption. Each assessment of physical protection system performance is with respect to a specific adversary action sequence. The method can treat both theft and sabotage objectives by threats of insiders, outsiders, and combinations of both.

Generalized Input--The following input data are required:

- detection probability for each sensor or other means of detection,
- probability of communication to the response force or other means of response,
- mean and standard deviation of response time, and
- mean and standard deviation of the time to perform each task in the adversary action sequence.

Generalized Output--The results of the analysis are expressed in terms of the probability that the physical protection system can respond in time to interrupt specific adversary action sequences

B.7 Insider Safeguards Effectiveness Model (ISEM)

Purpose--The purpose of ISEM[12 13] is to model the interaction of one adversary (either insider or outsider) as he traverses a prescribed physical path through a nuclear facility and facility safeguards system. The initial state of the safeguards system elements (e.g., sensors, computers, displays, etc.) is determined by the access authorizations of a group of facility personnel (guards and/or employees) identified as adversaries (insiders) who covertly tamper with the safeguards system elements prior to the potentially overt attack by the aforementioned adversary. ISEM allows a reasonably detailed study of guard tactics and procedures at a general facility.

Suggested use is the study of safeguards system interaction with a single overt adversary along a prescribed adversary physical path which was preceded by a covert attack on safeguards system elements by a group of insiders.

Generalized Input--The analyst must specify the following parameters:

- physical path characteristics,
- barrier characteristics,

- sensor system characteristics,
- adversary attributes,
- area access for facility personnel, and
- response force attributes.

Generalized Output--The following three user selectable output data sets are available from ISEM:

- an event sequence showing how events occurred along the physical path,

- a set of 22 statistical parameters with characterizations which summarize simulation results, and

- a set of 15 histograms which gives a pictorial presentation of the statistical results and further expands the summary information contained in the statistical parameters in item 2, above.

B.8 Set Equation Transformation System (SETS)

SETS[14 15] is designed to achieve the symbolic manipulation of set equations. The system allows the generation of set equations directly or by the logical combination of other set equations through a process of substitution. It also provides for the reduction of set equations by the application of set identities and for the permanent retention of set equations for use at a later time. The operations allowed in an equation are those of intersection, union, and complement, as defined in the algebra of sets. Thus, the system provides a comprehensive capability for generating and manipulating set equations symbolically. Moreover, since the processing that can be accomplished using SETS is valid for any Boolean algebra, the system is useful for processing the logic equations derived from fault trees. When used to manipulate fault trees, it can find all of the smallest cut sets of basic events that will cause the top event to occur or all of the smallest cut set of complements of basic events that will ensure that the top event will not occur.

The analyst creates a SETS user program using a user language which has procedure calls as the operational elements. They call for execution of procedures that are designed to read input or to accomplish some part of the processing of set equations. One category of procedure calls identifies individual set equations. A second category assigns identifiers for stored blocks of set equations. Separate input blocks are groups of set equations which occur as input to a SETS user program. Boolean equations may be directly input.

Intermediate and final results of the set equation transformation process are also user-called with the SETS user language procedure calls.

B.9 Path Analysis (PANL)

The computer code PANL may be used to perform critical-path analysis. PANL generates all paths for the facility from Boolean equations which are derived from an Adversary Sequence Diagram. It then calculates the characteristic limiting sequence for each path and identifies all critical paths. To account for commonality, the data for detection probabilities and penetration times are obtained from the following three data tables: (1) for going in through a barrier, (2) for going out through a barrier that was not penetrated on the way in, and (3) for going out through a barrier that was penetrated on the way in. This program continues to be developed and is presently being documented.

B.10 Critically Ordered Path Evaluator (COPE)

The computer code COPE[16] is used to perform critical-path analysis. Beginning with a description of all connections between areas on an Adversary Sequence Diagram, the code calculates the characteristic limiting sequence for all paths through the ASD, using a branch and bound network analysis.

The data for detection probabilities and penetration times associated with each barrier includes a variable which allows detection either before or after penetration. In addition, commonality is included in the calculation.

The output, in the form of the characteristic limiting sequences for each path, is ordered in terms of increasing cumulative probability of detection so that the most critical or nearly critical paths may be easily identified.

B.11 Safeguards Automated Facility Evaluation (SAFE)

Purpose--The objective of SAFE is to provide an automated approach to facility safeguards effectiveness evaluation, based upon basic information, such as facility layout and performance parameters for physical protection components. This procedure consists of a collection of functional modules for facility characterization, critical path generation, and path evaluation combined into a continuous stream of operations. The technique has been implemented on an interactive computer-timesharing system and makes use of computer graphics for the handling and presentation of information.

Method--The pertinent facility layout information must be digitized and organized into computer-usable data. Lines and nodes are identified by x-y coordinates, nodes are further defined by type, penetration delay time, standard deviation of delay time, and probability of detection. The process continues with automatic identification and weighting of arcs between nodes. The final output of the facility characterization module—a graph in which nodes represent access points or targets and arcs represent paths between nodes—is the input generation module.

The path generation function can be accomplished by several alternate techniques. One generator, SPTHB,[34] supplies the

shortest path from a node exterior to the graph to every node in a facility graph, minimizing time or detection probability. Another generator finds up to the kth shortest paths from an exterior node to every node of the graph. The preferred pathing routine, MINDPT,[37] uses the Very EASI[6] evaluation method. This method finds paths by minimizing detection probability up to a locus of points that are a guard-response time away from the target.

The output of the path generator is a collection of ordered sets of node identifiers which represent paths. This information, combined with data concerning the node parameters, is the input to a path evaluation module such as the EASI[6] path evaluation method. EASI is an analytical technique and, therefore, makes efficient use of computer time. Extra information required by this model includes expected response time of on-site guards, standard deviation of the response time, and probability of communication of an alarm. The output of EASI is an estimate of the probability of adversary interruption along the specified path.

This evaluation can be used in two modes—single path or multipath. During a single path evaluation by EASI, the probability of interruption is calculated and the user may request two or three-dimensional plots which show

probability of adversary interruption as a function of one or two of the other input variables. These graphs illustrate sensitivities related to upgrading the facility based upon the probability of interruption.

The multipath option displays, in tabular form, the EASI probability of interruption, the traversal time for each path, and the frequency at which nodes appear in the set of critical paths. The multipath evaluation acts like a filter, identifying paths which are particularly vulnerable and, thus, are candidates for study by more elaborate evaluation simulation modes such as FESEM[8] and ISEM.[12]

B.12 Generic Sabotage Fault Trees for Nuclear Power Plants[20]

This study introduces the use of generic sabotage fault trees (SFT) to construct specific SFT for nuclear power reactors. The SFT are used to systematically identify the sabotage actions which could lead to release of significant amounts of radioactivity from a nuclear power plant. Eleven generic SFT were developed. The preliminary results show that the technique is a useful tool for identifying the vital systems, components, and locations which, if protected, would largely reduce the likelihood of sabotage acts that could result in significant release of radioactivity. This information is needed during the licensing of nuclear power processing plants. The technique also shows several advantages over the previous method used to construct the specific SFT. Further work is needed to develop detailed procedures on ways to apply the technique to construct specific SFT for a given power plant. The automation of the technique for on-line computer application should also be pursued.

B.13 Physical Protection System Concept and Candidate Design Reports

The following documents describe physical protection system concepts and candidate conceptual designs for nuclear facilities:

1. L. D. Chapman, J. M. deMontmollin, J. E. Deveney, W. C. Fienning, J. W. Hickman, L. D. Watkins, and A. E. Winblad, Development of an Engineered Safeguards System Concept for a Mixed-Oxide Fuel Fabrication Facility, SAND76-0180, Sandia Laboratories, August 1976.

2. A. E. Winblad, editor, A Concept and Preliminary Definition of an Engineered Safeguards System for a Mixed-Oxide Fuel Fabrication Facility, (U), SAND76-0528, Sandia Laboratories, September 1976, confidential.

3. J. L. Darby, Preliminary Safeguards Concepts for a Typical Liquid Metal Fast Breeder Reactor, (U), SAND77-0597, Sandia Laboratories, June 1977, confidential.

4. J. W. Moyer, A Preliminary Safeguard Concept Definition for a Facility-Integrated, Fuel Cycle Plutonium Transportation Vehicle (PTV) and Shipping Container, SAND77-1274, Sandia Laboratories, November 1977.

5. W. C. Fienning, A. E. Winblad, and J. P. Shipley, A Preliminary Concept Definition for a Mixed-Oxide Fuel Fabrication Facility Safeguards System, SAND 77-0224, Sandia Laboratories, October 1977.

6. A. E. Winblad, W. C. Fienning, R. P. McKnight, R. E. Moll, and M. N. Cravens, "Preliminary Engineered Safeguards System Design for a Mixed-Oxide Fuel Fabrication Facility," SAND77-1155, Sandia Laboratories, December 1977, review draft.

7. C. S. Sonnier, Baseline Description and Safeguards Concerns for a Fuel-Cycle Plutonium Storage Facility, SAND77-1497, Sandia Laboratories, December 1977.

8. W. D. Chadwick, G. E. Rochau, W. C. Fienning, R. P. McKnight, and A. E. Winblad, "A Concept Definition of an Engineered Safeguards System for a Spent-Fuel Reprocessing Facility," (U) SAND77-1539, Sandia Laboratories December 1977, confidential review draft.

9. J. L. Darby and C. P. Cameron, "Preliminary Safeguards Concepts for Typical Light Water Reactors," SAND77-1307, Sandia Laboratories, confidential, to be published.

10. C. S. Sonnier and M. N. Cravens, "Preliminary Concepts for Detecting National Diversion of LWR Spent Fuel," SAND77-1954, Sandia Laboratories, to be published.

11. J. L. Darby, C. P. Cameron, W. D. Chadwick, "Concept Definition for a Physical Protection System for a Typical Pressurized Water Reactor," Sandia Laboratories, in progress.

References

1. M. N. Cravens, Jr. and A. E. Winblad, Physical Protection System Design Method, SAND77-0119, Sandia Laboratories, January 1978.

2. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, November 1976, revised October 1977.

3. Entry-Control Systems Handbook, SAND77-1033, Sandia Laboratories, September 1977.

4. Barrier Technology Handbook, SAND77-0777, Sandia Laboratories, October 1977.

5. Safeguards Central Control System Handbook, Sandia Laboratories, in progress.

6. H. A. Bennett, The EASI Approach to Physical Security Evaluation, SAND76-0500, NUREG760145, Sandia Laboratories, January 1977.

7. H. A. Bennett, User's Guide for Evaluating Physical Protection Security Capabilities of Nuclear Facilities by the EASI Method, Sandia Laboratories, SAND77-0082, June 1977.

8. L. D. Chapman, Effectiveness Evaluation of Alternative Fixed-Site Safeguards Security Systems, SAND76-6159, Sandia Laboratories, April 1977.

9. L. D. Chapman, G. A. Kinemond, and D. W. Sasser, User's Guide for Evaluating Fixed-Site Physical Protection Systems Using FESEM, SAND77-1367, Sandia Laboratories, November 1977.

10. L. D. Chapman, A Model for Evaluating Alternative Fixed-Site Security Systems, (U), SAND75-0512, Sandia Laboratories, April 1976, confidential.

11. L. D. Chapman, Fixed-Site Physical Protection System Modeling, SAND75-6061, Sandia Laboratories, December 1975.

12. D. D. Boozer and D. Engi, Simulation of Personnel Control Systems Using the Insider Safeguards Effectiveness Model (ISEM), SAND76-0682, Sandia Laboratories, April 1977.

13. D. D. Boozer and D. Engi, Insider Safeguards Effectiveness Model (ISEM) User's Guide, SAND77-0043, Sandia Laboratories, November 1977.

14. R.B.Worrell, Set Equation Transformation System (SETS), SLA-73-0028A, Sandia Laboratories, May 1974.

15. R. B. Worrell, Using the Set Equation Transformation System in Fault Tree Analysis, SAND74-0240, Sandia Laboratories, September 1974.

16. B. R. Fenchel, "A Computer Network Analysis of a Nuclear Facility," SAND77-1392, Sandia Laboratories, to be published.

17. L. M. Grady, "Automated Approach to Nuclear Facility Safeguards Effectiveness Evaluation," Transactions of the American Nuclear Society, 27 (1977) 184.

18. B. L. Hulme, Graph Theoretic Models of Theft Problems, 1. The Basic Theft Model, SAND75-0595, Sandia Laboratories, November 1975.

19. B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models, 1. Simultaneous Attack by Several Teams, SAND76-0314, Sandia Laboratories, July 1976.

20. N. R. Ortiz and G. B. Varnado, "Generic Sabotage Fault Trees for Nuclear Power Plants," SAND77-1805, Sandia Laboratories, to be published.

21. A Preliminary Assessment of Terrorist Threat to Nuclear Programs, SAND75-7062, contract report prepared for Sandia Laboratories by Historical Evaluation and Research Organization (HERO) September 1975.

22. Estimate of Security Personnel Required to Protect Nuclear Fuel Cycle Components Against Theft of Special Nuclear Material and Sabotage, International Research and Technology Corporation (IR&T), July 1975.

23. S. Burnham, editor, The Threat to Licensed Nuclear Facilities, MTR-7022, MITRE Corporation, September 1975.

24. Analysis of the Terrorist Threat to the Commercial Nuclear Industry, BDM/75-176-TR, BDM Corporation, September 1975.

25. B. M. Jenkins, An Approach to the Study of Potential Threats to Nuclear Programs, WN-9366-SL, Rand Corporation, January 1976.

26. J. Johnson, K. K. Kellen, G. Petty, and R. Strauch, Sophisticated Crimes as Analogs to Potential Threats to the Nuclear Industry: A Preliminary Assessment, WN(L)-9367-1-SL, Rand Corporation, January 1976.

27. R. Struach, Symbolic Bombing as an Analog Threat to the Nuclear Industry (A Preliminary Assessment), WN(L)-9482-SL, Rand Corporation, July 1976.

28. E. S. Wainstein, Threats and Incidents Involving Nuclear Material or Facilities, WN-9368-2-SL, Rand Corporation, September 1976.

29. K. K. Kellen and J. Krofcheck, Nuclear Hoaxes, Preliminary Analysis, WN(L)-9420-1-SL, Rand Corporation, October 1976.

30. P. deLeon, B. Jenkins, K. Kellen, and J. Krofcheck, Attributes of Potential Criminal Adversaries of U.S. Nuclear Programs, R-2225-SL, Rand Corporation, February 1978.

31. J. L. Darby, C. P. Cameron, and W. D. Chadwick, "Concept Definition for a Physical Protection System for a Typical Pressurized Water Reactor," Sandia Laboratories, in progress.

32. Reactor Safety Study, WASH-1400, U. S. Nuclear Regulatory Commission, October, 1975.

33. B. L. Hulme, The Region Adjacency Graph in Sabotage Studies, SAND76-0574, Sandia Laboratories, October 1976.

34. B. L. Hulme and D. B. Holdridge, SPTHB: A Subroutine for Finding Shortest Sabotage Paths, SAND77-1060, Sandia Laboratories, 1977.

35. W. D. Chadwick, G. E. Rochau, W. C. Fienning, R. P. McKnight, and A. E. Winblad, "A Concept Definition of an Engineered Safeguards System for a Spent-Fuel Reprocessing Facility," SAND77-1539, Sandia Laboratories, December 1977, confidential, review draft.

36. R. B. Worrell and D. W. Stack, Common-Cause Analysis Using SETS, SAND77-1832, Sandia Laboratories, December 1977.

37. B. L. Hulme, MINDPT: A Code for Minimizing Detection Probability Up To A Given Time Away From A Sabotage Target, SAND77-2039, Sandia Laboratories, December 1977.

*U.S. GOVERNMENT PRINTING OFFICE: 1978 261-324/48 1-3