27
7-17-78
25 to NTIS

SAND77-0644
Unlimited Release

Distribution
Category RS

Reactor Safeguards System Assessment and Design Volume I

G. Bruce Varnado, David M.Ericson, Jr., Sharon L. Daniel,
Harold A. Bennett, Bernie L. Hulme

Prepared by Sandia Laboratories, Albuquerque, New Mexico 87185
and Livermore, California 94550 for the United States Nuclear
Regulatory Commission under DOE Contract AT(29-1)-789.
Printed June 1978

Sandia Laboratories

SF 900 Q(7-73)

DISCLAIMER

Issued by Sandia Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE

Printed in the United States of America

Available from
National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

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

PAGES 1 to 2

WERE INTENTIONALLY

LEFT BLANK

SAND77-0644
Work Completed: October 1976
Unlimited Release
Printed June 1978

Distribution
Category RS

REACTOR SAFEGUARDS SYSTEM ASSESSMENT AND DESIGN

VOLUME I

G. Bruce Varnado
David M. Ericson, Jr.
Sharon L. Daniel
Nuclear Fuel Cycle Facility Analysis Division 5414

Harold A. Bennett
Safeguards Methodology Development Division 5724

Bernie L. Hulme
Numerical Mathematics Division 5122

Sandia Laboratories
Albuquerque, NM 87185

ABSTRACT

A methodology for assessing the effectiveness of safeguards systems was developed in this study and was applied to a nuclear power plant. The methodology combines fault tree analysis, graph-theoretic modeling, and simulation modeling to produce a quantitative measure of the effectiveness of reactor safeguards systems in repelling forcible attacks. A technique was developed for determining the minimum set of vital areas which must be protected to assure that all adversary sequences are interrupted. The relative importance of detection systems, barriers, response forces, and damage control measures was determined in extensive parameter variation studies, and example safeguards system designs were proposed for a typical power reactor.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions of the following individuals to the successful completion and reporting of this study:

R. B. Worrell, Division 1758, Sandia Laboratories, for his many helpful suggestions concerning the development of the Vital Location Analysis procedures, for the development of computer programs needed for manipulation of the fault tree equations, and for other constructive inputs to the general methodology development;

D. L. Mangan, Division 1739, Sandia Laboratories, for his assistance in acquiring and interpreting data on the expected performance characteristics and costs of physical security system hardware;

W. H. Immerman, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, for his technical review of the final report and suggestions for clarification of the presentation.

FOREWORD

This is Volume I of the final report on a program titled "Integrated Safeguards System Concepts for Power Reactors" conducted for the Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, by Sandia Laboratories. Volume II of the report which consists of several appendices containing the analytical details of the study is classified secret.

CONTENTS

VOLUME I

CONTENTS (cont)

VOLUME II

ILLUSTRATIONS

ILLUSTRATIONS (cont)

TABLES

SUMMARY

This report describes a general analytic framework and specific methods useful in the assessment of the effectiveness of reactor safeguards. The utility of the methods is demonstrated by application to a typical power reactor plant. Topics discussed include the characteristics of reactor plants which influence safeguards, the safeguards effectiveness evaluation methodology used in this study, application of the methodology to the analysis of safeguards systems for a typical light water reactor plant, and conclusions concerning the effects of variations in safeguards system design and component performance upon overall system effectiveness. The work forms the basis for further development of simplified techniques required for the design and licensing review of reactor safeguards systems.

Reactor plants are structurally very complex with many floor levels, compartments, and access points and are functionally very complex as well with several sources of radioactive material and many ways (direct and indirect) to release material from these sources. As a result, there are many paths one can take to reach sabotage targets, and the number of specific adversary action sequences which can produce public consequences is extremely large. In order to make it practical to comprehensively analyze safeguards systems, the methodology developed in this study focuses on identifying and evaluating those parts of the safeguards system necessary to assure that all adversary sequences can be interrupted. The methods for identifying plant areas where protection is required are applicable regardless of the nature of the adversary, but the methods used for quantitative evaluation of system performance are applicable only to forcible attack by outsiders. Extension of the evaluation methods to other types of adversary sequences requires further study.

The primary steps followed in analyzing reactor safeguards systems were to: (1) determine the events (destruction or manipulation of equipment) which can lead to release of radioactive material from each source, (2) determine where in the plant the failures can be initiated and which areas (target locations) must be protected to assure that release cannot occur, (3) select paths to the target locations which are in some sense optimum for the adversary, and (4) estimate the performance of the safeguards system in interrupting adversary sequences along the selected paths. The analytic techniques which have been applied to accomplish these steps are fault tree analysis, graph-theoretic modeling, and system simulation modeling. An interactive computer-graphics system is used to input data and display results of the path analysis.

The methodology was applied to a typical light water reactor plant to estimate the effectiveness of several alternative safeguards systems against forcible attacks by outsiders. The sensitivity of overall system effectiveness to changes in component performance was evaluated in order

to identify the key elements in the safeguards system. Based on the comparison of alternative configurations and the results of the sensitivity studies, an example safeguards system which could be constructed from currently available components was specified.

The methodology developed in this study provides several advances in safeguards system effectiveness modeling including: (1) the development of a systematic means of identifying the areas of the plant which must be protected to prevent sabotage, as well as the areas in which damage control could possibly replace physical protection measures as a means of preventing radioactive release, (2) the demonstration of the usefulness of graph-theoretic techniques in selecting adversary paths, and (3) the use of an interactive computer graphics system to display plant layout and path data. With some simplification and refinement, the general methodology used in this study can be applied by licensees and the NRC as a tool for the design and evaluation of safeguards systems.

REACTOR SAFEGUARDS SYSTEM ASSESSMENT AND DESIGN

CHAPTER 1

INTRODUCTION

This report describes the development and application of a methodology for evaluating the effectiveness of nuclear power reactor safeguards systems. Analytic techniques are used to identify the sabotage acts which could lead to release of radioactive material from a nuclear power plant, to determine the areas of a plant which must be protected to assure that significant release does not occur, to model the physical plant layout, and to evaluate the effectiveness of various safeguards systems. The methodology was used to identify those aspects of reactor safeguards systems which have the greatest effect on overall system performance and which, therefore, should be emphasized in the licensing process. With further refinements, the methodology can be used by the licensing reviewer to aid in assessing proposed or existing safeguards systems.

1.1 Objective

The objective of this study was to develop a reactor safeguards system assessment methodology and to demonstrate the applicability of this methodology to assessment and design of safeguards systems for a typical light water reactor (LWR).

1.2 Scope

Full achievement of the study objective was limited by conceptual and practical constraints. The function of reactor safeguards is to reduce to an acceptable level the public risk due to malevolent actions directed against reactor facilities. The conceptual basis for assessing public risk due to malevolent action does not currently exist. The components of risk have been defined in ERDA-7[1] as (1) the frequency of attempt to produce an event, (2) the conditional probability that attempts will be successful, and (3) the consequences of the events produced. However, the dependencies among these components and their quantitative relationships to safeguards system functions such as deterrence, physical protection, material control, and consequence mitigation are not well established. Thus, no overall measure of safeguards system performance in terms of risk reduction can yet be developed. In particular, at the time of this study, sufficient theoretical bases did not exist for detailed treatment of the probability of attempt, adversary actions during the preparation phase of an adversary action sequence (AAS), insider malevolent actions, deceit mode attacks, or consequences other than those directly due to release of radioactivity. On the other hand, there are quantifiable measures for one or more of the components of risk which can be used to assess safeguards system performance in the absence of an overall risk measure. Chapter 3, for example, discusses a measure (probability that adversary attempts will be defeated) used in this study to assess safeguards systems.

In addition to these theoretical constraints, practical difficulties arise in quantifying the safeguards system performance measure for facilities as structurally and functionally complex as reactor plants. The methodology must provide a measure of effectiveness encompassing the enormous number of AASs leading to radioactive release. As a result, the methodology developed is rather complex and still in preliminary form. To use the methodology, an analyst must have considerable expertise in reactor design and operation, familiarity with several analytic techniques, access to a large computer system, and a significant amount of time. In its present form, the methodology is difficult to use directly in reactor safeguards licensing and design. It does, however, represent a significant step in the development of a practical, systematic approach for safeguards system evaluation.

Within the scope of the limitations discussed above. a procedure for meeting the study objective was defined. First, the general characteristics of reactor plants were reviewed and alternative safeguards system configurations were developed (Chapter 2). Second, a methodology was developed to assess the effectiveness of the alternatives, allowing systematic, quantitative comparisons (Chapter 3). The steps in the methodology are:

1. Identify the adversary acts that can lead to radioactive release or theft of nuclear material (fault tree analysis).[2]
2. Identify the locations in the plant where these acts can be performed.
3. Identify a minimum set of locations which must be safeguarded to prevent release or theft (vital location analysis).
4. Identify those adversary acts which can be nullified by damage control measures.
5. Estimate the effectiveness of the candidate safeguards systems (critical path analysis and simulation modeling).

Third, the methodology was applied to a typical LWR plant with the alternative safeguards system configurations (Chapter 4). Sensitivity studies were run to determine the subsystems and parameters which have the greatest effect on safeguards system performance and cost. From this information, example reactor safeguards systems were defined by using available subsystem and component technology. Finally, directions were suggested for further development and improvement of the effectiveness evaluation methodology.

1.3 Background

Recent studies of the vulnerability of nuclear power reactors to sabotage have identified those actions which could lead to the release of radioactive material beyond plant boundaries and have proposed countermeasures for reducing the likelihood that such actions could be completed.[2] It was concluded that the design and operating features of nuclear power plants and their engineered safety features provide inherent protection against acts of sabotage which could endanger the public. Several recommendations were made for further reduction of power plant vulnerability. In addition, the Special Safeguards Study[3] and the ERDA Physical Protection Program[4] provided data and models useful in evaluating reactor safeguards.

Fault trees developed in the Reactor Sabotage Studies[2] provide information about the failures which an adversary could initiate to cause release from a typical LWR plant. Other data obtained from the sabotage studies included plant layout, equipment location, and location and activity level of radioactive sources. A preliminary algorithm for selecting optimum adversary paths was developed in the ERDA Physical Protection Program; data on the performance characteristics of physical protection system components (intrusion detection systems, barriers, access control systems, and the like) were also drawn from that program. A model developed in the Special Safeguards Study, which simulates the interaction between an adversary and the safeguards system at a fixed facility, was used to estimate the probability of defeating AASs along selected paths. Thus, much of the basic model and data development necessary to achieve the objective of this study was available at the outset. The major advancement contributed by the study was the combination of improved versions of the available models into a systematic, comprehensive methodology and the demonstration of applicability of the techniques to nuclear power plants.

CHAPTER 2

FACILITY CHARACTERIZATION

In order to develop a methodology for assessment of reactor safeguards, it is necessary to specify the characteristics of reactor plants that determine the safeguards requirements. The characteristics of interest include the sources of radioactive material in the plant and the sabotage acts that could lead to release from the sources, the physical layout and structural characteristics of the plant, and possible congiruations of the safeguards system. This chapter summarizes these characteristics for a typical LWR plant.

2.1 General Physical Characteristics

A typical nuclear power reactor plant is a large facility composed of (1) a main building (or complex of buildings) which houses the reactor, turbo-generator, control room, rad-waste facility, fuel storage area, and related equipment; (2) one or more separate buildings which house pumping and emergency power equipment, shops, etc.; and (3) switchgear and transformer yards outside the buildings. Figure 2.1 shows a plot plan for a typical plant. To provide seismic protection for safety-related equipment, the construction for much of the main building is heavily reinforced concrete 0.5 to 2 metres thick. Generally, there are no windows in the structure. In contrast, the doors are typically of light steel construction, with glass panes in some cases, and therefore are the most likely penetration points. The only other access points into the buildings are ventilation system vents and hatches on the top of the reactor building.

The interior of the structure is quite complex, containing several levels with many compartments on each level. Figure 2.2 shows the floor plan of one level of a typical two-unit plant; a set of floor plans for the buildings of interest is given in Appendix D.* The large numbers of doorways (interior and exterior) connecting the compartments on a level, and stairways or elevators connecting the different levels are important characteristics in the development of safeguards systems for the plant.

2.2 Sources of Radioactive Material

In principle, nuclear material can pose two kinds of hazards to the public: (1) blast effects from a nuclear explosion, and (2) internal or external radiation damage resulting from the dispersal of radioactive materials or from criticality incidents.[5] The low-enrichment fuel used in

*Appendices D through H appear in Volume II of SAND77-0644, a classified report.

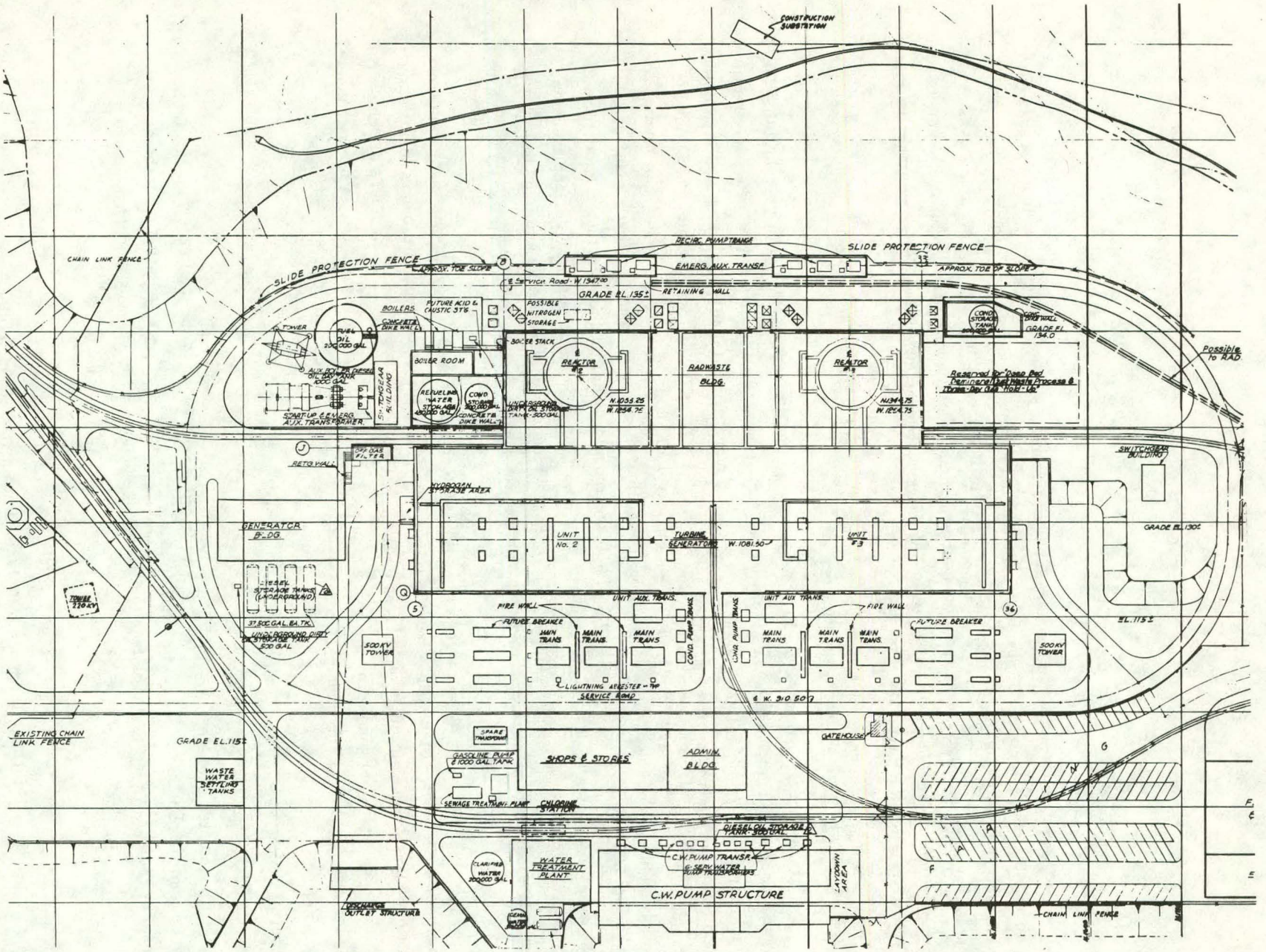


Figure 2.1. Plot Plan of a Typical Plant

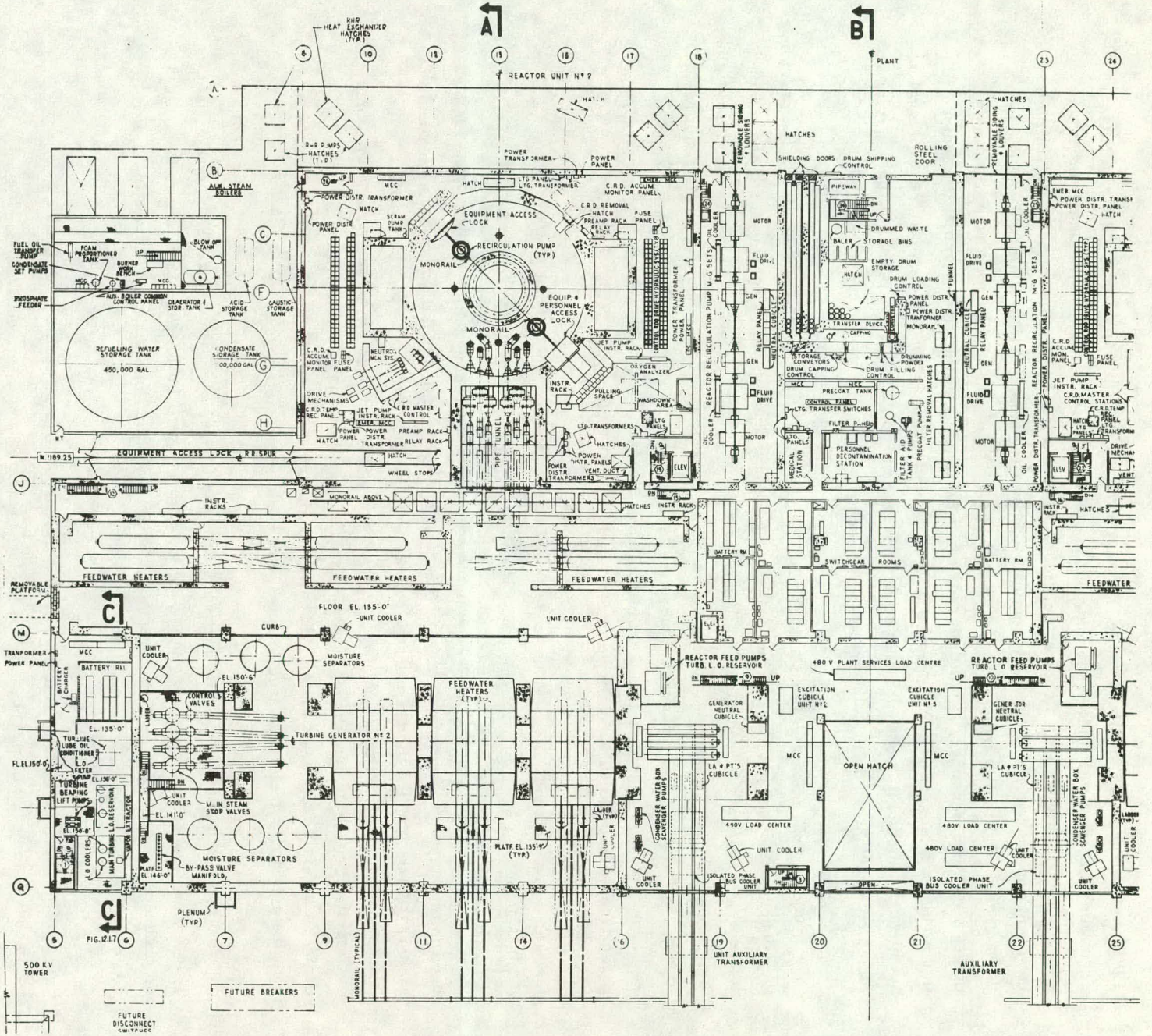


Figure 2.2. Floor Plan for One Level of a Typical Two-Unit Plant

LWRs, either uranium or mixed-oxide, cannot produce a nuclear explosion;[6,7] thus, a nuclear explosion can be a threat only if the material is stolen and processed to obtain a sufficient concentration of fissile atoms. Criticality incidents can be initiated with the low-enrichment fuel; however, the consequences would be confined to radiation damage within a limited region near the source.[5] Criticality incidents induced at the reactor site would therefore have little or no direct public consequences,* but theft of the fuel followed by initiation of a criticality incident in a highly populated area could produce a significant public hazard. Thus, theft is the malevolent act through which criticality incidents could endanger the public. The dispersal of the material is a major concern for acts of both theft and sabotage.

Nuclear (or radioactive) material is present in several LWR systems: the core of the reactor, the spent fuel storage pool, spent fuel shipping casks, the fresh fuel storage area, and the radioactive waste system. Although acts of sabotage or theft could be directed against any of the systems, their attractiveness as targets depends upon the adversary's purpose, technical ability, and resources, as well as the accessibility, physical form, chemical composition, amount, radiation level, and toxicity of the material contained in each system. Some of the factors which affect the attractiveness and the vulnerability of a plant and these possible targets are discussed in the sections which follow.

2.2.1 Reactor Core

The largest inventory of radioactive material (on the order of 10^{10} curies) in the plant is found in the core of the reactor. Most of this material is in sealed metal fuel rods in the form of fission products trapped in ceramic fuel pellets or in gas plenums at the tops of the rods. The core is located within a thick steel reactor pressure vessel (RPV) which is surrounded by a massive steel and concrete containment structure. This multiple containment system, intended primarily as a safety measure, also provides protection against malevolent acts (such as penetration from the exterior) which could lead to release of radioactive material.

Theft of material from the core is practically impossible. During operation of the plant the material is inaccessible; during refueling the RPV is open, but the fuel is highly radioactive and produces large quantities of decay heat. The possible theft options at LWRs are discussed in greater detail in Appendix A.

The sabotage options which could lead to release of radioactive material from the core are discussed in an earlier report.[2] The greatest potential for public consequences results from sabotage leading to core meltdown which generally requires (1) the loss of cooling necessary to remove fission product decay heat, and (2) the disablement of one or more systems of the engineered safety features. Systematic analysis of reactor systems indicates that there is an enormous

*Loss of generating capacity as a result of such an incident could cause indirect public consequences.

number of combinations of subsystem and component failures which could lead to core meltdown. The safeguards system must provide protection against initiation of all the possible combinations.

In addition to direct loss of coolant caused by breaching the primary reactor coolant boundary, cooling can be lost as a result of induced transient incidents in which all significant heat sinks and coolant sources are removed, resulting in eventual boil-off of the coolant inventory through the overpressure relief valves. Transient incidents are divided into two categories depending upon the time between sabotage-induced failure and the start of fuel melting. Short-term transients could lead to the start of core meltdown in 1 to 3 hours while long-term transient incidents require from 3 to 24 hours before melting begins.[2] The time required for a long-term transient to run its course provides an opportunity for damage control on the part of plant personnel to either nullify the incident or reduce its consequences.

2.2.2 Spent Fuel Storage Pool

Spent fuel removed from the core is placed in the spent fuel storage pool to allow radioactive fission products to decay sufficiently for off-site transport. The level of radioactivity of the fuel (total pool activity may be as high as 10^9 curies) necessitates remote handling and special shipping casks for transport. For some time after the fuel is removed from the core, the heat produced in the radioactive decay process is sufficient to cause melting if the fuel is not cooled. The pool, with walls of reinforced concrete 1 to 2 metres thick lined with stainless steel, contains roughly 1000 cubic meters (300,000 gallons) of circulating water to dissipate the decay heat and to provide shielding. The fuel assemblies, about 7 metres below the surface of the water, must be handled by an overhead crane.

Because of the size and weight of the fuel assemblies, the high level of radioactivity, and the need for cooling, theft of spent fuel would be very difficult. If stolen, the spent fuel conceivably could be used directly in crude dispersal schemes. Plutonium, which could be separated from the fuel only if the adversary had the technology and the facilities for handling the toxic materials, could be used in sophisticated dispersal devices or perhaps in nuclear explosive devices.

Sabotage at the spent fuel pool might be accomplished by removal of a fuel assembly from the pool resulting in overheating and cladding failure and the release of volatile fission products, explosive ejection of the fuel from the pool releasing the gaseous fission products from the fuel rods and dispersing fuel fragments, rearrangement of the fuel into a critical configuration, or removal of cooling, allowing the fuel to heat to the melting point with the resultant release of the volatile and semivolatile fission products. As in the case of the core, the largest off-site releases occur as a result of fuel melting. The only practical means of rapidly removing cooling is an explosive breach of the pool wall, an act requiring significant quantities of high explosives.

2.2.3 Spent Fuel Shipping Cask

After a period of cooling and decay, the spent fuel assemblies are loaded into special shipping casks for shipment to a reprocessing facility or long-term storage facility. The activity of a BWR spent fuel assembly after 120 days of cooling is about 10^6 curies. The shipping casks are heavily shielded and provide cooling for the fuel. A truck cask weighs about 35,000 kilograms and will carry up to seven fuel assemblies; a rail cask can weigh as much as 100,000 kilograms and carry 18 assemblies.

The options for use of the material following theft are the same as for the fuel from the spent fuel pool, the only difference being that the level of radioactivity will be considerably lower than that of fuel just removed from the core. Theft of a shipping cask would be somewhat less difficult than theft of spent fuel from the pool, particularly if the cask is already loaded on a transport vehicle. Successful escape would be a major problem because the adversary would have to transport the large, bulky package in a slow-moving vehicle (tractor-trailer rig). Theft of a rail car seems even more remote. Assuming that the on-site personnel are able to call for off-site assistance, recovery of a stolen cask is likely. Sabotage by explosive attack on a shipping cask awaiting shipment could cause limited dispersal of some of its radioactive contents, primarily on-site.

2.2.4 Fresh Fuel Storage Area

Fresh reactor fuel is shipped to the site where the 200- to 500-kilogram assemblies are stored in dry vaults* in the fuel handling area of the plant (usually adjacent to the spent fuel pool) for a short time pending refueling. At this stage, before it is brought into a critical configuration in the reactor core, the fuel is not highly radioactive and does not require heavy shielding

Low-enrichment uranium fresh fuel would not be a likely target for theft because of its low toxicity (not suitable for dispersal) and its low content of fissile isotopes (not suitable for nuclear explosive device).[5] Isotopic separation and enrichment facilities necessary to convert the fresh fuel into material useful in a nuclear explosive are probably beyond the resources of any subnational group. In the case of the mixed-oxide fuel cycle, the fresh fuel contains plutonium which can be chemically separated from uranium for use in both dispersal and nuclear explosive devices. Of course, the toxic properties of plutonium necessitate special handling procedures.

Sabotage of the fresh fuel in the storage area would involve rearranging the fuel into a critical configuration and the addition of a moderator. Such a procedure could produce a criticality incident with minor (on-site) consequences.

*In some plants the fresh fuel is stored under water in the spent fuel pool.

2.2.5 Radioactive Waste System

The radioactive waste system contains only a small amount of radioactivity (10^2 to 10^5 curies) compared with the other potential sources in the plant. Liquid and gaseous wastes may be stored in large tanks for a decay period prior to release to the environment. Rupturing these tanks could cause small off-site releases. Solid wastes, such as spent resins, are mixed with sand and cement and cast into steel drums. If stolen, the drummed waste could be used for dispersal; sabotage of the solid wastes on-site would have negligible consequences.

2.2.6 Summary

The primary mechanisms for release from each of the sources are summarized in Table 2.1. The events with greatest public consequences are the melting of fuel in the core or the spent fuel pool. Theft is not considered a serious problem at LWRs (see Appendix A). The material most likely to be of interest to the thief is fresh mixed-oxide fuel; the material that would be easiest to steal is probably solid waste. Diversion of small amounts of material over a period of time is not a likely option because fresh fuel is the only material that could be safely handled and it is accessible only after removal from the storage vault, disassembly of the fuel bundle, and opening of a fuel rod. Repeated occurrence of such a sequence of acts would not likely go unnoticed.

TABLE 2.1

Primary Concerns for Adversary Actions at LWRs

System	Primary Adversary Mechanism
Reactor Core	Sabotage leading to core meltdown
Spent Fuel Storage Pool	Sabotage leading to fuel melting or ejection from the pool
Fresh Fuel (Mixed-Oxide)	Theft and ultimate use for dispersal or nuclear explosive
Spent Fuel Shipping Cask	Theft and ultimate use for dispersal
Radioactive Waste System (Liquid and Gaseous)	Sabotage leading to rupture of holding tanks
Radioactive Waste System (Solid)	Theft and ultimate use in dispersal
Fresh Fuel (Uranium)	No likely threat

2.3 Alternate Safeguards System Configurations

As discussed in the previous section, there are numerous possible targets for sabotage or theft at a nuclear power reactor. Furthermore, the structural complexity of the plant means that there are many possible paths from the boundary of the plant to each of the targets. Consequently, there is an enormous number of AASs (combinations of targets and paths) which could lead to release of radioactive material. The safeguards system should provide a capability for interrupting every AAS.* One of the major challenges of the methodology development effort was to provide a means of assessing the effectiveness of reactor safeguards systems against the broad range of possible AASs.

The regulatory approach to safeguarding reactor plants is to define as "vital" all equipment "the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation,"[8] to require that all vital equipment be located within vital areas,[9] and to place physical protection requirements on the vital areas.[9] The licensee is required to demonstrate that the physical protection system for his plant provides "protection with high assurance" against sabotage by a range of adversaries. Protection with high assurance of all vital areas would satisfy the requirement of interrupting (with high assurance) all AASs. However, it might not be necessary to protect all vital areas to the same level.

An earlier study[2] has shown that release of radioactive material from a power reactor plant can be prevented by protection of an appropriate subset of the equipment classified as vital under the definition quoted above. It is also known that release as a result of the long-term transient incidents mentioned in Section 2.2.1 could be prevented by appropriate emergency response by the operating personnel. In upgrading the safeguards system for a plant, it might be sufficient to increase physical protection requirements for some minimum set of vital areas** in order to demonstrate high assurance protection. In addition, it might be possible to reduce requirements on some other vital areas by reliance on emergency response.

To explore the implications of varying levels of protection for vital areas three safeguards system configurations were examined:

1. Uniform level of protection for all vital areas consistent with present and proposed regulatory requirements[9]
2. Additional physical protection for the locations in a minimum critical location set

*Only the portions of AASs which occur on-site are considered because off-site actions (such as preparation for an attack) are not directly affected by the plant safeguards system.

**Protection of this set of vital areas is sufficient to assure that release does not occur. In the remainder of this report such a set of vital areas will be referred to as "a minimum critical location set."

3. Additional protection for the critical locations through use of damage control for long-term transient incidents and physical protection measures to prevent induced loss of coolant accidents (LOCA) and short-term transients.[2]

2.3.1 Uniform Protection for All Vital Areas (Configuration 1)

Current and proposed regulatory requirements at the time of this study are discussed in Appendix D. The thrust of the regulations is that all vital equipment must be enclosed by at least two barriers, one around the protected area[8] and one around the vital area. Thus, the minimum requirement is to provide a perimeter barrier (usually a chain-link fence) and one additional barrier around every vital area. Access to the protected and vital areas must be limited to persons who are authorized to enter the areas. When unoccupied, vital areas must be locked and protected by an intrusion alarm system.

The vital equipment and vital areas for the plant were identified in the fault tree and location analysis portions of the study. A typical LWR has vital equipment scattered throughout the facility. The plant used in this study has 36 vital equipment locations (see Appendix E) with one or more on every floor of the main building, in two separate buildings, and in the protected area outside of buildings.

For the vital equipment located inside the buildings, it is a straightforward matter to provide two protective barriers, the perimeter fence and the walls of the buildings. Two methods of providing the second barrier were considered: (1) access control at all exterior doors of all buildings containing vital areas and (2) access control at the entrances to the separate vital areas. Both of these approaches were evaluated in the analyses.

For some equipment which should be considered vital according to the regulatory definition (such as transformers located outside of buildings), provision of a second barrier is more difficult. A separate fence around the vital equipment would not add significantly to its protection, at least not in terms of barrier delay time,[10] and certainly would not provide protection equivalent to that for vital equipment located inside buildings. Construction of a reinforced concrete structure around vital equipment outside of the buildings seems to be the only means of providing the required second barrier. This would be a costly and perhaps impractical undertaking for existing plants.

2.3.2 Added Physical Protection (Configuration 2)

The second system configuration includes the physical protection measures for all vital equipment discussed above with added physical protection for a minimum critical location set (see Chapter 3). The added physical protection was in the form of an additional alarmed barrier around each critical location so that access to every critical location requires passage through at least three barriers. For critical locations inside the main building the additional barrier could generally be added by providing access controls for another set of doors. For example, the three

barriers were generally provided by employing access control at the perimeter fence, the exterior doors of the building, and the doors to the compartment or room enclosing the critical location.

Other forms of added physical protection (such as increased barrier delay or probability of detection) were also considered in the effectiveness evaluations to determine which factors have the greatest effect on the performance of the system. The information was used to develop an example safeguards system for the plant.

The implications of this configuration for the safeguards system include higher costs for access control equipment or procedures and for alarm systems. An increased impact on operability of the plant can also be expected due to reduced accessibility of the critical locations. On the positive side, the probability of release or theft of radioactive material should be reduced as a result of the added measures.

2.3.3 Added Physical Protection Plus Damage Control (Configuration 3)

The third approach considered was to provide additional protection for the critical locations by using a combination of physical protection and damage control measures. In this approach, damage control measures are used to nullify the adversary acts which lead to long-term transient incidents, and the remaining critical locations are given added physical protection as discussed in the previous section.

There are two reasons for considering damage control as a part of the safeguards system. First, if the requirements for physical protection can be reduced for some areas of the plant, the cost of safeguards (capital costs, recurring costs, and impact on operability) will be reduced. Second, damage control may be the only practicable mechanism for preventing radioactive release caused by destruction of vital equipment in exposed locations (outside of buildings). For example, it may be practically impossible to enclose in well protected structures some of the transformers located outside the buildings.

The damage control options and procedures which might be used to supplement physical protection measures have not been defined in detail. Instead, those events in the fault tree which lead to long-term transient incidents were treated as though they could always be prevented by damage control. Although the results for this configuration are not completely quantifiable, the procedure used does provide an indication of the potential benefits of damage control. Additional study is required to better define the nature and effectiveness of damage control measures and to determine plant design modifications necessary to accommodate damage control systems.

2.3.4 Example System Evaluation and Design

A baseline system was developed for each of the three alternative system configurations. The effectiveness of each configuration was then evaluated by using the methodology described in Chapter 3. The performance characteristics (barrier delay times, alarm system probability of detection, etc.) for the system components were varied over wide ranges to determine which components have the greatest effect on system effectiveness. These data were used along with information on the performance of currently available safeguards equipment to guide the development of example safeguards systems for an LWR. The practical limitations on the use of the subsystems and components which make up the safeguards system were considered in developing the example systems.

CHAPTER 3

METHODOLOGY

A methodology for systematic evaluation of reactor safeguards systems was developed based on the function of reactor safeguards and the general characteristics of LWR plants discussed in the previous chapter. This chapter discusses the principles and assumptions which underlie the methodology, the general analytic framework for application of the methodology, and the details of each step in the evaluation procedure.

3.1 Overview

The function of reactor safeguards is to reduce to an acceptable level the public risk due to malevolent actions directed against reactor facilities. Because there is currently no way to measure public risk directly, the overall safeguards function must be successively expanded into subfunctions which will lend themselves to measurement in some manner. Figure 3.1 illustrates one possible development useful in describing the scope and limitations of the methodology used in this study.

The reactor safeguards system functions of deterrence, physical protection, and consequence mitigation are related to the components of risk,[1]

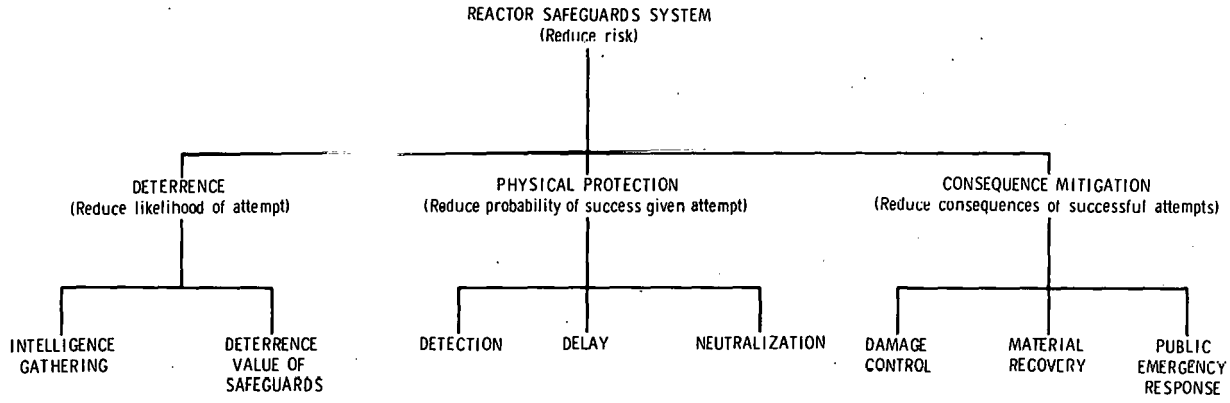


Figure 3.1. Safeguards System Functions

The reactor safeguards system functions of deterrence, physical protection, and consequence mitigation are related to the components of risk,[1] namely the frequency of attempts to produce an event, the conditional probability that attempts will be successful, and the consequences the events produce. However, the details of that relationship are not well established. The components of risk are not independent; for example, the frequency of attempt may be dependent upon the probability of success given an attempt. Because the dependencies among the components of risk and their relationships to safeguards functions are not completely defined, no overall measure for safeguards system performance can yet be identified. Data and concepts are not available for quantification of some of these functions (such as deterrence). In fact, we are not presently able to quantify the effectiveness of any of the functions (deterrence, physical protection, and consequence mitigation) in a precise sense for all adversary action modes. The methodology has therefore been limited to functions and adversary modes for which some level of quantification is possible.

The functions of intelligence gathering, material recovery, and public emergency response in Figure 3.1 are not under direct control of the licensee; rather, they are primarily the responsibility of government agencies. The performance of the physical protection system is directly related to risk and is the direct responsibility of the licensee. Modeling techniques have been developed in previous studies to estimate the probability of success of forcible attacks against a facility given the characteristics of the attacker and the physical protection system. Thus, the effectiveness of the physical protection system in preventing successful attempts was used in this study as a quantifiable measure in lieu of an overall risk assessment measure. The deterrence value is not currently amenable to analysis, but it is likely that deterrence will increase with improvements in physical protection system performance. The potential benefits of damage control and its influence on the physical protection system requirements were also examined in a simplified manner.

The problem of insider malevolent actions and the related issue of deceit mode attack were not addressed explicitly.* Additional work will be required to broaden the methods to include these considerations. The assessment was limited to groups of outsiders using force or stealth. A specific set of adversary attributes (numbers of attackers, weapons, tools, etc.) was not assumed; instead, these attributes were treated as variables with a range of values. It was assumed that the adversaries are limited to subnational groups. Because the reactor safeguards system has no direct interaction with off-site portions of the AAS (such as the preparation phase[1]), only the on-site segments were considered.

*A limited range of insider assistance is accommodated in the simulation model (Section 3.5).

In summary, the methodology developed in this study:

1. Produces a quantitative measure of effectiveness related to risk
2. Considers all sabotage-induced component and subsystem failures leading to significant release of radioactive material
3. Accounts for the structural complexity of reactor plants
4. Is limited to on-site portions of the AAS
5. Considers force and stealth modes of adversary action
6. Addresses outsider attacks only
7. Considers the impact of damage control measures.

Figure 3.2 illustrates the major steps in the methodology developed to satisfy the requirements and limitations listed above. The fundamental analytical tools used in the methodology are fault tree analysis, an extension of basic fault tree techniques called vital location analysis, graph-theoretic modeling, and system simulation modeling. Fault trees are developed to identify the means by which significant release of radioactive material could be initiated by sabotage of vital systems in the plant. These fault trees, along with information on the location of systems and components, identify the buildings, rooms, and compartments from which sabotage can be accomplished as well as those that must be protected to prevent release from the plant. In other words, the vital location analysis identifies the potential sabotage targets. The impact of damage control procedures on the number of targets is also examined by manipulation of the fault trees. Paths from the boundary of the plant to each of the targets are then selected by application of graph-theoretic techniques. The effectiveness of the plant safeguards system in interrupting the adversary action sequences along these paths is examined in a simulation model applicable to force or stealth modes of attack. The role of each of these mathematical techniques in the effectiveness evaluation process is discussed below.

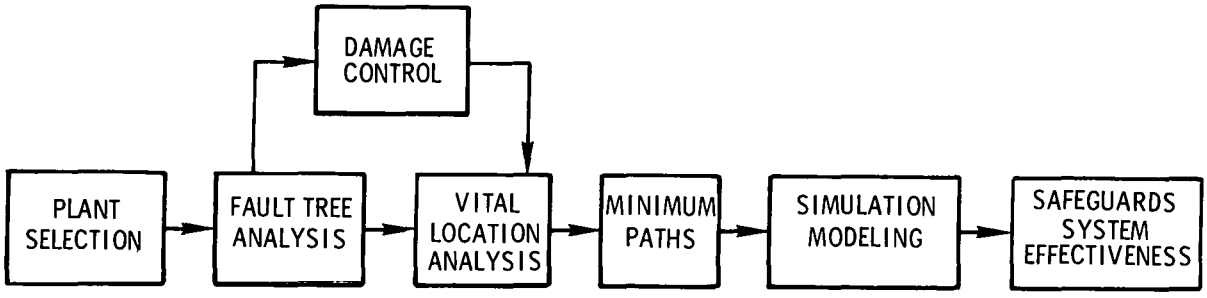


Figure 3.2. Major Steps in the Methodology

3.2 Fault Tree Analysis

Nuclear power reactors are designed with redundant and diverse systems to prevent release of radioactive material. To define the many possible combinations of events which could cause a significant release from the plant requires the application of a systematic analytic method; fault tree analysis has been found to be an appropriate tool for this purpose. The fault tree analysis provides a means of determining the potential sabotage targets for a reactor.

A fault tree is a logic diagram which graphically represents the combinations of component and subsystem events that can result in a specified undesired system state. The undesired state (or event) for our purposes is the release of significant amounts of radioactive material from the plant as a result of sabotage. In the fault tree analysis, this undesired event is developed into logical combinations of less complicated events, each of which is further developed in turn until primary events terminate each branch of the tree. Primary events are individual sabotage acts such as disabling a pump or severing a pipe. As an example, Figure 3.3 shows the top portion of the sabotage fault tree for an LWR. In this figure, the undesired event is developed into intermediate events representing release from each of the primary sources of radioactive material. Fault tree symbols are identified in Table 3.1. Each gate in the tree represents the logical operation (OR or AND) by which the inputs combine to produce an output. Figure 3.3 illustrates that release from the plant can occur as a result of release from any one of three possible sources. Release from one of the sources, the spent fuel pool, is developed further in Figure 3.4. Each branch of the tree is developed in a similar manner.

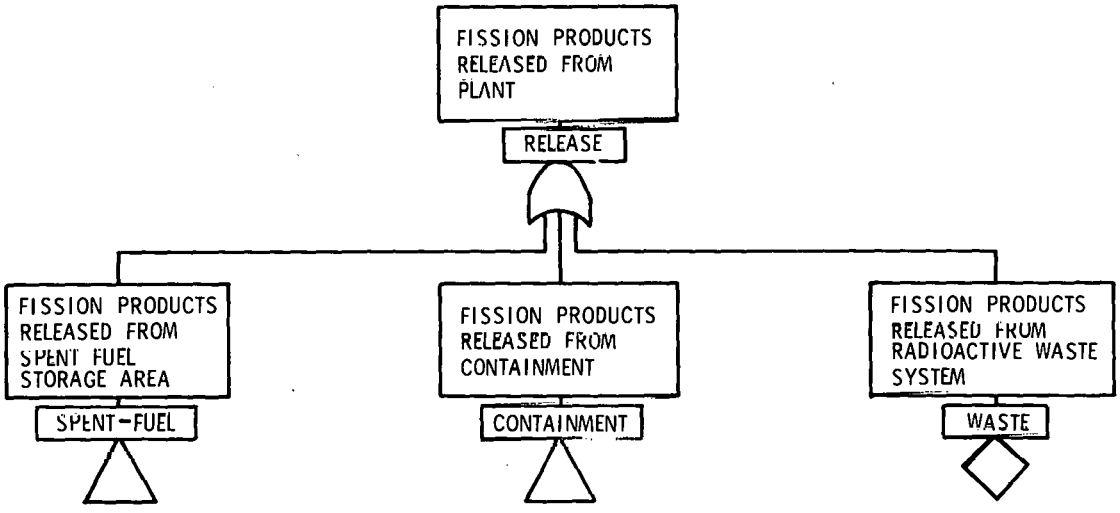
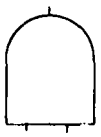
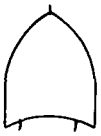
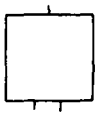
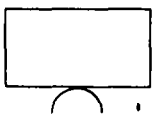
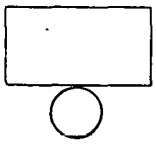
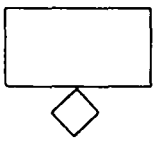


Figure 3.3. Fault Tree for [FISSION PRODUCTS RELEASED FROM PLANT]

TABLE 3.1

Symbols Used in the Graphical Representation of a Fault Tree

		Gates
AND GATE		The AND gate describes the logical operation whereby the coexistence of all input events is required for the output to occur.
OR GATE		The OR gate describes the logical operation whereby the output event will occur if one or more of the input events occurs.
SPECIAL GATE		The SPECIAL gate describes the logical operation whereby the output event will occur if a specified combination of input events occurs. The definition of the gate must be accompanied by a logic equation specifying the output event occurrence as a function of the input event occurrences.
		Intermediate Events
INTERMEDIATE EVENT		A rectangle above a gate represents the output event produced by the gate's logic.
		Primary Events
BASIC EVENT		The rectangle above a circle identifies a BASIC event. A basic event is one whose causes will not be further identified.
UNDEVELOPED EVENT		The rectangle above a diamond identifies an undeveloped event whose causes have not been identified, often because there is a more attractive alternative.
		Transfer Symbols
TRANSFER IN		The triangles are used as transfer symbols. The event logic flows from the transfer-out symbol to the transfer-in symbol in a manner as if the events or gates were connected directly with a single line.
TRANSFER OUT		

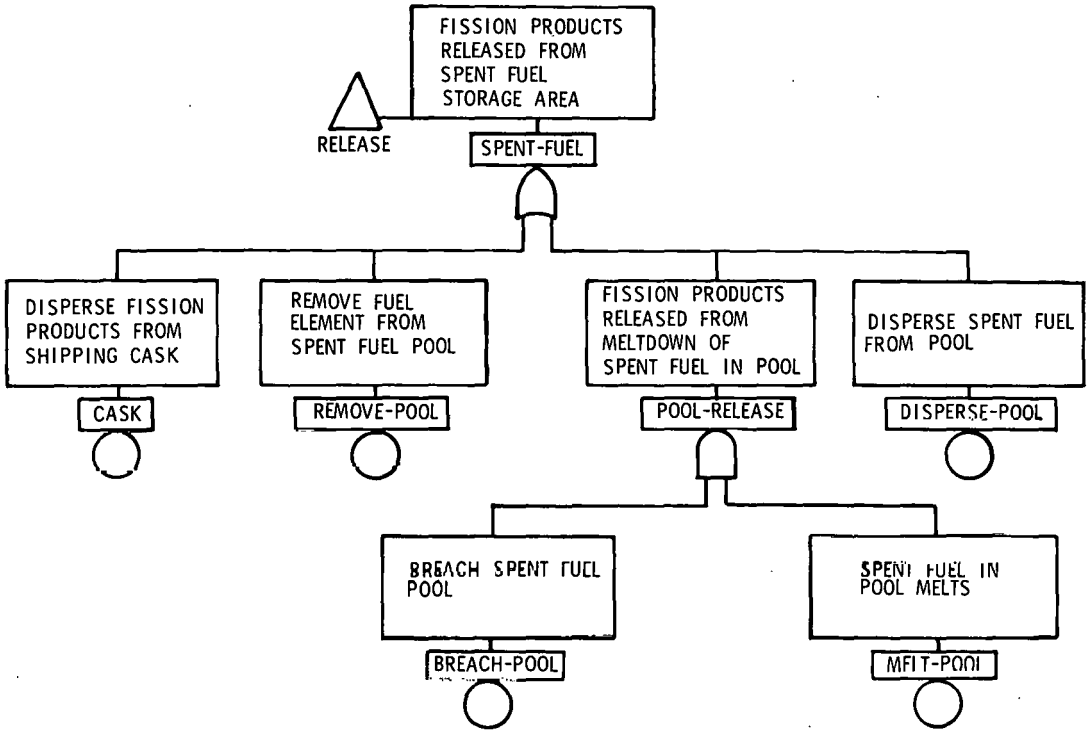


Figure 3.4. Fault Tree for [FISSION PRODUCTS RELEASED FROM SPENT FUEL STORAGE AREA]

From a fault tree an equivalent Boolean (logic) equation can be developed.[11,12] Each event in the tree is given a label as indicated in the small rectangle associated with each event symbol in Figures 3.3 and 3.4. In the Boolean equation these labels are referred to as literals, and the literals are joined together by the logical operators $\vee$ (OR) and $\wedge$ (AND) as indicated by the fault tree gates. The Boolean equation for the branch of the tree shown in Figure 3.4 is:

$$\text{SPENT-FUEL} = \text{CASK} \vee \text{REMOVE-POOL} \vee \text{POOL-RELEASE} \vee \text{DISPERSE-POOL} \ . \tag{3.1}$$

Replacing the event POOL-RELEASE with its logical equivalent POOL-RELEASE = BREACH-POOL $\wedge$ MELT-POOL gives:

$$\text{SPENT-FUEL} = \text{CASK} \vee \text{REMOVE-POOL} \vee \text{DISPERSE-POOL} \vee \text{BREACH-POOL} \wedge \text{MELT-POOL} \ , \tag{3.2}$$

where the $\wedge$ (AND) operation is done before $\vee$ (OR) in the same way that multiplication precedes addition in ordinary algebra. Equation 3.2 contains four terms separated by OR operators. The first three terms have one literal and the last term has two literals. The occurrence of any term in such an equation causes the output event on the left-hand side of the equation. Thus, Equation 3.2 simply states that the event SPENT-FUEL occurs if CASK occurs or REMOVE-POOL occurs or DISPERSE-POOL occurs, or if both BREACH-POOL and MELT-POOL occur. A logic equation,

equivalent to the fault tree, is obtained by successive substitution of events lower in the tree for ones higher until the undesired event is expressed solely in terms of primary events. Each combination of primary events sufficient to cause release appears as a term in the logic equation representing the tree; thus each term represents a "scenario" which must be prevented. Boolean algebraic manipulation of the equation[11] provides a powerful analytic tool for determining protection requirements.

3.3 Vital Location Analysis

The primary events in the fault trees are sabotage actions which in proper combinations (as specified by the logic of the tree) can lead to release of radioactive material from the plant. It is also important to know the specific locations in the plant to which the adversary must go to accomplish these acts in order to ensure that the safeguards system design includes protective mechanisms for the buildings, rooms, and compartments within which the sabotage actions can be accomplished. In the next step in the modeling process, Vital Location Analysis, each primary event in the system fault tree is replaced by the location or logical combination of locations where the action can be accomplished. This amounts to a transformation of variables* in the event equation described above to obtain a location equation for the undesired event. This location equation represents the combinations of locations to which the adversary must gain access in order to cause the undesired event. Each combination of locations (each term in the location equation) may represent a single combination or thousands of combinations of primary events, depending upon how many events can be accomplished at each location and how the events combine to produce release. Because there are usually fewer locations than primary events, the location equation is typically much simpler than the event equation.

Figure 3.5 illustrates the mapping from the event space to the location space with a simple example. The ten initiating events (E1 through E10) combine in six ways to produce the undesired event, SAB; that is, there are six terms in the event equation, Equation 3.3, where each term is enclosed in parentheses.

$$SAB = (E3) \vee (E4) \vee (E5) \vee (E1 \wedge E2) \vee (E6 \wedge E7) \vee (E8 \wedge E9 \wedge E10) \quad . \tag{3.3}$$

*The location analysis uses the SETS Boolean manipulation program in ways similar to those used in common cause analysis.[13,14]

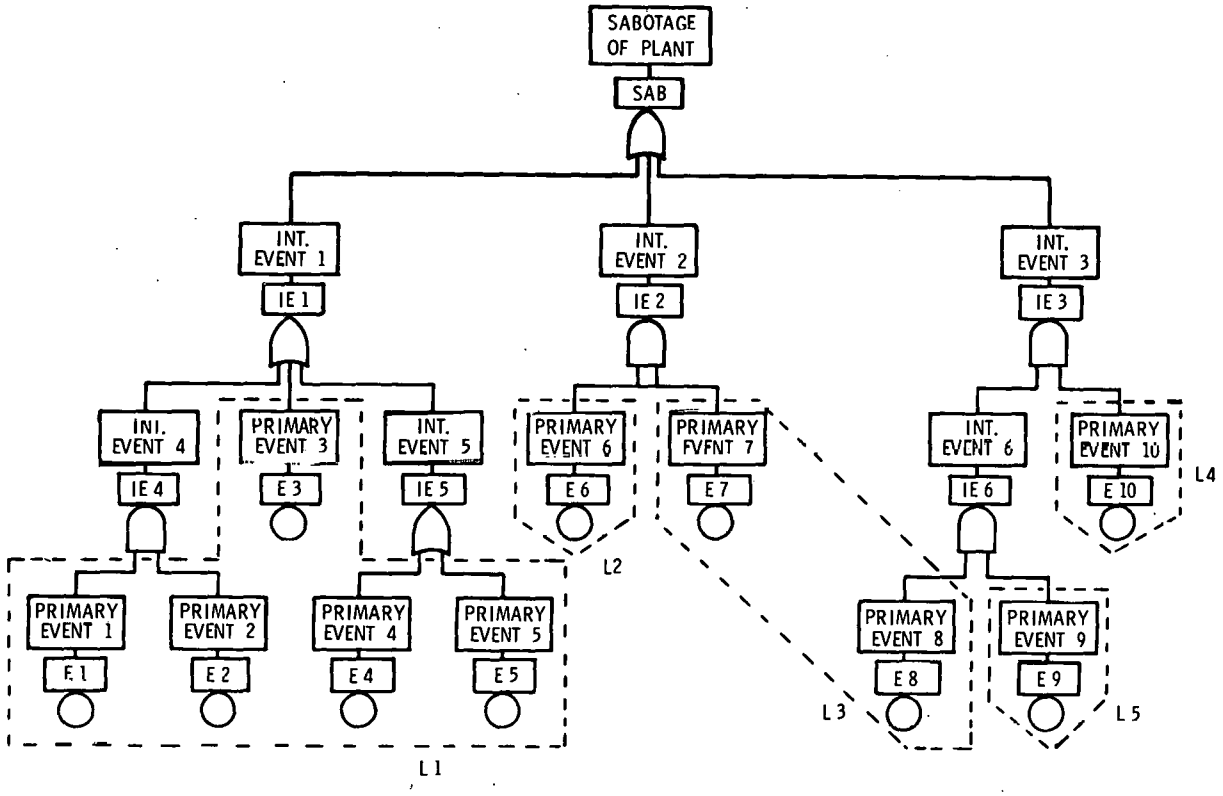


Figure 3.5. Example Fault Tree Events and Locations

The dashed lines in Figure 3.5 indicate the locations (L1 through L5) at which the events can be accomplished. For example, primary events E1, E2, E3, E4, and E5 can all be accomplished at plant location L1. Replacing the events in Equation 3.3 with locations and applying the appropriate Boolean identities* gives three combinations of locations at which the undesired event can be initiated as shown in Equation 3.4.

$$SAB = (L1) \vee (L2 \wedge L3) \vee (L3 \wedge L4 \wedge L5) \quad . \tag{3.4}$$

Figure 3.6 illustrates a location tree for the example. The six terms in the event equation are translated into three terms in the location equation as follows:

$$SAB = \underbrace{(E3) \vee (E4) \vee (E5) \vee (E1 \wedge E2)} \vee \underbrace{(E6 \wedge E7)} \vee \underbrace{(E8 \wedge E9 \wedge E10)}$$

$$= \qquad (L1) \qquad \vee (L2 \wedge L3) \vee (L3 \wedge L4 \wedge L5) \cdot$$

*In Boolean algebra the following identities hold: $A \vee A = A$; $A \wedge A = A$; $A \vee (A \wedge B) = A$.

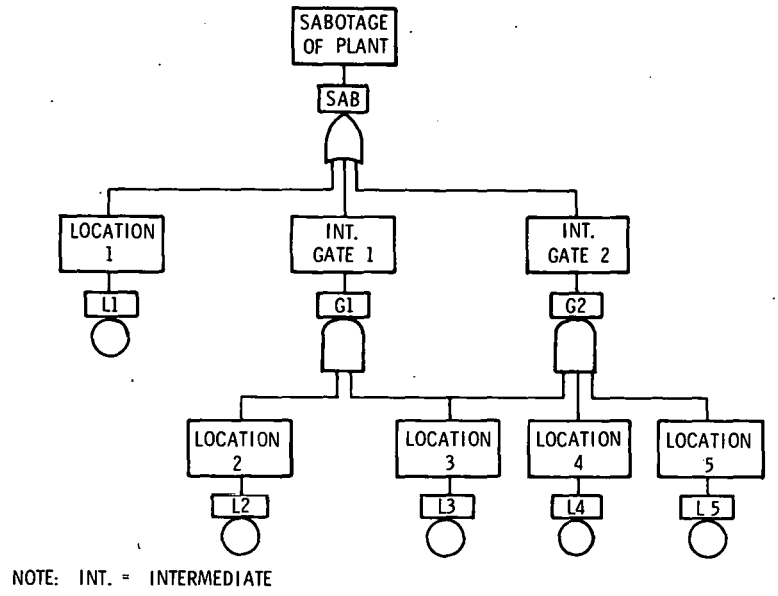


Figure 3.6. Example Location Tree

As in the case of this simple example, the transformation from sabotage acts to locations generally reduces the number of literals and the number of terms in the equation. This reduction is essential in enabling us to perform some of the subsequent analyses.

Because there are too many event combinations in the reactor fault tree to list them all, it is impossible (and unnecessary) to list all of the event combinations in each location set as was done in the example. The location equation is processed further to identify a minimum set of locations (minimum critical location set) the protection of which will interrupt all possible sequences leading to release. This is done by taking the Boolean complement (logical NOT) of the location equation.

Whereas a Boolean equation for an event represents the ways the event can occur in terms of the occurrence of the literals in the equation, the complement of the equation represents the ways to preclude the event in terms of nonoccurrence of the literals. The complement of SAB is:

$$\overline{SAB} = (\overline{L1} \wedge \overline{L3}) \vee (\overline{L1} \wedge \overline{L2} \wedge \overline{L4}) \vee (\overline{L1} \wedge \overline{L2} \wedge \overline{L5}) \ , \qquad (3.5)$$

where the overline indicates the complement (nonoccurrence) of the event. For the locations, the complement implies that access has been denied. Equation 3.5 shows that SAB will not occur if access is denied to both L1 and L3, or to L1 and L2 and L4, or to L1 and L2 and L5. If access is denied to all the locations in one term of the complement equation, then none of the event combinations leading to release can be accomplished. The terms in the complement equation can be ordered according to the number of locations in each term or any quantitative values (such as cost of protection or impact on operability) which can be associated with each location.

Damage control, which provides a defense against the results of certain sabotage acts,[2] can reduce the requirements for physical protection in some areas of the plant. The potential impact of damage control measures on the minimum number of locations which must be protected can also be assessed by manipulation of the fault trees. Consider, for example, Equation 3.5 which indicates that a combination of access denial to L1 and L3 will preclude SAB. If all sabotage acts at L3 could be negated by damage control measures, then SAB could be precluded by just protecting L1. Analyses such as these can help set priorities for protection of vital locations.

3.4 Minimum Path Analysis

The previous portion of the analysis identified a set of plant locations which the safeguards system must protect. The next step is to select for detailed analysis one or more paths from the boundary of the facility to each of the locations of interest. The paths of greatest interest are ones which optimize the adversary's probability of success and therefore place the greatest stress on the safeguards system. The process of selecting candidates for these "most stressing" paths is discussed in this section.

Rather than trying to evaluate every AAS independently, the approach taken here is to determine an upper bound on the likelihood of adversary success. To conservatively evaluate the safeguards systems, we have assumed that the adversary will optimize his action sequence; thus, it is necessary to know what paths through the plant are optimal for the adversary. Given the critical locations, identified by means of the above fault tree and vital location analyses, the approach used in this study is to find one or more minimum-time paths to each critical location. Minimizing time does not necessarily maximize probability of adversary success. But, as is discussed in Section 3.5, minimizing time is probably a good adversary strategy for forcible attack against the example plant. Techniques are under development which will allow computation of paths that are truly optimum for the adversary.

Paths are computed in a graph-theoretic model of the plant and are displayed on a computer graphics system as discussed in the following sections.

3.4.1 Graph-Theoretic Modeling

For purposes of pathfinding, a discrete model of the plant layout, called a graph, is developed. A graph is simply a network of nodes and arcs. The nodes represent locations on the boundary, on the internal barriers, and at targets, while the arcs represent ways to travel between locations. Both the nodes and the arcs are assigned weights which are measures of some quantity to be minimized.

The particular kinds of paths to be found and the rules for computing path length depend on the meaning of the weights, whether the weights depend upon the direction of travel, the type of penetrations assumed at the nodes, and whether the problem is that of theft or sabotage. In

models available at the time of this study, the weights are nonnegative constants, independent of the direction of travel. In the graphs used in this study, the weights indicate adversary action times for different tasks in the sequence, and path length is the sum of the weights of the nodes and arcs in the path. The node weights represent barrier and boundary penetration times as well as material removal or equipment destruction times, and the arc weights represent transit times. In this case, shortest paths are those which minimize time. Other measures of path length, such as distance or detection probability can be used also, but only shortest-time paths were considered in this study.

Algorithms for selection of minimum paths have been developed for both theft and sabotage problems,[15,16] the primary difference being that to succeed in a theft the adversary must steal something and escape while escape of the saboteur is not essential to sabotage success. Therefore, the sabotage problem is to find all the shortest paths beginning at any boundary node and passing through a sufficient set of vital target nodes, but not returning to the boundary. This problem is difficult to solve, being related to the "traveling salesman problem"[17] for which no efficient (polynomial run time) algorithms are known. However, a lower bound on the sabotage times can be obtained efficiently by studying the worst-case situation of simultaneous sabotage by several teams each having only one target. Here the problem is to find all the shortest paths from the boundary to each target location. (See Reference 16 for a detailed description of this model together with a treatment of node and arc weights which depend on the direction of travel, as well as a study of the independence of the paths of the several sabotage teams.)

In a complex facility such as a nuclear power plant, an adversary has an enormous number of alternative routes to the target areas from which to choose. Identifying and evaluating the length of every path of the type to be minimized is impractical, even with a computer. For example, a graph with only 15 nodes can have as many as $13! = 6,227,020,800$ paths between a given pair of nodes, and reactor plant models can involve more than 100 nodes. Furthermore, it is not sufficient to find just one shortest path to some target. In order to provide adequate safeguards, the analyst must know all the shortest paths, particularly the very obscure ones.

A very efficient shortest path algorithm, due to Dijkstra[18,19] and modified by Yen,[20,21] has been adapted and applied to both the theft and the simultaneous sabotage problems. This algorithm is the best known procedure for finding the lengths of the shortest paths from one node to all others. When supplemented with a process which retraces and saves all the shortest paths as well as their lengths, the procedure is guaranteed to work in a run time proportional to the square of the number of nodes. The efficiency of the Dijkstra scheme stems from the fact that it gathers information only about the shortest paths and thereby avoids wasting time on the vast number of nonshortest paths. In Appendix B, a description is given of the Dijkstra-Yen algorithm as it is applied to the simultaneous sabotage problem.

3.4.2 Computer Graphics Display System

An interactive computer graphics program has been developed to display the shortest paths in a graph of a nuclear power reactor plant. The physical layout of the plant (locations of buildings, obstacles, equipment, and vital materials) can be displayed in plan view on the graphics screen together with the shortest paths to the vital locations. The interactive capability allows the analyst to change plant characteristics from the graphics terminal.

The internal barriers subdivide a plant into regions, and each level of a building contains one or more regions. To display the physical arrangement of either a level or a region, it is necessary to digitize (1) the end points of lines defining the level or region, (2) the coordinates of the graph nodes (boundary, barrier, and target) of the level or region, and (3) the coordinates of pseudo-nodes* which outline obstacles within a region. These coordinates are also used to automatically compute the arc weights for the graph model.

The arc weights are the transit times between each pair of nodes in a region. In each region an auxiliary graph is constructed by connecting every node and pseudo-node by a straight line to every other node and pseudo-node, except that such lines intersecting obstacles in the region are deleted. Floyd's algorithm[22,19] is applied to each auxiliary graph to find the lengths of the shortest paths between every pair of nodes in the region. Because of the way the auxiliary graph is constructed, these distances are the lengths of routes which go around, not through, obstacles within a region. Therefore, distances for shortest physical routes between nodes are obtained, and these are divided by travel speeds to obtain the desired arc weights.

3.5 Simulation Model

A dynamic simulation model was developed in the Special Safeguards Study to simulate the complex interactions between adversaries and security system components.[23] The purpose of the model is to explore the relative importance to safeguards system effectiveness of various safeguard system characteristics (such as probability of intrusion detection, delay times, and guard force characteristics), adversary attributes, and attack paths.

The Forcible Entry Safeguard Effectiveness Model (FESEM) was used to evaluate alternative safeguards system configurations. The model requires as input the characteristics of the fixed-site to be evaluated including (1) the number, size, and response time for the response forces and probability of their receiving valid communication of both external and internal attacks,** and probability of their receiving valid communication of both external and internal attacks,**

*Pseudo-nodes are used only in determining shortest arcs around obstacles and do not appear explicitly in the graph-theoretic representation of the plant.

**External implies no inside assistance while internal means the adversary has inside assistance.

(2) the number, type, and thickness of barriers, and the probability of detection at alarmed barriers for external and internal attacks, (3) the distance between barriers, and (4) the probability of a high explosive (HE) detonation being detected if the adversary uses HE to penetrate a barrier. The information for items (2) and (3) can be obtained from the data used or generated in the minimum path analysis.

The model is capable of selecting the adversary attributes from a range of input values for attacks against the fixed-site design. These attributes include the number of adversaries, types of weapons (side arms or automatic weapons), and their resources for barrier penetration (such as tools but no HE or tools plus HE). In addition, four types of adversary attacks can be simulated: sabotage/internal, sabotage/external, theft/internal, and theft/external. Internal attacks imply that the adversaries have an insider working at the fixed-site who may, by intent or under duress, degrade the alarm and communication systems. The mode of transportation (vehicles, no vehicles, or air vehicles) and the dedication of the adversaries are also selected as input variables in the generation of adversary attributes.

Given these inputs, along with an attack path, the FESEM can simulate a large number of adversary attacks against the site design to evaluate the effectiveness of the design concept. Barrier breaks, delays provided by barriers, crossing times between barriers, and advancements along the paths are simulated by a random sample from input probability distributions. Alarms at a given barrier may trigger communications to the on-site guard force which moves to the scene and assesses the situation. Off-site guards are called if a serious alarm condition exists. Upon the arrival of any guard force, an engagement is initiated with the adversary. During the engagement simulation,[24,25,26] the adversary advancement is assumed to be interrupted. If the adversary wins the engagement, then his advancement continues until interrupted by the arrival of the next response force or completion of the theft or sabotage. This ends one simulation. After a large number of attacks has been simulated, statistics are accumulated to determine the relative effectiveness of the safeguards system against the assumed level of threat.

The primary output of the simulation model is the probability of adversary defeat, P_{SI}, which represents the probability that the safeguards system will function properly and will prevent the adversary from completing his intended malevolent action. In principle, a P_{SI} could be computed for every forcible adversary action sequence which might result in release or theft of material; in practice, it is possible to consider only a small fraction of the very large set of possible sequences. Thus, the simulation modeling was limited to sequences along the shortest-time paths to each of the critical locations. This procedure determines an approximate lower bound on P_{SI} for all sequences in the following manner. Because one or more of the critical locations must be visited in every sequence, the time to complete any sequence must be greater than or equal to the shortest of the paths to the critical locations. Such minimum-time paths are not, however, guaranteed to be the minimum P_{SI} paths because P_{SI} depends on factors other than time. On the other hand, each target in the system configurations considered is surrounded

by at least two layers of detection devices, each layer having uniform detection probability (all the doors into the reactor building have the same kind of alarm). This means that shortest-time paths in this study tend to have least detection probability also. Thus, the P_{SI} for a minimum-time path is likely to be close to the minimum P_{SI} for forcible attacks because P_{SI} can be expected to increase as the duration of the adversary sequence increases. Further work is required to develop a measure for the graph which will guarantee that minimum P_{SI} paths are selected.

Damage control measures were assumed to provide assured interruption of all sequences leading to long-term transient incidents in those safeguards system configurations using damage control; that is, no simulation was performed for those acts following destruction or damaging manipulation of equipment.

3.6 Summary

Although the methodology discussed in this chapter is limited in the range of adversary sequences that can be analyzed and addresses a measure related to risk rather than quantifying risk directly, it represents an important step in the development of a comprehensive safeguards system evaluation procedure. The basic steps of identifying targets, finding minimum paths to those targets, and evaluating adversary success along those paths provide a logical approach for safeguards system evaluation, regardless of the adversary action mode or facility type. The models and input data can be upgraded as the conceptual and practical constraints on the safeguards system assessment problem are overcome. The next chapter presents the results of application of the methodology to an LWR plant.

CHAPTER 4

APPLICATION OF THE METHODOLOGY TO A TYPICAL LWR PLANT

To evaluate different safeguards system options and to verify the applicability of the method described in the previous chapter, a detailed, conceptual study was performed for a typical nuclear power reactor plant. This typical plant provided a physical model for the structural characteristics and equipment layout. Safeguards systems representing the three alternative system configurations discussed in Chapter 2 were proposed for the typical plant. The effectiveness of each of the systems was evaluated by application of the methodology discussed in Chapter 3. The elements of the safeguards systems which contribute most to overall system effectiveness were identified by examining in the simulation model the sensitivity of the effectiveness measure (P_{SI}) to changes in the system parameters. Finally, an example safeguards system was designed, based on the insights gained from these analyses. In this chapter, the implementation and evaluation of the system configurations are discussed, the concepts for LWR safeguards systems developed from the evaluations are summarized, and exemplary system designs are presented.

4.1 Assessment of Alternative System Configurations

4.1.1 Scope of the Evaluation

The problem studied in detail is a forcible attack by a group of outsiders with the objective of sabotage. Some limited theft sequences are also evaluated. Actions of interest are those that occur from the time the perimeter penetration begins until the adversary has completed the destruction or damaging manipulations which will lead to off-site release (sabotage) or until he has removed nuclear material from the site (theft). In the system configuration which uses damage control measures, it is assumed that all long-term transient incidents[2] can be nullified by the damage control actions.

The adversary attributes were treated parametrically to establish the critical values of the attributes for various system configurations. The number of attackers ranged from 4 to 16. It was assumed that the adversary force was armed with automatic weapons and that they breached barriers without the use of explosives. * Penetration of building walls was assumed to occur at

*The use of explosives increases the probability of detection of barrier penetration in the simulation model because it is likely that someone would hear the explosion, but does not significantly decrease barrier penetration times for the barriers of interest.

doorways; the locks were picked or cutting equipment was used to penetrate the doors. The adversary was assumed to be traveling on foot, and the motivational parameter was varied from medium to high. Shortest-time paths were computed for each of the critical locations for each of the safeguards system configurations, and these paths were used in the parametric studies of system performance. The parametric studies disclosed the physical protection elements which had the greatest effect on the overall system performance measure, P_{SI}. Upgrades in these elements were proposed in exemplary safeguards system designs in an attempt to develop cost-effective options for site protection.

4.1.2 Fault Tree Analysis Results

The fault tree for sabotage of the example plant was developed in an earlier study.[2] There are approximately 250 primary events in the tree and an enormous number of ways these events can combine to cause release of radioactive material from the plant. The basic events in the fault tree were replaced with the locations at which they can be accomplished (see Appendix E). With the exception of the locations of transformers outside the main structures, the locations are rooms, compartments, or buildings enclosed by physical barriers. The unit auxiliary, emergency auxiliary, start-up and emergency, and cooling water pump transformers are located in four widely separated regions of the protected area and have been given separate location numbers even through it is not necessary to penetrate a barrier in traveling between them. The basic events in the typical-plant fault tree and the locations with which each can be replaced are given in Appendix E.

Thirty-six vital areas were identified for the 250 primary events. In some locations many events can be initiated (the drywell for example), and some events can be initiated at more than one location (disabling a valve at the valve or at its motor control center for example). There are 123 combinations of locations from which sabotage can be initiated for the typical plant, ranging from a single location to as many as six separate locations. Thus, the transformation from sabotage acts to locations reduces the number of literals from 250 to 36 and the number of terms from an enormous number to 123 in the equations for the typical plant.

The complement of the radioactive material release equation for the typical plant contains many terms (combinations of locations) each containing 15 or more literals (locations). Denying adversary access to the locations in any term of the complement equation assures that the undesired event cannot be initiated. Thus, to protect the example plant, protection of 15 of the 36 target areas would assure interruption of all adversary action sequences.

Certain of the locations in the typical plant are not enclosed in secure structures and would be very difficult to protect. To evaluate the impact of not protecting such equipment, we assumed that the adversary was able to complete the sabotage acts at only the exposed locations and found that release of radioactive material could occur under these conditions. That is true because certain long-term transient incidents can be initiated if the adversary gains access to the exposed locations.

To assess the possible benefits of damage control, those initiating or intermediate events which lead to long-term transients were eliminated from the fault tree. The resulting equation for release contained 185 combinations of from one to eight locations (Appendix E). The complement of the damage control equation contained many terms, the minimum one having 11 locations. Thus, an effective damage control capability could reduce by four the number of locations for which physical protection is essential.

One additional factor has been considered to reduce further the number of locations that must be considered, namely that some locations are "inside" other locations. The plot plans in Appendix D show, for example, that access to the containment penetration rooms (L6 and L32), the drywell (L4), and the steam tunnel (L14) requires access to the third level of the reactor building (L5). Denying access to L5 automatically denies access to L4, L6, L14, and L32. Taking these common features and damage control into account, one finds that the minimum complement set contains eight locations. These are the eight locations of the plant against which attacks were simulated.

Figure 4.1 illustrates the process of selecting the priority areas for protection for the example plant. In this example the objective was to find the minimum number of locations whose protection eliminates the possibility of radioactive release caused by sabotage. Criteria other than number of locations could be used to select the best complement set. Cost or impact on plant operability might be of interest to the plant owners. If quantitative values for these or other criteria can be established for each location, the complement sets can be ordered according to those criteria. The optimum set for some other measure may not be the set with the minimum number of elements.

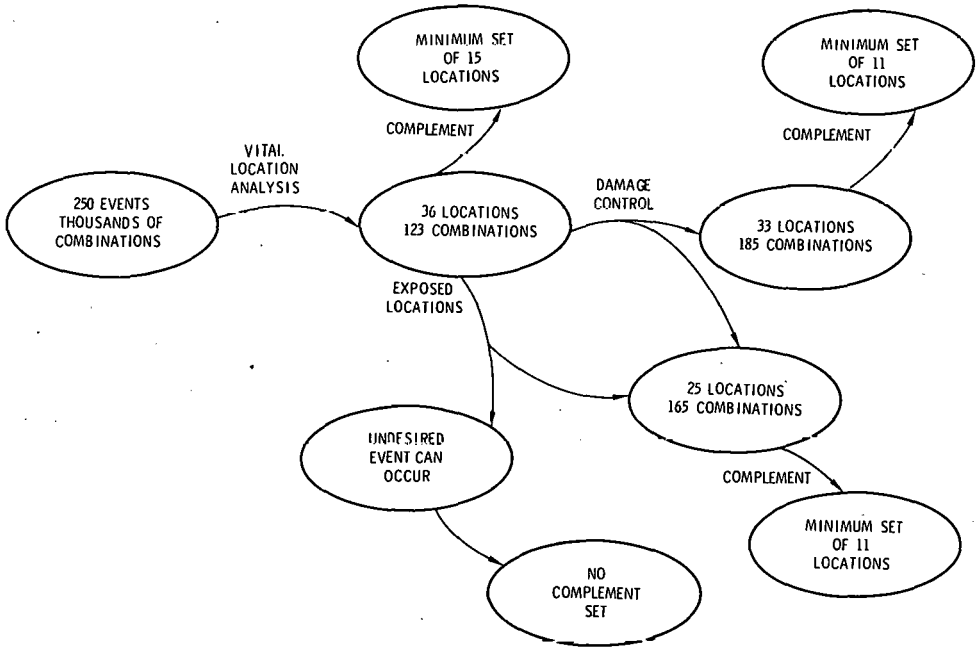


Figure 4.1 Selection of Critical Locations

4.1.3 Graph Model of the Plant

A graph of the example plant was developed for use in the process of optimum path selection. The coordinates of all points of interest were obtained from scaled plot plans of the facility, and the graph was constructed to give an accurate visual representation of the site.

First, the plant was divided into "levels" to provide a convenient unit for display of results. A level was assigned for each floor of the main structure, the diesel generator building, the pump structure, two floors of the administration building, and for the region outside the buildings. Level designations are discussed and illustrated in Appendix F. Level 7, the outside area, is shown in Figure 4.2, and Level 3, the third floor of the main building, is shown in Figure 4.3.

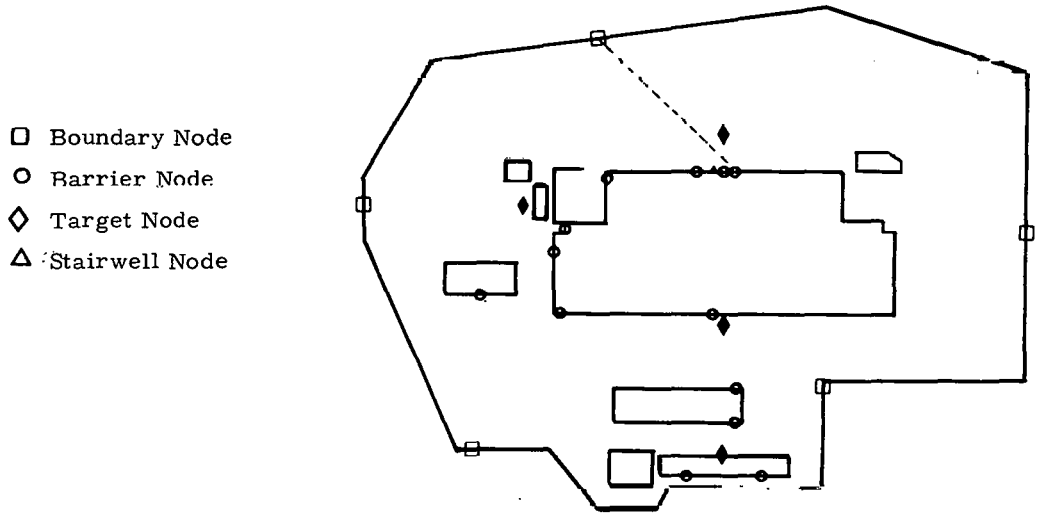


Figure 4.2 Simplified Overall Plot Plan

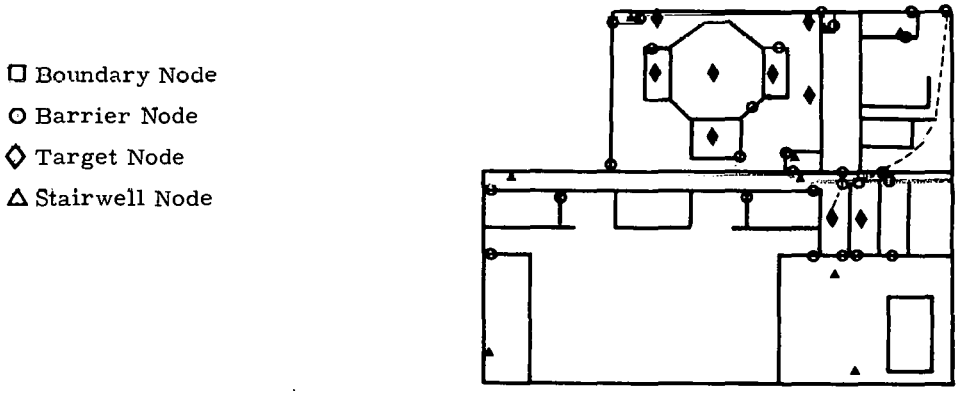


Figure 4.3 Simplified Floor Plan for Level 3 of the Main Building

For each level, regions were determined, based on the physical layout, so that each region represents an area within which movement is unimpeded by barriers. In most instances the regions had the same physical boundaries as the locations defined in the location analysis. * Penetration points in the barriers which surround each region, target points within the vital areas, and points at which transitions from one level to another can occur were identified as nodes in the graph. The boundaries of obstacles which paths must bypass were marked with pseudo-nodes to allow the construction of physical paths in each region. In some cases doorways were omitted if they led to dead-ends or could be combined with adjacent ones to form a single node (roll-up equipment doors adjacent to personnel doors, for example).

The reactor buildings and turbine buildings for the two units of the example plant are mirror-imaged about the centerline of the main structure. The radwaste building and control room are shared by the two units. To reduce the number of nodes in the problem, the duplicated portions of the plant were not included. Paths to vital locations in one unit will be the mirror images of those in the other so that all of the unique paths are included by considering only half the plant.

Five boundary nodes were arbitrarily selected as penetration points in the perimeter fence, as shown by the squares in Figure 4.2, to give representative cases for adversary access to the site. In addition to the five boundary nodes, there are 120 barrier nodes, 32 hardware or vital equipment nodes, 652 arcs, 11 levels, and 82 regions in the graph for the example plant.

A time-weight was assigned to each node and arc in the graph. The node weights are estimates of the mean time it would take the adversary to penetrate a barrier or to complete a sabotage act on a piece of equipment. Table 4.1 lists the barrier node weight values used for the typical plant graph. Different sets of doors were locked in the alternative system configuration and the appropriate node weights on the graph were changed to reflect these differences. The computer graphics model used the data on node positions to find the shortest possible arcs between every pair of nodes in each region. The length of each arc was divided by a speed of 1.3 m/s (3 mph) to obtain a transit time. The speed used was an estimate of the rate of travel for an adversary on foot.

---

*The exception is the area inside the perimeter boundary but outside the buildings. For computing paths, this area is treated as a single region, whereas in the location analysis, each set of transformers in the yard was assigned a different location.

TABLE 4.1

Barrier Node Weights for the Example Plant*

Barrier Type	Penetration Time (s)			Standard Deviation
	Mean	Min	Max	
Chain Link Fence	30	15	45	5
Steel Door, Locked	180	120	240	20
Watertight Door, Locked	600	420	780	60
Gate House	120	100	140	7

*Barrier node weights are estimates based on experimental data available at the time of the study[10] and the judgement of physical protection system designers.

The weights for arcs connecting one level to another (via stairwells or elevators) were assigned rather than computed in the graphics program to avoid unnecessary complication. For these arcs, the weights were based on the vertical distance between levels and an assumed vertical speed of approximately 0.5 m/s.

The algorithm described in Chapter 3 and in Appendix B was used to find the shortest-time paths from the boundary of the facility to each of the vital areas. The data on these paths for each system configuration are tabulated and displayed in Appendix F. The shortest-time path to a particular target for one configuration is illustrated by the dashed lines on Figures 4.2 and 4.3. Barrier sequences, penetration times, and transit times were extracted from the shortest path data, for use in the simulation modeling.

4.1.4 Simulation Modeling

The final step in the evaluation process is the simulation of adversary/physical protection system interaction. Details of the application of the FESEM to the typical plant with the alternative safeguards system configurations are given in Appendix G. This section contains a summary of the basic approach and general results.

Components and subsystems were selected to implement each of the alternative configurations for the plant studied. Appendix D contains plant layout drawings showing the locations of barrier and alarm systems for each of the configurations. The safeguards system for each configuration was given the following parameters: (1) communication to the on-site and off-site response forces occurs with a probability of 0.9; (2) the on-site guard force includes four guards who can respond to an alarm; two were scheduled to arrive in 2 minutes, one in 2-1/2 minutes, and one in 3 minutes after an alarm; (3) the off-site force was composed of one man in 15 minutes, one in 30 minutes, 20 in an hour, and 30 in 2 hours; (4) it was assumed that all guards were armed and were prepared to engage the adversary with lethal force; and (5) the guard dedication and

sophistication parameter was set at "medium" for the baseline systems. These data on the site parameters together with the adversary description given earlier (4 to 16 attackers, automatic weapons, tools without HE for barrier penetration, medium dedication and sophistication) were used in the FESEM to estimate the effectiveness for each system configuration. The parameters were then varied for configuration 3 to determine sensitivities and critical elements.

After some preliminary simulation runs to establish trends and expected directions for the analysis, an example target was selected from the critical location set for use in a detailed parametric study. The example target was chosen because of its importance to operation of emergency systems and because the time required to gain access to and disable it is short compared to the access and sabotage times for other locations. This latter fact implies that an attack on the example target puts a greater stress on the physical protection system than would attacks on other vital areas.

Configuration 1 -- The configuration 1 safeguards system design is based on the requirements of existing and proposed regulations for power reactor protection. The system represents an interpretation of applicable guidance[9] and does not necessarily represent a design that would be acceptable to the NRC. The basic requirement is to provide at least two access-controlled barriers around every vital area. The perimeter fence is used as one of the required barriers and is provided with intrusion detection in the form of an alarm system and periodic surveillance (see Appendix D). The probability of detection for the perimeter alarm system was 0.5 for the simulation runs. A closed circuit TV (CCTV) system in the proposed design provides additional detection capability in the protected area. The effects of variation of alarm system probability of detection are discussed below and in Appendix G.

The requirement for a second barrier was satisfied in two different system designs. First, access control was applied at all exterior doors to the buildings containing vital areas (configuration 1a). Second, access control was applied at the doors that open directly into each vital area (configuration 1b); that is, the barrier closest to each vital area was locked and alarmed. In some instances exterior doors open directly into vital areas so that the access controlled doors are the same for both configurations. The second barrier for vital equipment located outside the buildings necessitates the addition of an access-controlled structure around the equipment. Probability of detection for the door alarm systems was 0.97.

Figure 4.4 illustrates the attack sequence along the shortest path to the example target location for configurations 1a and 1b. Mean values of penetration, transit and sabotage times are shown along with detection probabilities at the alarmed barriers. The estimated P_{SI} from FESEM was 0.8 for configuration 1a and 0.51 for configuration 1b.

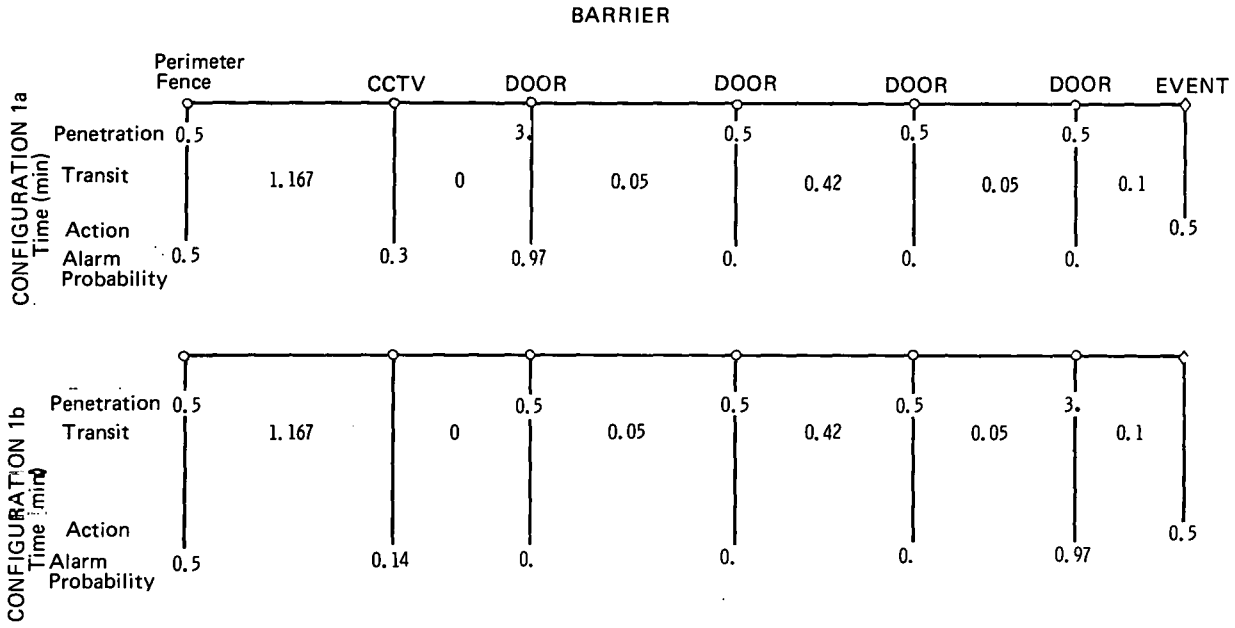


Figure 4.4 Schematic Diagram for the Shortest-Time Path to an Example Target Location for Configurations 1a and 1b

Configuration 2 -- The configuration 2 safeguards system provides two access-controlled barriers for all vital areas as required by the regulations and adds an additional barrier around each critical location. Again, the perimeter fence forms the first barrier. The second barrier is provided by using access control measures at all exterior doors to buildings containing vital areas (as in configuration 1a) and the third by using access control at the doors into the critical locations.* The value for probability of detection at the perimeter fence was 0.5 and at alarmed doors 0.97, the same as those used in the system for configuration 1.

Figure 4.5 illustrates the attack sequence along the shortest-time path to the target location for configuration 2.** The P_{SI} for this sequence was 0.96.

Configuration 3 -- The safeguards system for configuration 3 is the same as for configuration 2 except that the sabotage acts which lead to long-term transient incidents are countered by damage control rather than by physical protection. No vital area or critical location physical

*It is not necessary to provide a third physically separate barrier around the critical location if the penetration time and probability of detection through the walls of the structure are at least as great as the penetration time and probability of detection through two levels of access control at the normal access points. Thus, an additional barrier was not supplied around the heavily reinforced concrete reactor building, but at least two locked and alarmed doors must be penetrated to gain access to it.

**This sequence is the same for configuration 3. Damage control in this analysis merely eliminates the need for protection of some of the other critical locations and thus effects the cost of the system.

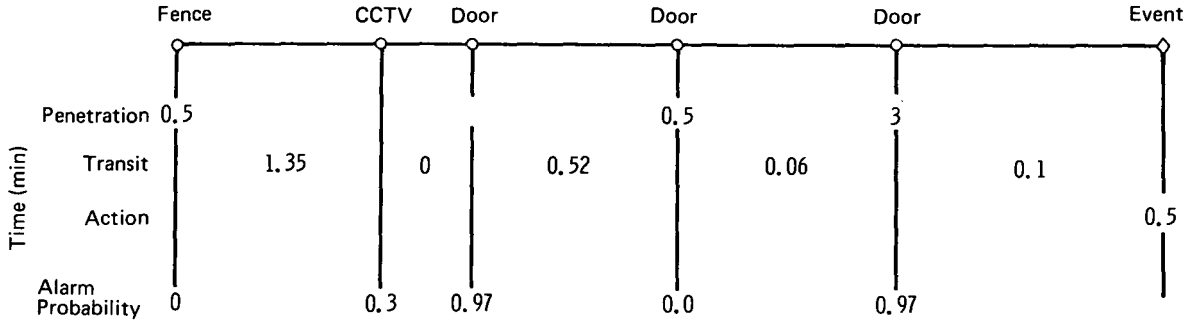


Figure 4.5 Schematic Diagram for Shortest-Time Path to the Target Location for Configuration 2 or 3

protection measures are provided for equipment whose destruction contributes only to long-term transients. If damage control measures are at least as effective in nullifying long-term transients as physical protection measures are in preventing access to the equipment involved, then configuration 3 provides an overall probability of sequence interruption as high as that for configuration 2 at a potentially lower cost.* The P_{SI} for the critical locations in configuration 3 was the same as for configuration 2 (for the example target location the value was 0.96).

Comparison of the Alternative System Configurations -- Table 4.2 summarizes the result of the effectiveness evaluation (in terms of P_{SI} for the example target) for the three safeguards system configurations. With the system characteristics assumed for the simulations, configuration 3 appears to offer the most cost-effective approach to safeguarding the plant. Further analyses performed on these configurations show the variation in effectiveness with changes in system characteristics such as alarm probability (see Appendix G). For example, the addition of a high (0.9) probability of detection perimeter alarm system raises the P_{SI} for configurations 1a and 1b substantially and reduces the apparent advantage of configuration 3. But the potential cost savings make the use of damage control a very attractive option particularly for existing plants where physical protection for some critical locations may be impractical. Thus, configuration 3 was used as the baseline configuration for the detailed system performance studies discussed in the following section.

*The nature and effectiveness of damage control measures require further study for quantification. The cost of damage control equipment, system modifications, and training offset at least some of the savings in physical protection system costs.

TABLE 4.2

Comparison of System Configuration Effectiveness

Configuration	Physical Protection Requirements	Probability of Sequence Interruption
1a	All vital areas	0.80
1b	All vital areas	0.51
2	All vital areas plus added protection for 15 critical locations	0.96
3	All vital areas plus added protection for 11 critical locations	0.96

4.2 Parameter Variation Studies

The sensitivity of P_{SI} to changes in the configuration 3 safeguards system characteristics was evaluated to guide the development of an example system for the plant. Alarm system performance and composition, barrier delay times, on-and-off site response force characteristics and communications reliability were examined in the evaluations. The results of the parameter variation studies are summarized below.

4.2.1 Alarm Systems

Intrusion alarms form an important part of the physical protection system. The configuration 3 system has alarms with high probability of detection (0.97) on exterior and selected interior doors. Studies were made of the variation in P_{SI} with changes in door alarm detection probability and of the relative importance of perimeter and door alarm systems.

The sensitivity of P_{SI} to the probability of detection of the perimeter alarm system and the interdependence of perimeter and building alarms are illustrated in Figure 4.6. The points on the ordinate show the variation with door alarm probability when there is no fence alarm system. P_{SI} drops from about 0.95 for the baseline case to about 0.4 with the door alarm reduced to a low value (0.1) as might be the case if the alarm could be defeated.

With high (0.97) probability of detection of the door alarms, increasing the perimeter alarm probability does not significantly improve P_{SI}, but it makes a dramatic improvement in system performance if the door alarms function in the medium to low range. One might conclude that a high door alarm probability is sufficient for intrusion detection in the physical protection system. However, another factor should be considered, namely, the locations at which engagements between adversary and response forces occur. Because both forces are armed and pitched battles are assumed probable, it is desirable that engagements occur outside of buildings to prevent collateral damage. The effect of the perimeter alarm on the location of engagements is illustrated in Figure 4.7. With only CCTV surveillance and no perimeter alarm, less than 30 percent of the engagements occur outside of buildings, but with a high alarm probability at the fence, practically all of them do.

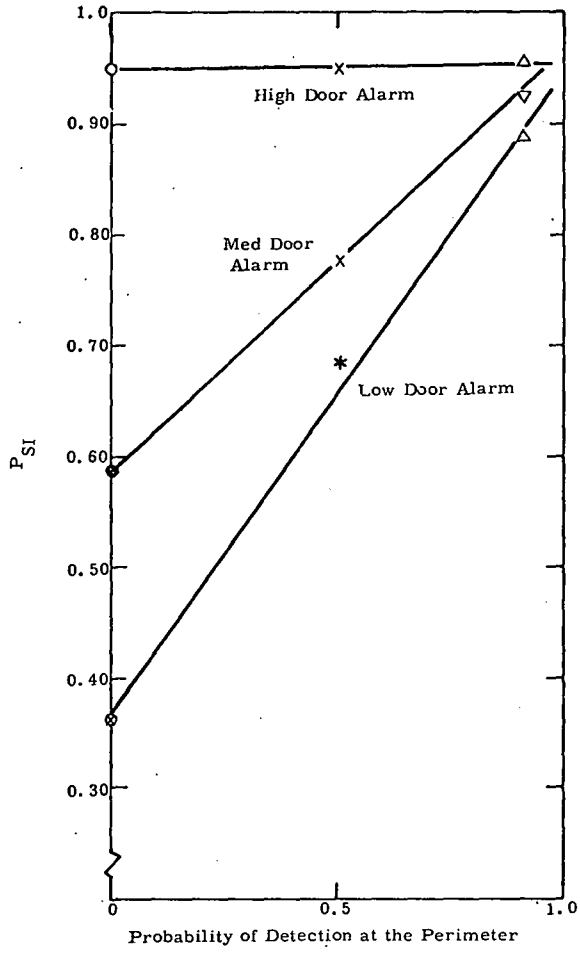
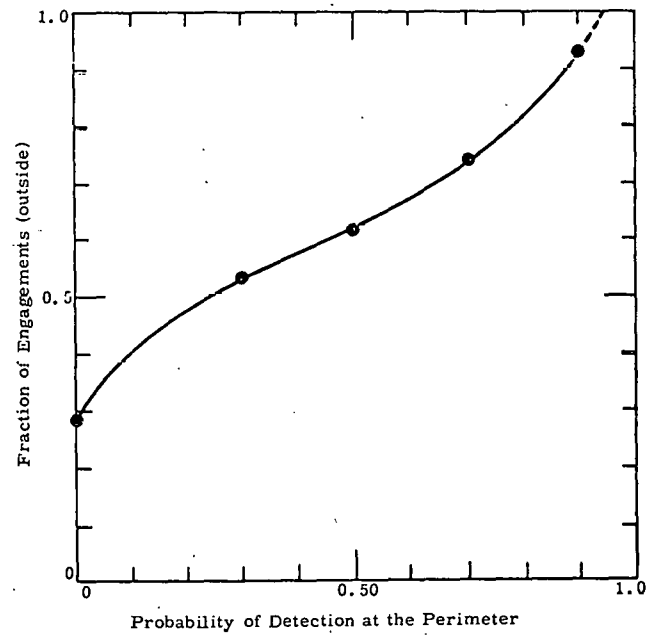


Figure 4.6 Sensitivity of Overall System Performance to Changes in Probability of Detection at the Plant Perimeter

Figure 4.7 Variation in the Location of Engagements with Changes in Probability of Detection at the Plant Perimeter



4.2.2 Barrier Delay

Barrier delay times are difficult to estimate and will vary widely with the abilities and resources of the adversary as well as with the condition of the plant. The sensitivity of P_{SI} to changes in barrier delay is illustrated in Figure 4.8. Clearly, if the barrier delay is not at least as long as the guard response time (2 minutes for the model), P_{SI} is adversely affected. A similar condition holds for the fraction of engagements that occur outside, but the fraction depends more heavily upon the probability of detection at the fence (or by surveillance) than upon delay.

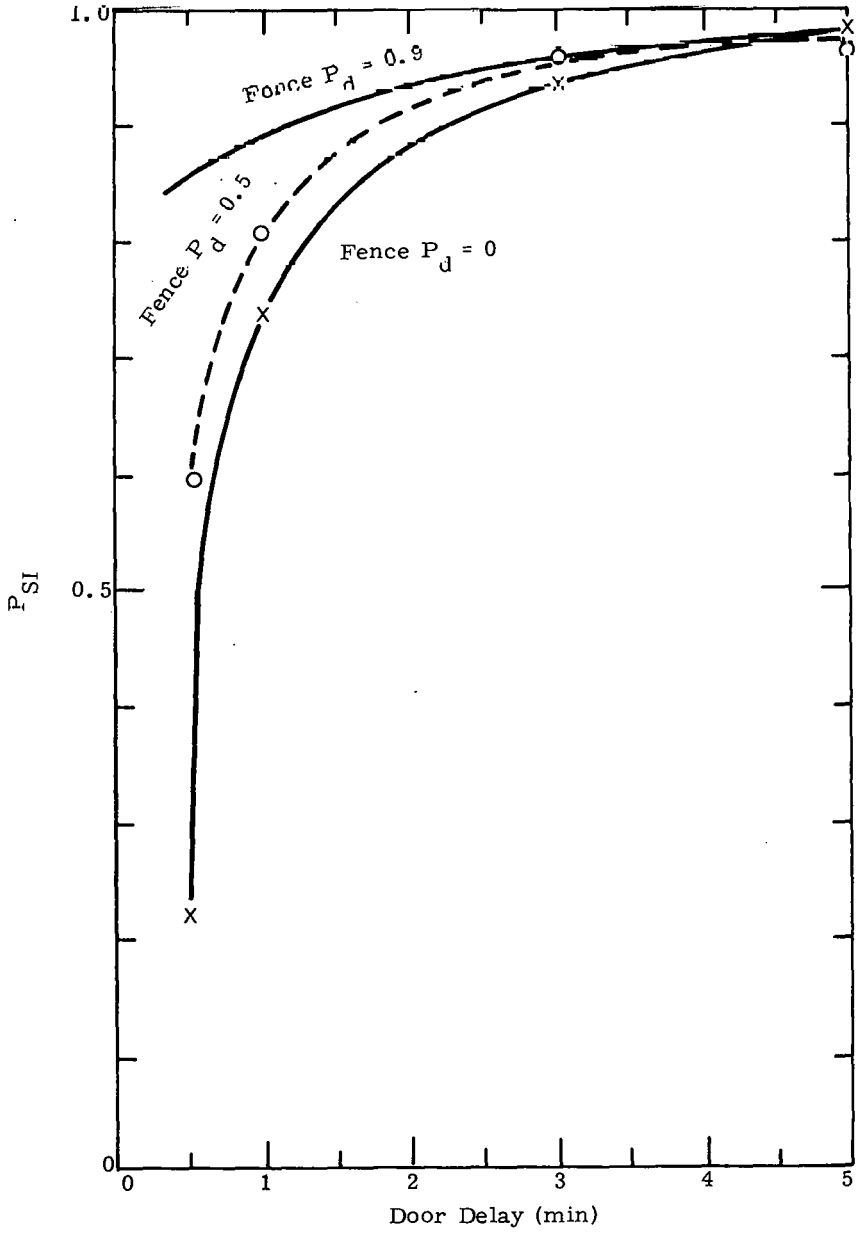


Figure 4.8 Sensitivity of Overall System Performance to Changes in Penetration Time for Locked Steel Doors

4.2.3 On-Site Response Force

Several characteristics of the on-site response force were examined including response time, number of guards, arrival rate, and motivation. The results of these analyses are given in Appendix G.

4.2.4 Communications

Reliable communications between the security control center and the on-site guards and between the plant and the off-site response force are essential. Figure 4.9 illustrates the dependence of P_{SI} on the communications probabilities.

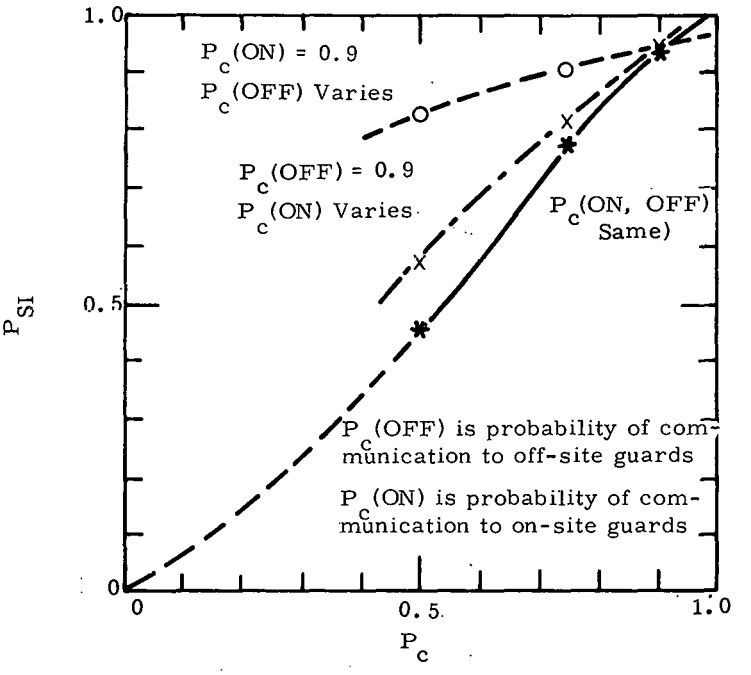


Figure 4.9 Sensitivity of Overall System Performance to Changes in Communications Probabilities

4.2.5 Off-Site Response Force

The off-site response force, made up of local law enforcement officers or off-duty guards, supplements the on-site force and constitutes the final line of defense for the plant. With the baseline system, P_{SI} was not very sensitive to changes in the response time of the off-site force. Doubling the off-site response time reduced P_{SI} by about 10 percent. Thus, time of arrival of the off-site force is not critical, given the assumed size of the on-site and adversary forces.

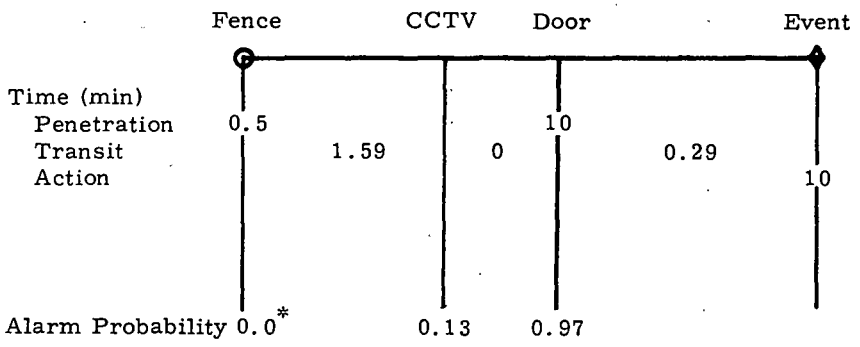
Personnel costs are a major part of the cost of the physical protection system (see Appendix D). It would be economically attractive to reduce the number of on-site guards and rely on local law enforcement agencies to provide the needed manpower. We examined this option by reducing the on-site force and varying the response times and numbers of the off-site forces. The results indicate that on-site guards can be traded for off-site guards under certain conditions. The response time of the off-site force must be comparable to the penetration time from the boundary to the target area. This implies an off-site force located near the plant that can respond in a matter of minutes. A perimeter alarm system is even more important if off-site forces are to carry the major responsibility for site defense; a prompt call for assistance as soon as an attack begins is critical.

Off-site forces are subject to unexpected delays. The adversary could disrupt communications, eliminate bridges in the approach route, or ambush the off-site force along the way. It is unlikely that local law enforcement agencies could supply the required manpower in a timely fashion to some power reactor plants in rural locations. Thus, the main responsibility for response to adversary actions must remain with the on-site force.

4.2.6 Evaluation of Other Critical Locations

The critical locations considered in the parameter variation studies are within the main reactor/generator structure. There are locations of interest within the outside, special-purpose buildings (diesel generator building and pump structure) which may be more representative of vital areas in other facilities. These special-purpose buildings differ from the main structure in that they are closer to the boundary of the plant, they have massive, watertight doors instead of standard steel ones, and they have only a single barrier (excluding the perimeter fence) surrounding the equipment of interest instead of two or more. The path to a special-purpose building without a third barrier added is illustrated in Figure 4.10. The penetration time for the watertight door was estimated to be 10 minutes. The probability of detection by the CCTV system is lower because the adversary would be in exposed areas for shorter periods of time on paths to the special-purpose buildings. The doors which lead into the buildings are not visible with the CCTV system in the baseline model.

The results for the pump structure and diesel generator building are compared with those for the main building locations in Figure 4.11. The special-purpose buildings are more vulnerable to attack and depend more heavily upon a perimeter alarm system for protection. The increased barrier delay time does not compensate for a lower detection probability.



*Varied during analysis 0/.5/.9

Figure 4.10 Schematic Diagram for the Shortest-Time Path to a Special Purpose Building

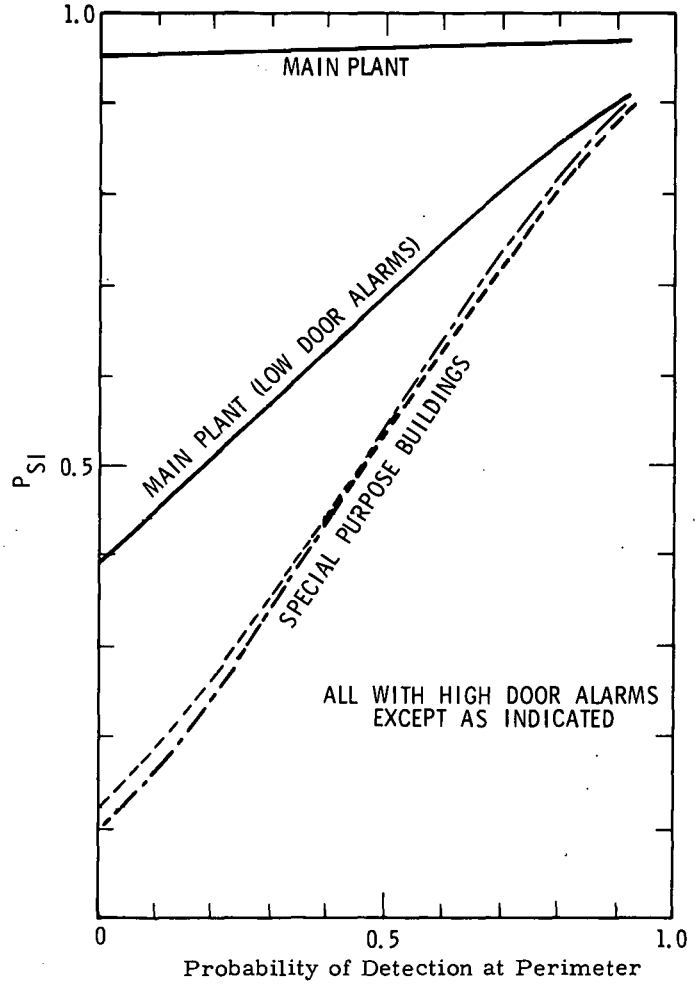


Figure 4.11 Comparison of P_{SI} for Special Purpose Buildings with that of the Main Building

4.2.7 Air Attack

Several air attack possibilities are discussed in Appendix G. Landing a helicopter on the roof of the reactor building could be a credible act if the target were on the refueling floor (top floor of the reactor building). However, paths from the roof to the other vital locations require as many locked door penetrations as do paths from the boundary. The advantage of the air attack for most locations is that it eliminates direct penetration of the perimeter barrier (a small time gain) and may eliminate detection at the boundary if the craft would fly in and land (on the roof or in the yard) without being observed. Simulation runs to check the effects of these variations in paths to the vital locations indicated that P_{SI} is not significantly reduced for the air attack.

4.2.8 Theft

The problem of theft of nuclear material from power reactors is discussed in Appendix A. From the possible theft scenarios, one was selected for limited analysis to see whether any unique problems might be uncovered. We postulated that the objective of theft would be new fuel elements and that the attempt would occur while the fuel was still loaded on the truck that brought it on-site. The truck was assumed to be parked in the reactor building ready for unloading. For the baseline model, the P_{SI} was about 0.95, even assuming the time required to get the truck started, and off-site was as short as 5 minutes. Perimeter alarms were effective in offsetting low door alarms and in forcing engagements to occur outside the building as was the case for sabotage. For an external threat, theft does not appear to pose any more severe problems for the safeguards system than does sabotage.

4.2.9 Summary of the Assessment Results

Two primary kinds of results were obtained from the analyses discussed in this section: comparison of the alternative safeguards system configurations and identification of key safeguards system parameters. Given the constraints and assumptions used in the models, the general results of the comparison of system configurations are essentially those one would expect, based on intuition. The point of the exercise is that some (at least crude) quantification of overall system performance is possible to support intuition. A method of decomposing a portion of the safeguards analysis into damage control and physical protection components has been demonstrated. In the future it may be possible to estimate realistically the effectiveness of damage control mechanisms in an analysis equivalent to the simulation model used for physical protection system evaluation instead of assuming that damage control is totally effective at zero cost against all long-term transient incidents.

Within the constraints of the model assumptions, configuration 3 was judged to offer the best potential performance/cost trade-off. This configuration, which was used as the basis for development of the example system designs, (1) provides physical protection for all vital areas consistent with existing and proposed regulatory requirements, (2) adds an additional level of

physical protection for the eight locations* whose protection will prevent induced LOCA incidents and provide mitigating systems to recover from short-term transients, and (3) relies on damage control to counter long-term transient incidents.

The following general observations are based on the results of the parameter variation studies:

1. Perimeter and exterior door alarm systems provide complementary functions. A high probability of detection at the door compensates in total probability of adversary defeat for a low perimeter alarm probability and vice versa. However, a high perimeter alarm probability is necessary if the adversary is to be confronted by the guard force prior to entry into the buildings.
2. Barrier delay times should be at least as long as guard response times.
3. Rapid response by even a small number of guards (assuming the guards can ambush the adversary force) is very important. Dispersal of the response force over the plant area with a reliable communications system could reduce the response time to alarmed positions and thus be a more effective configuration than that of locating all of the response force at a single location.
4. The off-site response force contributes significantly to the P_{SI} only if (a) the on-site force is badly outnumbered and (b) the off-site force can respond within the barrier delay time. For many rural facilities it may be very difficult to arrange for short off-site response time, indicating that an adequate on-site force is imperative.
5. Theft sequences at a power reactor are generally less difficult to interrupt than are sabotage sequences because additional time is required to load the large fuel assemblies and escape.

The results of the system evaluations were used along with information on the performance of currently available system components to develop example safeguards systems for a typical reactor. This is discussed in the next section.

4.3 Example System Configuration

Based on the results of the alternative system configuration evaluations and the parameter variation studies discussed in the previous section, an example safeguards system was proposed for a typical LWR plant. Configuration 3 was used as the basis for the example system design. We arbitrarily established as a design objective a probability of sequence interruption of greater

*The number and position of critical locations will vary from plant to plant.

than 0.9 for forcible attacks against the critical locations of a typical plant by a group of outsiders along minimum time paths. The component and subsystem performance characteristics required to meet this objective were determined from the results of the parameter variation studies. Subsystems and components with the required performance characteristics as determined by test and evaluation in related studies were selected for use in the example system. Options for implementation of the system configuration were considered and associated costs (capital and annual) were computed. This section discusses an example system which meets the design objective and possible modifications to that system which would improve performance or provide interruptive mechanisms for a broader range of adversary actions.

4.3.1 Baseline Example System Description

The system is intended to meet existing and proposed regulatory guidance as summarized in Appendix D and provide a P_{SI} greater than 0.9. The primary components of the baseline system are:

1. Perimeter fence. The perimeter fence is a standard 2.5 meter high chain link fence topped with barbed wire. Penetration time is estimated as 30 seconds.

2. Perimeter alarm system. A fence-mounted vibration or strain sensing system is used for the perimeter alarm. The probability of detection for the system is assumed to be 0.5.

3. Exterior doors. All exterior doors to the main building, the diesel generator building, and the pump structure are locked and alarmed. The doors are all-steel with no viewing port. Estimated penetration time is 3 minutes.

4. Interior doors. Doors into vital locations are locked and alarmed and are of all steel construction. Estimated penetration time is 3 minutes.

5. Door intrusion alarms. The alarms on all exterior and interior alarmed doors are magnetic switch, self-checking, and tamper-indicating systems. All alarms annunciate in the security control station and one other place with an indication of the location of the alarm. Probability of detection if the door is opened is assumed to be 0.97.

6. Guard force. The guard force consists of seven men on day shift, five for other shifts. It is assumed that the guards are armed and trained in the use of arms and that they will use lethal force, if necessary, to stop an adversary attack. Four of the guards are available for response to adversary actions.

7. External surveillance. Closed circuit TV (CCTV) is used for surveillance of the plant area outside buildings. A random scan pattern is used to achieve coverage of the perimeter with a minimum number of cameras. Based on the distances from the perimeter to the buildings, the scan rate of the cameras, and the door delay time, the probability of detection for CCTV surveillance is estimated to be approximately 0.3.

8. Hardened control room. The control room is a bullet-resistant structure with locked doors and positive access control.

9. Security control station. The main security control station is a bullet-resistant structure not visible from off-site. The intrusion alarm indicators and surveillance viewing screens are in this room. The security control station is assumed to be located so that two guards could reach any exterior door within 2 minutes of an alarm. Possible locations for the station were identified both inside and outside of the main building.

10. Off-site response force. Based on the manpower available from local law enforcement agencies, the off-site response is assumed to be one man in 15 minutes, one man in 30 minutes, 20 men in 60 minutes, and 30 men in 120 minutes. Two separate means of communication with the off-site response are available.

11. Damage control measures. Damage control procedures and equipment were assumed to be capable of providing sufficient cooling to nullify long-term transient incidents.

Appendix H contains a brief discussion of the performance characteristics of currently available safeguards system components and subsystems. Appendix D presents the rationale used in selecting example system components and provides cost estimate details for an example system and several alternates. The performance and cost data for the example system are summarized below.

The P_{SI} for the shortest-time sequence to each of the critical locations was determined for the example system. The mean value and standard deviation of P_{SI} as a function of perimeter alarm probability is given in Figure 4.12. The data for all the critical locations are grouped in a fairly tight band about the mean. These and other data presented in Appendix G indicate that the conclusions based on the study of the example target location are generally applicable for all vital locations in the main building.

The example system meets the design objective if the door intrusion alarm system functions with the estimated probability of detection of 0.97. As discussed in Appendix H, the balanced magnetic door alarm used in the baseline system is highly reliable if the door is opened; however, the system can be defeated if the door is cut through. With a probability of detection of 0.1 on the doors alarms, as might be the case if the door were cut, the P_{SI} for the baseline system is reduced to 0.68. Several alternate system designs were considered to offset this potential weakness in the door alarm system.

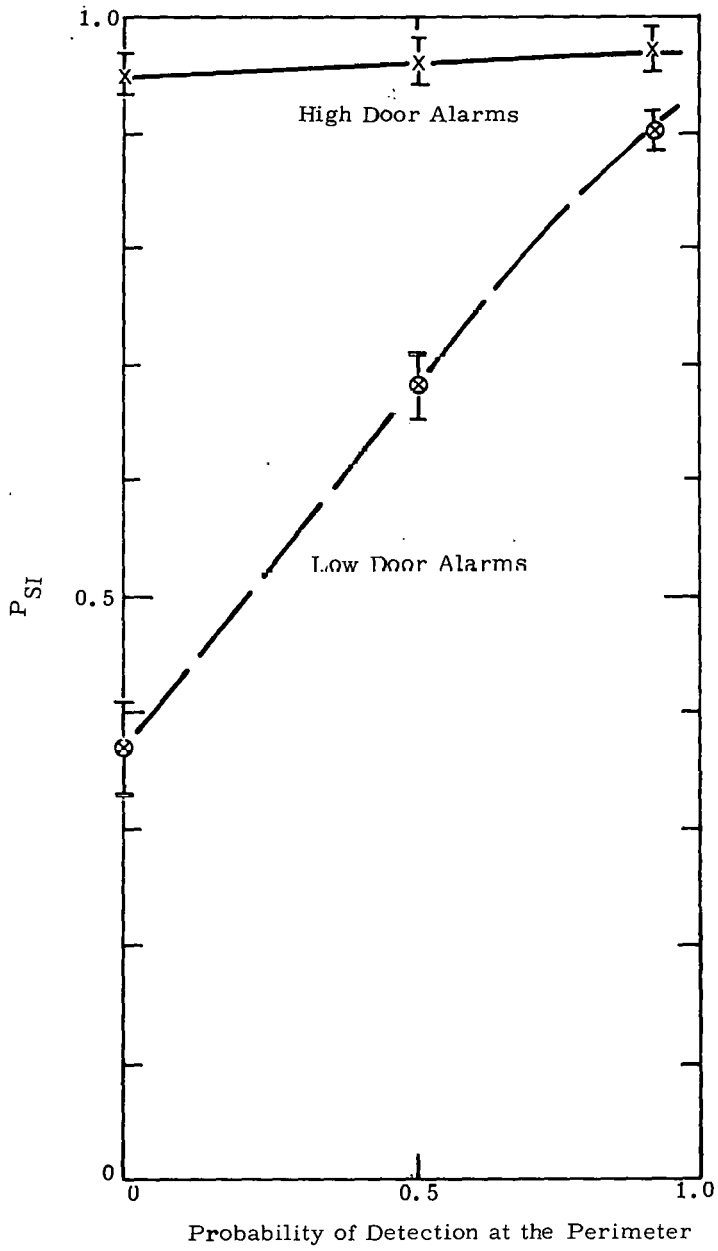


Figure 4.12 Average Values of P_{SI} for the Eight Critical Locations. The bars about the data points indicate standard deviations

4.3.2 Alternate Example Systems

One way to increase confidence in the performance of the door alarm system is to attach a wire grid to each door to detect attempts at direct penetration (cutting through the door). Adding this grid arrangement to all exterior doors and retaining the magnetic switch alarms gives a high degree of confidence that an alarm will sound when a door is penetrated, whether it is opened normally or cut through. The baseline system plus the wire grid addition to the door alarm system is labeled Alternate 1 in Figure 4.13. The total system cost is increased by about 4 percent by this addition and the P_{SI} is 0.95. However, it must be emphasized that with the relatively poor performance of a fence-mounted perimeter alarm system a significant fraction of guard-adversary engagements can occur inside the plant structures.

The parameter variation studies indicated that the probability of detection of the perimeter alarm system has a very significant effect on the fraction of engagements that occurs outside the buildings, and, of course, on overall probability of adversary defeat. The fence-mounted perimeter alarm system used in the baseline system has relatively poor performance when

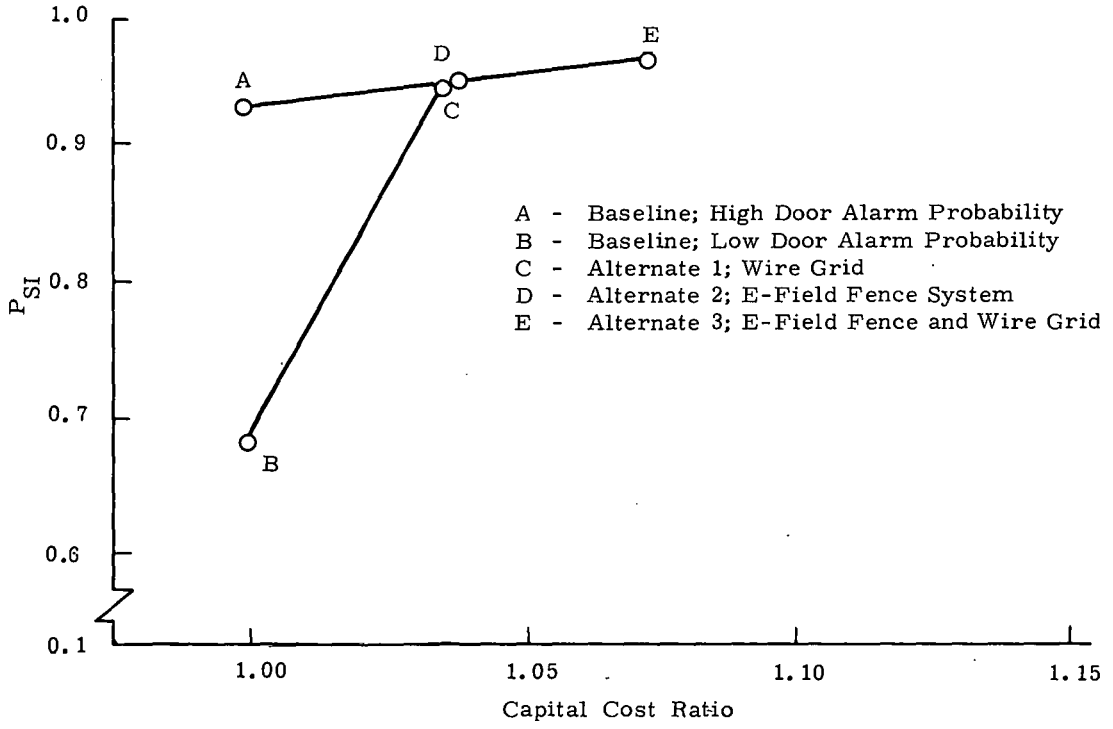


Figure 4.13 Variation in Overall System Performance with Capital Cost Ratio for the Example Systems

compared with certain other perimeter detection schemes (Appendix H). This system was chosen for several reasons: (1) the equipment is now commercially available, (2) there is no regulatory specification on detection probability or certification procedure, and (3) it is presumed that the simplest system would be the most desirable to the licensee. The second alternate example system replaces the fence-mounted system with an E-field sensor system. The E-field sensor is a new approach to perimeter alarm systems that detects disturbances in the electric field around a transmitter-receiver antenna array. By isolating the antenna in the zone between two fences, a probability of detection of approximately 0.9 with a false alarm rate substantially lower than many other systems can be achieved even in adverse weather conditions (see Appendix H). The E-field sensor system plus a second fence would add only about 3.5 percent to the baseline system cost (alternate 2) because the E-field sensor would replace the fence-mounted perimeter alarm system. The performance of this system is comparable to that of alternate 1, but it has the advantages of less electrical installation, less equipment inside the plant proper, and would result in fewer guard-adversary engagements inside buildings.

If the additional security of door alarm on direct penetration or opening is deemed appropriate, the wire grid system may be installed in addition to the two-fence E-field system for a total investment of 7.5 percent above initial cost (alternate 3). As discussed in Appendix H, performance of this system (baseline equipment plus two-fence E-field sensor arrangement, plus door grid alarm) is very good in terms of sequence interruption and location of engagements.

4.3.3 Comparison of Exemplary Systems

Figure 4.13 compares the alternatives discussed in the previous section. The probability of adversary defeat, P_{SI}, is plotted as a function of the capital cost ratio where the capital cost ratio is defined as the capital cost including modifications divided by the baseline exemplary system capital cost. If the door alarms are only marginally effective (particularly if they can be circumvented by cutting through the door instead of opening it), then the 3.5 percent increase in capital costs associated with alternate 1 provides considerable increase in effectiveness. Similar results are evident if the E-field sensor with an additional fence (alternate 2) is selected. Once one has provided perimeter alarms of high quality, additional treatment of the doors (alternate 3) offers only slight improvement in P_{SI}.

CHAPTER 5

RESULTS AND CONCLUSIONS

The general results and conclusions of this study fall into two categories: (1) those related to the methodology for safeguards system effectiveness evaluation, and (2) those related to safeguards system concepts for power reactors. The following sections summarize the main points in these two areas.

5.1 Methodology for Effectiveness Evaluation

5.1.1 Study Results

A general framework for the evaluation of LWR safeguards systems has been developed. This extension of existing capabilities for safeguards system effectiveness evaluation was a major accomplishment of the study. The applicability of the methodology to the development of LWR safeguards system concepts and designs was demonstrated by detailed analysis of the sabotage problem for a typical LWR plant.

A primary contribution of this study to safeguards evaluation technology is the concept of interrupting all adversary sequences which would release radioactive material from a plant by denying access to a selected set of plant locations. A systematic approach was developed for identifying sets of locations whose protection is sufficient to assure that release cannot be initiated. For the typical LWR used in this study, it was found that denying adversary access to eleven locations within the plant and providing damage control measures at four others would assure that the adversary could not complete any of the enormous number of possible combinations of sabotage acts leading to radioactive release.

This study also provided the first application of graph-theoretic path minimization techniques to safeguards problems. The introduction of these mathematical tools into the safeguards research effort and the demonstration of their usefulness in the selection of minimum paths in a large, physically complex power reactor facility represents a significant advancement in the methodology for safeguards system evaluation. Associated with the use of graph-theoretic models was the development of a computer graphics display system as an interactive input-output mechanism. Both the graph-theoretic algorithms and the computer graphics system have great potential for future development of more powerful analytic tools.

5.1.2 Future Refinements

The methodology discussed in this report employs what may be termed "laboratory tools" to accomplish the required analyses. These analytical models are somewhat unwieldy and difficult to use and in most instances require the use of large computer systems. In order for the methodology to be used extensively by licensing reviewers and safeguards system designers, several refinements are necessary. In addition, the methodology must be extended in several areas to address the full spectrum of possible adversary actions and to consider more explicitly the implications of safeguards system performance on public risk.

Because all LWRs have many design features in common, the sabotage fault tree analyses may be significantly simplified and aided by the development of generic fault trees which represent broad classes of reactor design. This approach can remove several existing limitations on the use of fault tree analysis. For example, in addition to being well acquainted with the design and functions of reactor systems, the analyst must have a command of fault tree analysis techniques and Boolean algebra. Also, a relatively large effort (several man months) is required to develop a detailed tree for a specific system and the trees produced by different analysts may differ in content and level of detail included. Generic models could be used to rapidly develop detailed fault trees in a structured, consistent manner and could also prove useful in the study of reactor safety issues.

The vital location analysis could be improved by simplifying the procedures for obtaining the complement of the fault trees. Because of the large size and complexity of the sabotage fault trees for a power reactor, an analyst must go through a rather complicated set of manipulations to reduce and complement the trees. This process should be standardized and, if possible, automated. In addition, better techniques should be developed for selecting the set of locations that must be protected to assure that release of radioactive material does not occur. In this study, the selection was based on minimizing the number of locations which must be protected; however, other factors such as cost or impact on operability or safety could be of greater importance to the analyst. The fault tree analysis codes now in use can sort the results of the fault tree reduction in order of measures (weights) associated with the literals (locations) in the equations. Further research should be conducted to identify appropriate measures and formalize procedures for using these measures in determining minimum protection requirements for reactor plants.

In the area of minimum path analysis, the primary improvement needed is to develop path selection criteria that truly optimize the probability of adversary success instead of simply minimizing a single parameter such as time. The computer graphics display system could be improved by simplifying and standardizing the data acquisition process. The most important step would be to automate the digitization of the plant layout, the node numbering, and node weighting procedures.

The nature and effectiveness of damage control measures should be studied in greater detail. In addition to identifying the sabotage acts which can be nullified or mitigated by damage control, such a study should identify methods of performing damage control tasks, equipment required, and means of realistically estimating effectiveness.

Extensions of the methodology are necessary to overcome conceptual limitations now preventing detailed treatment of such issues as insider malevolent action and the deterrance value of safeguards.

In summary, future development of safeguards system evaluation methodology should stress simplifying the models, formalizing the analytical procedures, and eliminating where possible the requirement for use of large computers. In this way a transferrable, user-oriented package can be developed to assist the regulatory staff and the licensee in assuring that reactor safeguards are adequate. Although it may never be possible to quantify the risk of reactor sabotage, the tools discussed in this report, when improved as discussed in this section, can certainly aid the analyst in making more consistant and supportable decisions regarding the design and evaluation of reactor safeguards systems.

5.2 Safeguards System Concepts

The following conclusions concerning safeguards systems for LWRs are based on the analytical studies discussed in Chapter 4.

5.2.1 System Configuration

For the system configurations considered in the study, the best combination of system effectiveness, cost, and expected impact on operability was achieved in that configuration which used physical protection and damage control measures to provide added protection for the critical locations (configuration 3). In this configuration at least three barriers, two of which provide a significant time delay,* must be penetrated in order to reach the critical locations. A system which provides only two barriers around the vital areas (configuration 1) is much more dependent on a rapid guard response and will therefore require a larger number of on-site guards to achieve a level of effectiveness comparable to configuration 3.

5.2.2 Key Safeguards System Elements

The parameter variation studies provided a basis for comparison of the relative importance of various safeguards system elements. The resulting conclusions are summarized below.

*As discussed in Appendix H, a standard chain link fence does not provide a significant time delay to a forcible attack.

- Early detection of malevolent action is necessary. A perimeter intrusion alarm system which provides a high probability of detection is therefore of primary importance. A high probability of detection at the perimeter reduces significantly the effects of variations in the characteristics of all other system components.

- Barrier delay times should be commensurate with guard response times. This has two possible implications for the size and deployment of the guard force. First, some guards should be available for immediate response to alarms at all times. Second, dispersal of the guards over the site instead of locating them all at a single point may be necessary to assure timely response to all plant areas.

- An assessment system (closed circuit television, for example) which allows the guard force to determine the location and probable objectives of an adversary force can reduce the number of on-site guards required by giving the guards the advantage of surprise.* In the system studied, approximately one-fourth as many guards were required when the guards ambushed the adversaries as when the adversaries had the advantage of ambushing the response force.

- On-site guards are more effective than off-site response forces in countering a forcible attack. Rapid response by even a small number of on-site guards can provide significant delay to adversary progress (if the guards ambush the adversaries).

- The use of damage control measures can potentially reduce the cost of safeguards systems for LWRs by reducing the requirements for physical protection for some plant areas. More study is needed to determine to what extent damage control can offset the need for physical protection at LWRs.

5.2.3 Example System

An example system was proposed using currently available safeguards system components and subsystems (Appendix D). The example system provides a probability, as estimated by the simulation model, greater than 0.9 of interrupting adversary sequences along minimum time paths to the critical locations by an outsider adversary group of four to eight individuals. The initial and annual costs of the example system were each estimated to be approximately one million dollars.

---

*A reliable communications system is also implied.

REFERENCES

1. C. A. Bennett, W. M. Murphey, and T. S. Sherr, Societal Risk Approach to Safeguards Design and Evaluation, ERDA-7, Energy Research and Development Administration, June 1975.

2. Safety and Security of Nuclear Power Reactors to Acts of Sabotage, SAND75-0504, Sandia Laboratories, Albuquerque, New Mexico, March 1976.

3. Physical Protection of Special Nuclear Material in the Commercial Fuel Cycle (U), SAND75-0457, Sandia Laboratories, Albuquerque, New Mexico, March 1976.

4. Physical Protection of Nuclear Materials at Fixed Facilities, FY 76 Program Definition, Sandia Laboratories, Albuquerque, New Mexico, May 1975.

5. Assessment of Domestic Safeguards for Low-Enriched Uranium, INMM Safeguards Committee, Institute of Nuclear Materials Management Seventeenth Annual Meeting, Seattle, Washington, June 1976.

6. H. A. Bethe, "The Necessity of Fission Power," Scientific American, Volume 23, No. 1, Janaury 1976.

7. M. Wilrich and T. B. Taylor, Nuclear Theft: Risks and Safeguards, Ballinger Publishing Company, 1974.

8. The Code of Federal Regulations, Title 10, Energy, Part 73.2, January 1975.

9. The Code of Federal Regulations, Title 10, Energy, Part 73.55 (proposed), Published for Comment November 1974.

10. R. T. Moore, Barrier Penetration Tests, U. S. Dept. of Commerce, National Bureau of Standards, NBS Technical Note 837, June 1974.

11. R. B. Worrell, Set Equation Transformation System (SETS), SLA-73-0028A, Sandia Laboratories, Albuquerque, New Mexico, July 1973.

12. R. B. Worrell, "Using the Set Equation Transformation System in Fault Tree Analysis," in Reliability and Fault Tree Analysis, ed. by R. E. Barlow, J. B. Fussell, and N. D. Singpurwalla, SIAM, Philadelphia, pp. 165-185, 1975.

13. R. B. Worrell and G. R. Burdick, "Qualitative Analysis in Reliability and Safety Studies," IEEE Transactions Reliability, Vol. R-25, No. 3, August 1976.

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

15. B. L. Hulme, Graph Theoretic Models of Theft Problems. I. The Basic Theft Model, SAND75-0595, Sandia Laboratories, Albuquerque, New Mexico, November 1975.

16. B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models. I. Simultaneous Attack by Several Teams, SAND76-0314, Sandia Laboratories, Albuquerque, New Mexico, July 1976.

17. M. Bellmore and G. L. Nemhauser, "The Traveling Salesman Problem: A Survey," Operations Res., Vol. 16, pp. 538-558, 1968.

18. E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs," Numer. Math., Vol. 1, pp. 269-271, 1959.

19. N. Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice-Hall, Englewood Cliffs, 1974.

20. J. Y. Yen, "Finding the Lengths of All Shortest Paths in N-Node Nonnegative-Distance Complete Networks Using $(1/2)N^3$ Additions and N^3 Comparisons," J. Assoc, Comput. Mach., Vol. 19, pp. 423-424, 1972

21. T. A. Williams, and G. P. White, "A Note on Yen's Algorithm for Finding the Length of All Shortest Paths in N-Node Nonnegative-Distance Networks," J. Assoc, Comput, Mach., Vol. 20, pp. 389-390, 1973.

22. R. W. Floyd, "Algorithm 97, Shortest Path," Comm. ACM., Vol. 5, p. 345, 1962.

23. L. D. Chapman, Effectiveness Evaluation of Alternative Fixed-Site Safeguard Security Systems, SAND75-6159, Sandia Laboratories, Albuquerque, New Mexico, presented at the 1976 Summer Computer Simulation Conference, July 12-14, 1976, Washington, DC.

24. H. A. Bennett, Dynamic Model of a Terrorist Attack, SAND75-0658, Sandia Laboratories, Albuquerque, New Mexico, February 1976.

25. F. W. Lanchester, Aircraft in Warfare: The Dawn of the Fourth Arm, Constable, London, 1916.

26. P. M. Morse and G. E. Kimball, Methods of Operations Research, John Wiley and Sons, 1971.

APPENDIX A

Theft of Nuclear Material from LWR Plants

Any discussion of the possible threat to the nation or individuals by the theft of radioactive material is speculative. The large amount of discussion in the media of this threat is indicative of the controversy of this issue. Articles such as "Will Terrorists Go Nuclear?", "How Improbable is the Home-made Nuclear Bomb?", and "Can We Protect Ourselves Against Plutonium?" [A.1, A.2, A.3] illustrate the public concern with the potential threats of and to nuclear materials. As our national energy needs bring about the development of more nuclear reactor plants, the use of radioactive materials increases. This appendix discusses the problem of theft of radioactive material from light water reactors.

A.1 Theft Objectives

It is easy to imagine various possibilities for nuclear theft, but it is difficult to distinguish between credible and incredible situations. A recent study by BDM Corporation[A.4] gives a detailed analysis of possible malevolent motives and actions against nuclear facilities. The motives of malefactors mentioned in the BDM report are similar to those summarized in Table A.1. Regardless of the malefactors or motives, the possibility of theft of nuclear material must be considered. Theft of enough nuclear material to make a bomb or a radiological weapon (dispersal device) is of basic concern. Either of these uses, or credible threat of use, could have extensive consequences.

The amount of material required to make a nuclear explosive device depends on many factors including the type of device, the knowledge and skills of the bomb maker, and the equipment and facilities at his disposal. Estimates of the minimum amounts of fissile material needed vary but are generally in the range of a few kilograms. There are many conflicting opinions on how successful an individual or small group could be in producing a nuclear explosive device. A conservative approach is to assume that a crude device could be produced by a group with significant resources and a minimum of a few kilograms of fissile material. Because of the low fissile content of LWR fuels, the amount of material that would have to be stolen to obtain the minimum fissile mass is several hundred kilograms.

TABLE A.1

Motives and Malefactors for Theft of Radioactive Material

Possible Malefactors

- Foreign governments and their agents, acting under orders
- Sub-units of foreign governments and their agents or military forces, acting with or without official sanction
- Individuals or groups engaged in domestic subversive activity: extremists, terrorists
- Criminals -- highly organized, loosely associated, or individual
- Psychopaths, severe neurotics, and psychotics
- Mercenaries
- Disgruntled employees
- Persons who act impulsively or opportunistically

Possible Motives

- International enmity or rivalry
- Sectional or factional enmity, such as civil war, terrorism
- Desire to create panic or interrupt electrical power, either for its own sake or secondary to some other design
- Desire to establish credibility of later threats of repetition, demands for blackmail payments, etc.
- Desire to obtain special nuclear materials for bombs
- Desire to obtain radioactive waste materials for terror, homicide, blackmail, or resale
- Sadistic motivation, merely to cause suffering
- Suicidal/homicidal motivation: to die spectacularly, take other lives at the same time
- Publicity motivation: to get one's name in the papers, or to publicize some specific cause
- Psychotic motivation

Radiological weapons could be produced with much smaller amounts of nuclear material and with materials other than reactor fuels. Plutonium is the most widely recognized hazardous material for use in dispersal devices, but spent fuel or radioactive wastes could also be used. Again, estimates of the amount of material which pose a hazard vary greatly. Dispersal in an aerosol of finely divided particles of a highly toxic material such as plutonium could have significant consequences.

While it is by no means certain what constitutes a hazardous amount of nuclear material, it is clear that such materials are available in sufficient quantity in practically all stages of the fuel cycle. The next section briefly discusses the LWR fuel cycle in order to place the reactor plant in perspective with other fuel cycle facilities.

A.2 The LWR Fuel Cycle

Figure A.1 shows the typical steps in a LWR fuel cycle (with and without plutonium recycle). First, uranium ore is extracted from a mine. This natural uranium presents no potential for making weapons and is only slightly radioactive. The ore is shipped to a mill where it is concentrated into a type of uranium oxide, U_3O_8, called "yellowcake." Yellowcake is shipped to conversion facilities where it is converted to uranium hexafluoride, UF_6, a gas. The uranium hexafluoride is then shipped to a gaseous diffusion enrichment plant where it is enriched to between 2 and 4 percent U^{235}. This concentration of low-enrichment uranium is also too low to make weapons and is only slightly radioactive. The uranium is converted from a fluoride to an oxide before it is made into fuel.

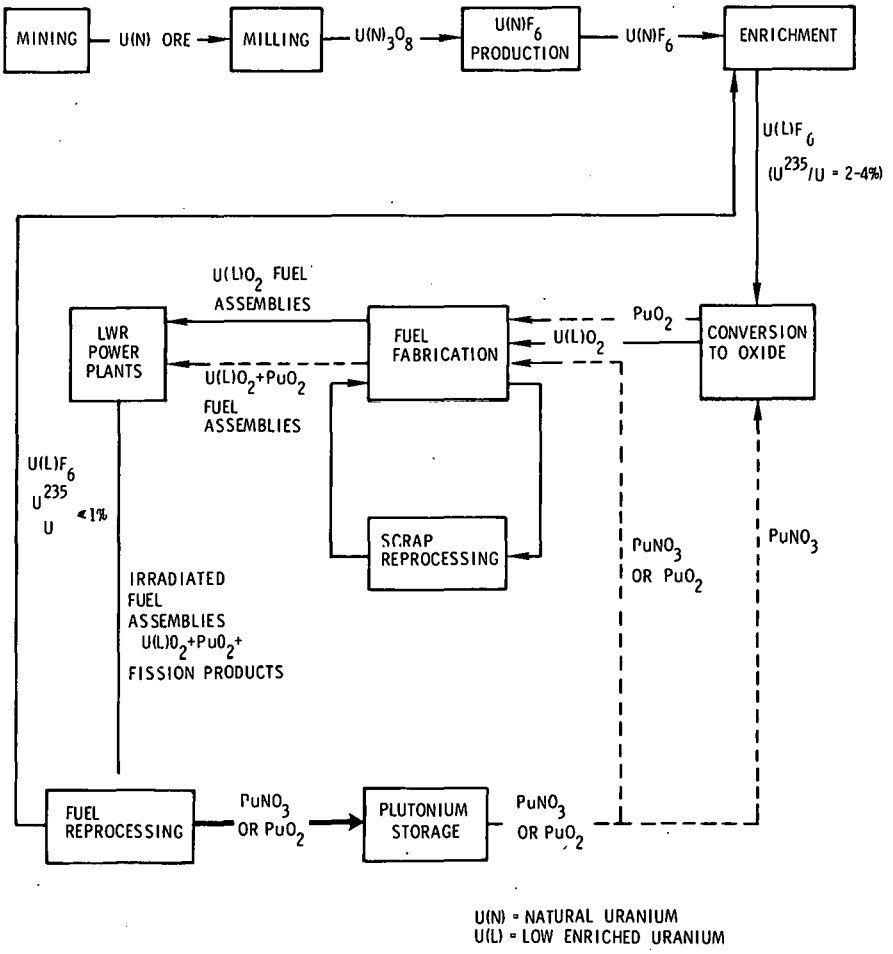


Figure A.1. Light Water Reactor (LWR) Fuel Cycle

At this point in the fuel cycle, the uranium oxide can be made into uranium dioxide fuel pellets or mixed with plutonium oxide and made into "mixed-oxide" fuel pellets. The nuclear fuel currently being used in LWR plants is in the form of uranium dioxide which has been sintered and compacted into pellets approximately 1.25 cm in diameter and 2 cm in length. The pellets are inserted into a zircaloy tube which is welded shut at both ends to form a fuel rod. The rods are bundled together into fuel assemblies. A PWR fuel assembly is made up of about 200 rods and weighs 500 kilograms (1100 pounds). BWR assemblies typically weigh 200 kilograms (440 pounds) and contain about 50 fuel rods.[A.6, A.7]

Fresh fuel is shipped by truck from the fuel fabrication plant to LWR power plants. There are typically two fuel assemblies in each shipping container (see Figures A.2 and A.3). A truckload consists of 16 containers of BWR assemblies or 6 containers of PWR assemblies.[A.7, A.8]

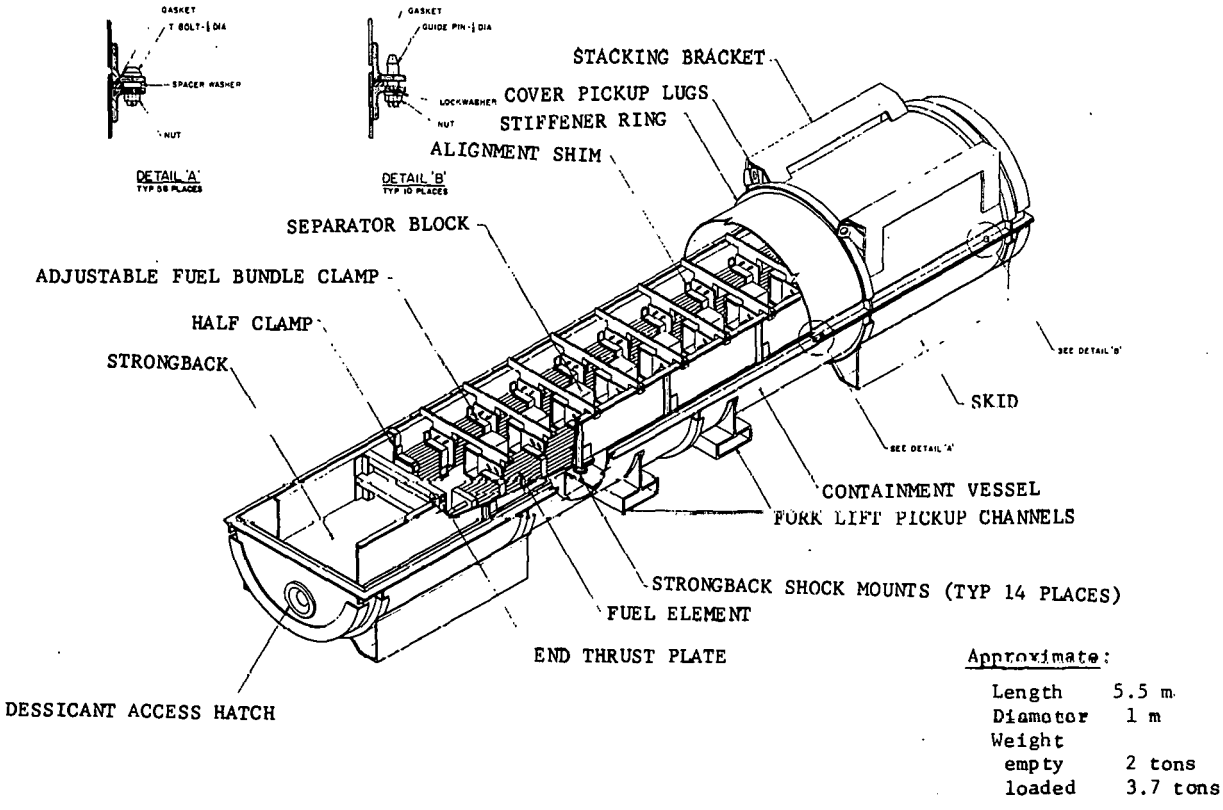
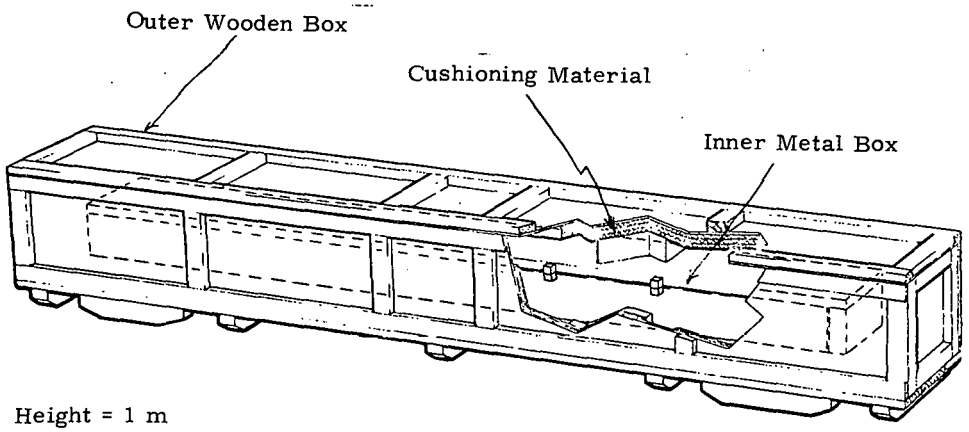


Figure A.2. PWR Fuel Assembly Shipping Container

When the fuel assemblies arrive at an LWR power plant, they are unloaded by crane into the fuel storage area. In PWR plants and some of the newer BWR plants, this area is contained in the fuel handling building (see Figures A.4 and A.5). This building is connected to the reactor building by the fuel transfer tube. In most BWR plants, the fresh fuel is stored on the top floor, called the refueling floor, of the reactor building (see Figure A.6). The reactor building of a



Height = 1 m
Width = 1 m
Length = 5.2 m
Loaded Weight = 1300 kg

Figure A.3. BWR Fuel Assembly Shipping Container

BWR is a four to six story square or circular building that entirely encloses primary containment. At some sites the fresh fuel is stored in the spent fuel pool to save additional handling.

Generally, fresh fuel is received at the reactor 3 or 4 weeks prior to refueling. Reactors are refueled roughly once a year. PWR plants change 20 to 33 percent of the fuel during the refueling cycle which takes between 14 and 21 days depending on the reactor size. From 25 to 33 percent of the fuel is replaced in BWR plants in a 12 to 18 day refueling cycle.[A.9]

After the irradiated or spent fuel is unloaded from the reactor core and replaced with new fuel, the spent fuel is placed under water in a storage pool to allow for radioactive decay and cooling prior to being loaded into a shipping cask for transport to a reprocessing plant. This storage period varies from 90 to 360 days, depending on the policies and economics of the utility. Unlike fresh fuel, spent fuel generally is in storage at LWR plants year round.

After 150 days of cooling, each PWR fuel assembly still contains approximately 2 million curies of radioactivity. A BWR spent fuel assembly contains about 1 million curies.[A.8] Because of this activity, spent fuel requires special shipping casks for transport to a reprocessing facility. Shipping casks for spent fuel must meet regulatory requirements for fissile material and large quantity packages. Radiation shielding of thick steel, lead, or uranium is provided in the cask wall. The cask also must provide a means of dissipating the heat caused by radioactive decay. Water is usually used as a coolant.[A.8, A.10]

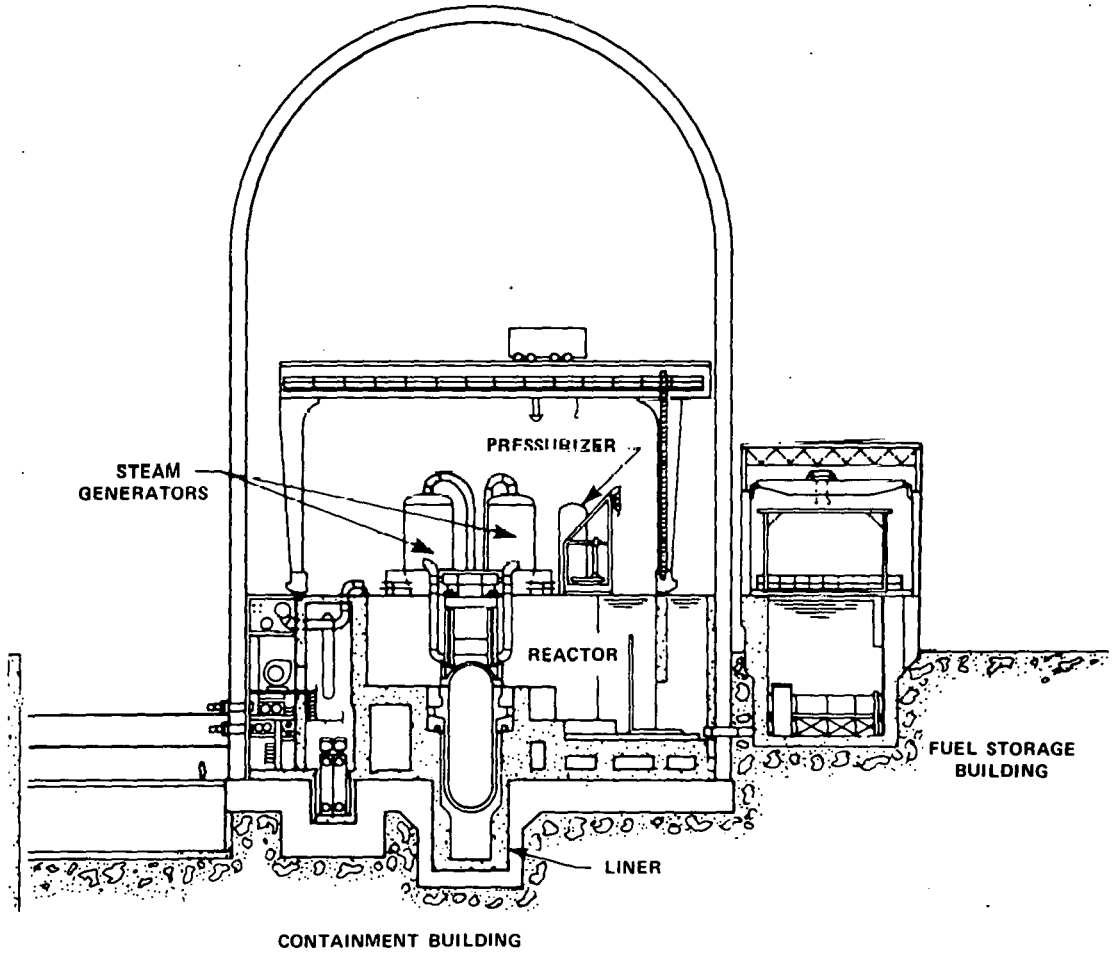


Figure A.4. Cross Section of a Typical PWR Plant

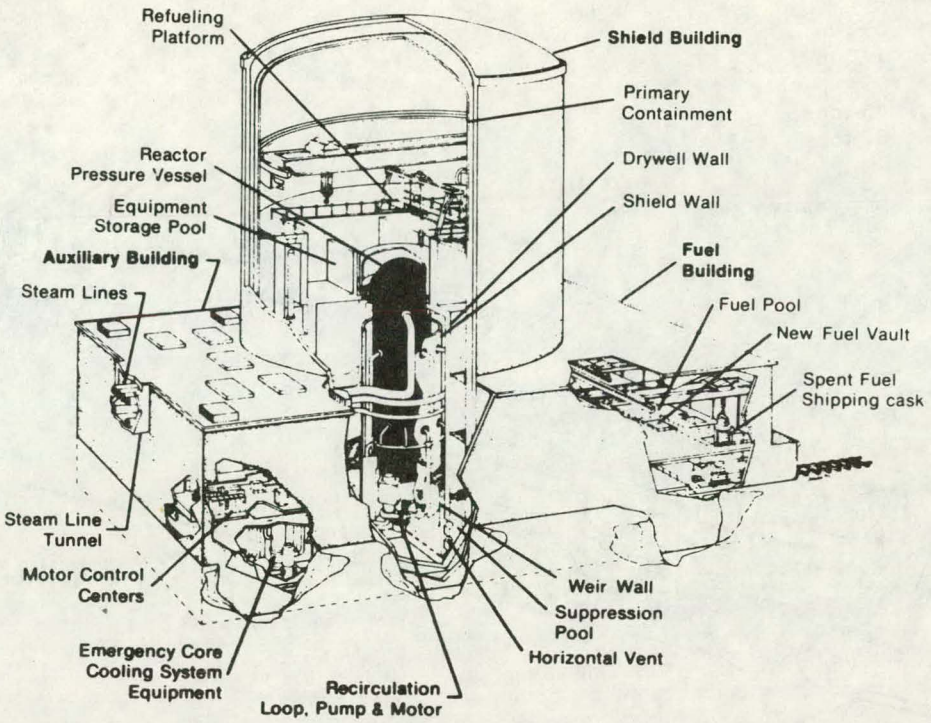


Figure A.5. Mark III Reactor Building, Fuel Building, and Auxiliary Building

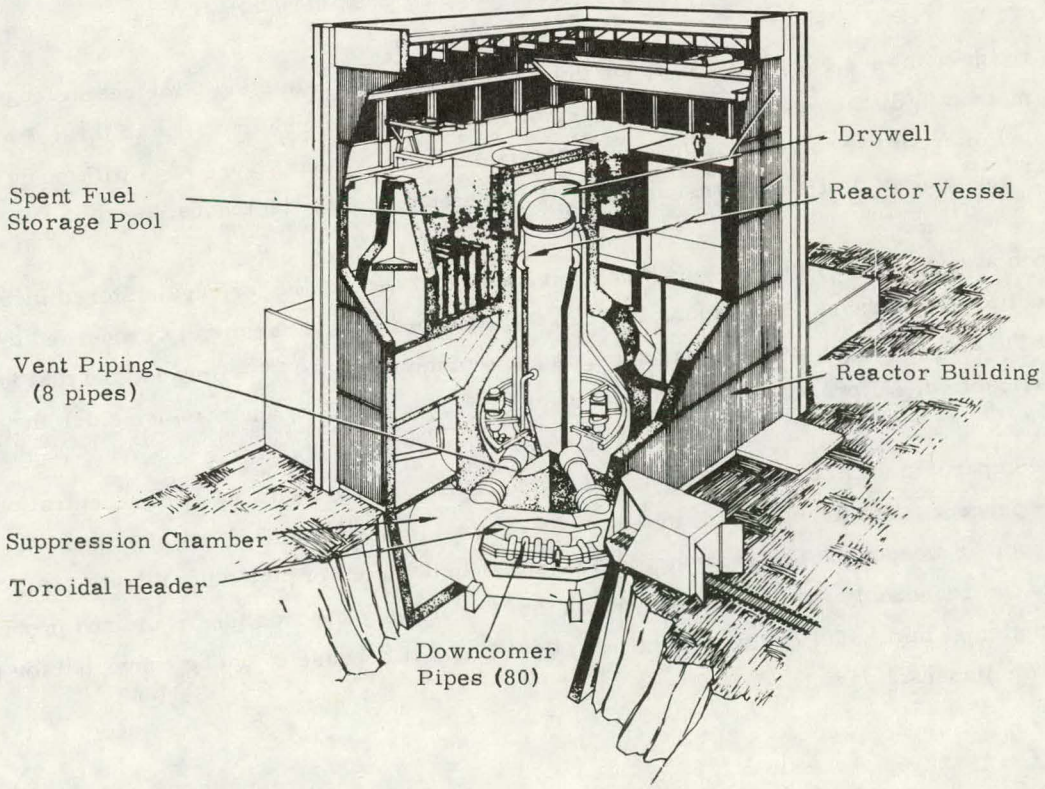


Figure A.6. BWR Reactor Building Cutaway Drawing

Approximate:

Length	5.3 m
Diameter	1.6 m
Weight	
empty	55 tons
loaded	67 tons

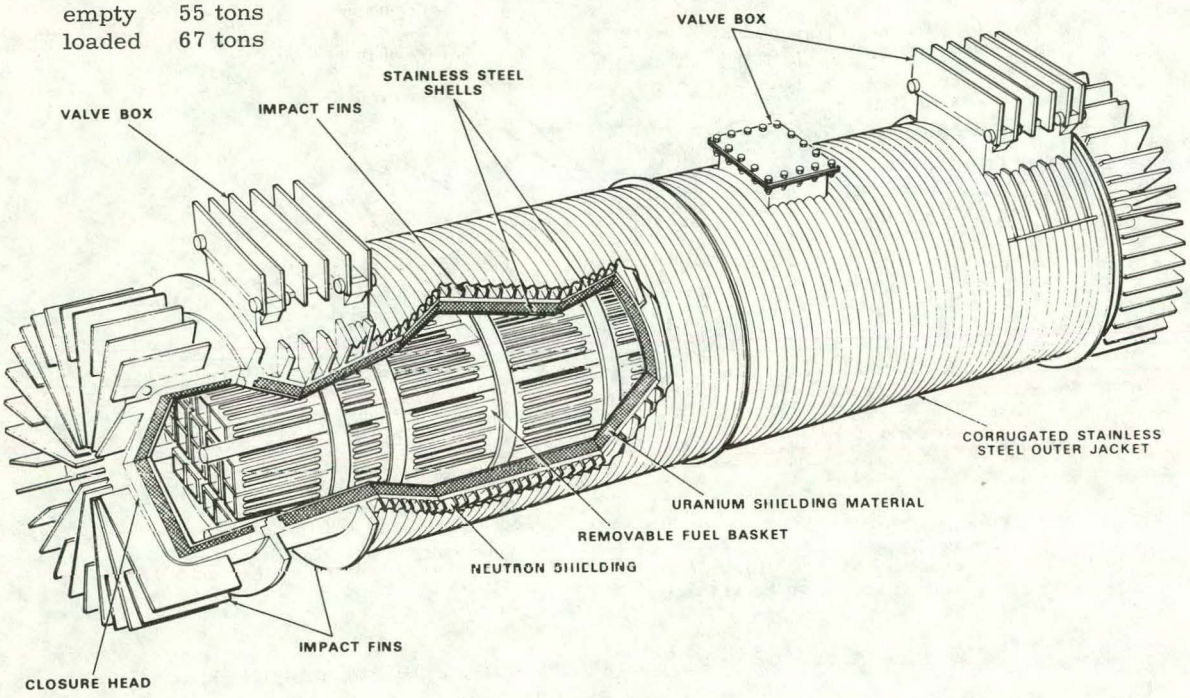


Figure A.7. Spent Fuel Shipping Cask (Truck)

A truck cask (see Figure A.7) is cylindrical in shape, approximately 5 metres in length and 1.5 metres in diameter, and weighs up to 35 tonnes. It will carry from one to three PWR assemblies or from two to seven BWR assemblies. A rail cask (see Figure A.8) will carry up to 7 PWR assemblies or 18 BWR assemblies. It weighs from 70 to 100 tonnes.

Upon arrival at the reprocessing plant, the spent fuel assemblies are again stored in water for an additional 150 days. The assemblies are then chopped up and chemically processed to separate the uranium, plutonium and in some cases neptunium.[A.7, A.11] Because the fuel is highly radioactive, all processing operations require remote handling and massive shielding.

The separated uranium is in the form of uranium hexafluoride with a U^{235} concentration of about one percent. The neptunium in the spent fuel is mainly neptunium-237, which cannot be used to make nuclear weapons. The separated plutonium is in the form of plutonium nitrate solution, a form that is reasonably safe to handle. Plutonium is certainly the most desirable and probably the only material in the fuel cycle of significant theft interest because it can be converted for use in bombs or dispersal devices.

Approximate weight of cask
and shipping assembly:

empty 70 tons
loaded 82 tons

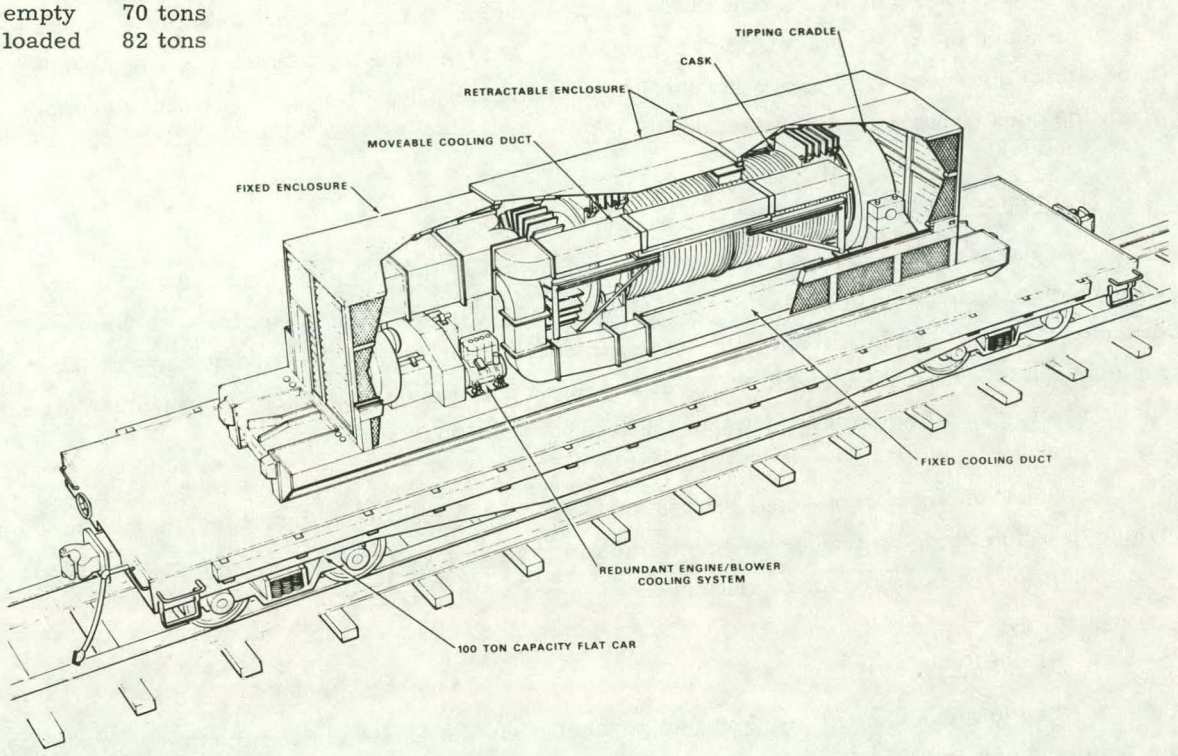


Figure A.8. Spent Fuel Shipping Cask (Rail)

The chemical form of plutonium at the fuel reprocessing site and plutonium storage facilities make them more likely theft targets than is the reactor plant itself. In a recent article on U.S. Energy,[A.12] Manson Benedict, Institute Professor Emeritus, M.I.T., gave the following answer to the question "How likely is plutonium theft?"

> The only places in a nuclear power system where plutonium is pure enough and free enough of radioactivity to make theft a serious risk are plants that reprocess fuel discharged from reactors, and plants that fabricate fuel for reactors.

A.3 Theft Targets at LWR Plants

Nuclear material can be present in several areas of LWR plants: the reactor core, the spent fuel storage pool (SFSP), spent fuel shipping casks, the fresh fuel storage pit, and the radioactive waste system. The vulnerability of these areas or systems to theft and the possible uses of material in them are discussed in the sections which follow.

A.3.1 Reactor Core

Fuel in the core is inaccessible during operation of the reactor. Massive physical barriers surround the core, making theft impossible. During refueling, the fuel is more readily accessible; however, it is highly radioactive and extremely hot. Removal of a fuel assembly from the core is not a credible theft option.

A.3.2 Radioactive Waste System

Gaseous and liquid radioactive wastes are stored in tanks prior to release from the site. Solid wastes such as spent resins are mixed with sand and cement and cast in steel drums. None of these waste materials are suitable for use in nuclear explosive devices, but they could be used for dispersal. The low radioactivity level of radioactive wastes would not significantly endanger public health or safety; however, dispersal may have political impact.

Theft of liquid or gaseous wastes requires transfer of the material from a tank to a container in which it can be transported from the site. Drummed solid waste is easy to handle if transportation off the site can be arranged.

A.3.3 Fresh Fuel

The low-enrichment uranium fuel presently used in LWRs is not suitable for direct use in fission bombs and is only slightly radioactive. The fresh fuel would have to be enriched in the U^{235} isotope in order to make it usable as the core material in a bomb. Only two methods of enriching uranium have been highly developed: gaseous diffusion and gas centrifugation. Gas diffusion requires very large amounts of electric power and large capital investments (hundreds of millions of dollars) in complex equipment and huge facilities. Gas centrifuge systems are extremely complex, but it is generally claimed that the electric power and capital investments are substantially lower than for gaseous diffusion. The present extreme cost and complexity of uranium enrichment probably put it beyond the reach of any but the highly industrialized nations.[A.5] Its low toxicity makes low enriched uranium fuel unsuitable for dispersal. Thus, it seems reasonable to conclude that uranium dioxide fuel is not a likely theft target.

The most attractive theft candidate at a LWR plant would be fresh mixed-oxide fuel assemblies. Several problems need to be considered pertaining to theft of mixed-oxide fuel. Assuming plutonium and uranium oxide powders are mixed uniformly in a ratio of one part plutonium to 150 parts uranium,[A.7] thieves would need to steal about 1500 kilograms (3300 pounds) of mixed-oxide fuel to have enough plutonium oxide to make a crude bomb. The mixed-oxide fuel has much too low a concentration of plutonium to be directly usable in a fission bomb. It would be necessary to extract the plutonium oxide from such a mixture. The processes for plutonium extraction are thoroughly described in unclassified publications[A.7] and are less complicated than those required to reduce plutonium oxide to metallic form. In any case, whenever recycled plutonium is used in fresh LWR fuel, the fuel assemblies contain plutonium that is fairly easy to separate from the uranium.

The weight of the assemblies is a deterrent to theft. In a recent article[A.13] on proposed safeguard measures, Dr. Theodore B. Taylor made the following statement:

> It now appears likely that rather massive gamma-ray and, in some cases, neutron shielding will be required to insure insignificant radiation exposure to workers at all points in the fuel cycle for systems that use recycled plutonium or uranium-233. This would mean that, for reasons not connected with safeguards, heavy containers and barriers will have to be used in the storage, transport, and fabrication of nuclear fuels from the time they are separated at a reprocessing plant to the time they are placed in reactors for refuelling. These barriers and containers will make theft much more difficult.

Another point for consideration is the availability of mixed-oxide fuel at LWR plants. Fresh fuel is on site for a maximum of 6 to 8 weeks per year.

A.3.4 Spent Fuel

Spent fuel can be present in two areas: the SFSP or in spent fuel shipping casks. Spent fuel could be reprocessed to recover the fissile material or could be used directly for dispersal. However, spent fuel presents problems for would-be thieves including the weight of the assemblies and, probably most important, the toxic nature of the material. Spent fuel is dangerous to handle because it emits penetrating gamma rays. Thus, thieves would need heavy shielding to handle the spent fuel. The theft of assemblies already in casks for shipment to reprocessing plants temporarily eliminates the immediate radiation danger but increases the size and weight problem. In addition, spent fuel ready for shipment is on location at the reactor plant for a very limited amount of time.

A third problem is chemical separation. One 500 kilogram PWR spent fuel assembly contains about 2 to 3 kilograms of plutonium.[A.10] However, the plutonium would have to be chemically separated from highly radioactive fission products before it could be used in a bomb or dispersal device. Before uranium, plutonium, and fission products can be separated, the fuel cladding must be removed. The fuel rods have to be chopped into short pieces and dissolved in acid. This solution is then treated chemically by a method known as the Purex process. Since the fuel is highly radioactive, all processing operations require remote handling and massive shielding. Very little information is available on the cost of reprocessing spent fuel.[A.11]

A.4 Theft Attack Modes

Theft of nuclear material from an LWR plant involves gaining access to the site, gaining access to the area in which the material is stored, loading the material for transport, and removing the material from the site. The only materials which are accessible and transportable are fresh fuel, spent fuel, and drummed solid waste. This section discusses ways theft of these materials might be attempted.

Diversion (theft of material by repeatedly and secretly removing small amounts) is not a problem at LWRs. The fuel (fresh and spent) is contained in welded fuel rods which are bundled in fuel assemblies and stored under water or in dry vaults. Spent fuel cannot be handled directly at all because of its high radiation levels. Theft of the fresh fuel pellets would require removing an assembly from its storage location, disassembling it, cutting a fuel rod, removing the pellets, closing the rod, and reassembling and replacing the fuel bundle. This sequence would require a significant amount of time and the use of the fuel handling equipment. The fresh fuel is on-site only a short while before being loaded into the core; therefore, the time available for diversion is limited. Once the refueling operation starts, there are continual operations in the fuel storage area, making unobserved access to the fuel highly improbable. The drummed waste is cast in concrete in large steel drums and is not accessible for small-quantity removal.

The attack modes listed in ERDA-7 are force, stealth, and deceit.[A.14] Stealth does not appear to be a credible theft mode because removal from the site requires vehicular transport* which implies forceful exit or some form of deceit at the exit portal. In addition, it appears unlikely that a thief could operate the fuel handling equipment and load a shipping cask without being noticed.

Deceit might be in the form of forged material movement authorization, concealment of material in an authorized shipment or vehicle, etc. Proper controls on the transportation interface are essential to counter theft by deceit.

Forceful attack seems to be the most credible of these modes. Removal of fuel from the SFSP or fresh fuel storage area is time-consuming, and for spent fuel there is the added problem of packaging the material for movement. Although spent fuel already loaded in shipping casks could be stolen with less difficulty, there is still the problem of handling and transporting the several-tonne weight of the material and container. A heavy transport vehicle would be required to remove a spent fuel cask. The vehicle would have to be brought on-site into the fuel handling area and driven off-site. Simple vehicle access barriers could preclude such attacks.

The fresh fuel presents less of a problem for a thief because it can be handled without shielding or cooling. One assembly weighing 200 to 500 kilograms could be moved in a light truck or even by a small helicopter. The ideal time to attempt theft of fresh fuel may be while it is still on the delivery truck awaiting unloading in the fuel or reactor building. Again, the transportation interface is critical. Helicopter attack by landing on the roof of the fuel handling area is also a possibility.

Theft of drummed waste by forceful means would be a conceptually simple operation. The material is already packaged for transport, so gaining access to the rad-waste area would be the primary problem.

---

*The smallest item of interest is a 55-gallon drum full of concrete.

A.5 Summary and Conclusions

There are nuclear materials at LWR plants which could be of interest to a thief, but these materials are more readily available in other parts of the fuel cycle. Fresh fuel, spent fuel in shipping casks, and drummed solid wastes could be theft targets. The way these materials are packaged and stored essentially eliminates the possibility of diversion at LWRs. The material control function consists of item control on the fuel assemblies and waste containers.

The following measures will reduce the chances of successful theft at LWR Plants.

- Make it impossible to operate fuel handling equipment (overhead crane) except as authorized and supervised.
- Provide vehicle barriers around fuel handling building and waste loading area. These barriers should prevent entry of unauthorized vehicles and unauthorized exit of authorized vehicles.
- Provide a level of physical protection for fresh fuel at least equal to that provided during transportation of the fuel.
- Provide an item control system to continuously account for fuel assemblies and indicate any tampering with the fuel.
- Require positive identity verification and material movement authorization for all shipments.
- Search all vehicles leaving the site for contraband.

A.6 References

A.1 Brian M. Jenkins, "Will Terrorists Go Nuclear?", Testimony given before the Committee of Energy and Diminishing Materials of the California State Assembly, November 19, 1975.

A.2 Lydia Dotto, "How Improbable is the Homemade Nuclear Bomb?", Science Forum, Vol. 7, No. 5, pp. 3-5, October 1974.

A.3 David F. Salisbury, "Can We Protect Ourselves Against Plutonium?", Technology Review, pp. 6-7, December 1975.

A.4 Analysis of the Terrorist Threat to the Commercial Nuclear Industry, The BDM Corporation, BDM/75-176-TR, September 1975.

A.5 D. Krieger, "Nuclear Power: A Trojan Horse for Terrorists," Nuclear Proliferation Problems, Stockholm International Peace Research Institute, The MIT Press, Cambridge, Massachusetts, 1974.

A.6 G. C. Masche, Systems Summary of a Westinghouse Pressurized Water Reactor Nuclear Power Plant, Westinghouse Electric Corporation, 1971.

A.7 M. Willrich and T. B. Taylor, Nuclear Theft: Risks and Safeguards, Ballinger Publishing Company, Cambridge, Massachusetts, 1974.

A.8 Environmental Survey of Transportation of Radioactive Materials to and from Nuclear Power Plants, Directorate of Regulatory Standards, U.S. Atomic Energy Commission, WASH-1238, December 1972.

A.9 Kenneth C. Lish, Nuclear Power Plant Systems and Equipment, Industrial Press Inc., New York, New York, 1972.

A.10 The Threat to Licensed Nuclear Facilities, The Mitre Corporation, MTR-76022, September 1975.

A.11 B. M. Jasani, "Nuclear Fuel Reprocessing Plants," Nuclear Proliferation Problems, Stockholm International Peace Research Institute, The MIT Press, Cambridge, Massachusetts, 1974.

A.12 Manson Benedict, "U.S. Energy: The Plan That Can Work," Technology Review, pp. 52-59, May 1975.

A.13 T. B. Taylor, "Proposed Safeguard Measures to Assure Against Nuclear Theft or Sabotage," Aware, No. 47, August 1974, pp. 3-7.

A.14 C. A. Bennet, W. A. Murphey, and T. S. Sherr, Societal Risk Approach to Safeguards Design and Evaluation, ERDA-7, Energy Research and Development Administration, June 1975.

APPENDIX B

SHORTEST SABOTAGE PATH ALGORITHM

This appendix describes the application of the Dijkstra-Yen algorithm[B.1, B.2] to a simultaneous sabotage problem.

B.1 Algorithm Description

Let G be a simultaneous sabotage graph[B.3] with the hardware nodes numbered from 1 to n_1, the barrier nodes numbered from $n_1 + 1$ to $n_1 + n_2$, and the boundary nodes numbered from $n_1 + n_2 + 1$ to $N = n_1 + n_2 + n_3$. Let $w_i \geq 0$, $1 \leq i \leq N$, denote the node weights and $a_{ij} \geq 0$, $1 \leq i, j \leq N$, the arc weights of G. The node and arc weights are combined to form an N by N "direct distance" matrix D by first halving the barrier node weights

$$w_i \leftarrow w_i/2 \ , \ n_1 + 1 \leq i \leq n_1 + n_2 \ ,$$

and then setting

$$d_{ij} = \begin{cases} w_i + a_{ij} + w_j, \text{ if arc } (i,j) \in G \ , \\ \infty \ , \text{ otherwise, } 1 \leq i, j \leq N \ . \end{cases}$$

Thus, $d_{ij} < \infty$ is the distance between the centers of two adjacent barrier nodes, or the distance from the center of a barrier node all the way through an adjacent hardware or boundary node, etc. In this case, D is symmetric and corresponds to a model in which the node and arc weights do not depend on the direction of travel. When some nodes and/or arcs have different weights for opposite directions, then D is unsymmetric and its construction must take this into account. See Reference B.3 for the details.

For each hardware node $h = 1, 2, \ldots, n_1$, the lengths of the shortest paths from the boundary to h are computed as follows. Hardware node h is given a permanent label of zero, and all other barrier and boundary nodes are given temporary labels of infinity. Permanent labels are the exact lengths of shortest paths from the corresponding nodes to h, while temporary labels are only estimates of this quantity. From the last permanently labeled node i, each temporarily labeled node j is examined. If

$$\text{label}_j > d_{ji} + \text{label}_i$$

then label_j is reduced to $d_{ji} + \text{label}_i$. After all temporarily labeled nodes have been examined, the smallest temporary node label is made permanent since there is no way to reduce it further. In case of a tie, it does not matter which node is made permanent first. This process is repeated from the last permanent node, continuing until a boundary node is permanently labeled. Because nodes are permanently labeled in order of increasing distance from h, this boundary node is a boundary node closest to h.

After checking for any other boundary nodes equally close to h, a supplementary procedure retraces all the shortest path from the boundary to h. At each stage of the retrace, beginning with a permanently labeled boundary node, if j is a permanently labeled node in a shortest path, then every permanently labeled node i adjacent to j is examined. If

$$\text{label}_j = d_{ji} + \text{label}_i ,$$

then the directed arc (j,i) belongs to a shortest path from the boundary to h. The retrace ends when j = h. The set of directed arcs saved during the retrace constitutes a directed subgraph, which contains all the desired paths, and in which every path from a boundary node to h is a desired path.

B.2 References

B.1 E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs," Numer. Math., Vol. 1, pp. 269-271, 1959.

B.2 J. Y. Yen, "Finding the Lengths of All Shortest Paths in N-Node Nonnegative-Distance Complete Networks Using $(1/2)N^3$ Additions and N^3 Comparisons," J. Assoc. Comput. Mach., Vol. 19, pp. 423-424, 1972.

B.3 B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models. I. Simultaneous Attack by Several Teams, SAND76-0314, Sandia Laboratories, Albuquerque, New Mexico, July 1976.

APPENDIX C

COMPUTER GRAPHICS MODEL

This appendix is a brief description of the computer graphics program used to identify and display the critical paths in a facility graph.

C.1 Description

An interactive computer graphics program, SABPTH, has been developed to compute and display the shortest-time paths from the boundary of a facility to any of its vital locations. A facility is described in terms of a graph-theoretic model[C.1] by defining: (1) boundary nodes--possible points of penetration at the perimeter of the site, (2) barrier nodes--possible points of penetration on the building structures (such as doorways and windows), (3) hardware (target) nodes--locations of vital materials or equipment, (4) pseudo-nodes--points which outline obstacles within a region, and (5) stairwell nodes--barrier nodes used in connecting different floor levels of a facility. The analyst needs to provide node weights (estimated penetration time) for the hardware, barrier and boundary nodes and arc weights (transit times) for the stairwell interconnections. All other arc weights are computed.

The internal barriers subdivide a facility into regions. A region is defined as any area within which one can move unimpeded. All node connections within a region are of interest. Each level of a building is composed of one or more regions (see the example in Figure C.1). To display the details of either a level or region, it is necessary to digitize (1) the coordinates of the end points of lines defining the boundaries of each region, (2) the coordinates of the graph nodes (boundary, barrier, and hardware), and (3) the coordinates of pseudo-nodes which outline obstacles within a region. These coordinates are used to compute automatically the arc weights for the graph model.

In each region an auxiliary graph is constructed by connecting every node and pseudo-node by a straight line to every other node and pseudo-node, with the exception of lines that intersect any obstacle in the region. Floyd's algorithm[C.2, C.3] is applied to each auxiliary graph to find the lengths of the shortest paths between each pair of nodes. The construction of the auxiliary graph shows the lengths of routes which go around, not through, obstacles within a region. The distances for shortest physical routes between nodes are divided by an assumed speed to obtain arc weights.

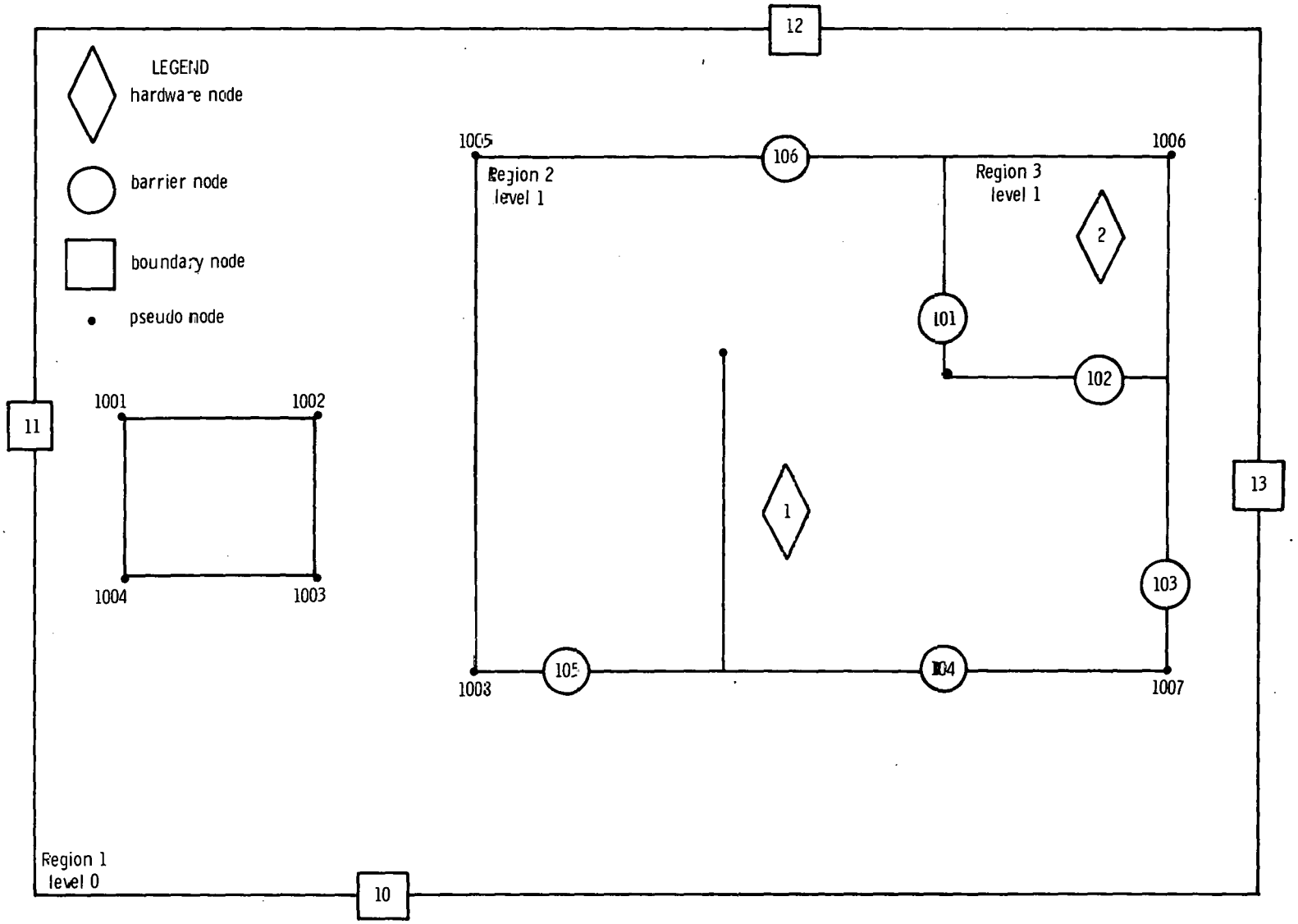


Figure C.1. Example of a Plant Layout as Represented in the Computer Graphics System

After determining the arc weights in each region, the Dijkstra algorithm[C.3, C.4] modified by Yen[C.5, C.6] is used to find the shortest paths from the boundary to each vital area in the facility. These paths can be viewed by the analyst on the computer graphics screen in three ways: (1) the physical path to any particular vital area, level by level, (2) all the path segments on any level of the facility, or (3) all the path segments in any region. The second option enables the analyst to have an overall view of the concentration of path segments and thereby helps to identify areas of the plant where additional barrier delays may be required. The analyst can make reference copies of the paths through the facility on a hard-copy unit connected to the graphics system. The program output provides barrier sequences and delay time information for use in simulation modeling.

Through the interactive capability of the graphics system, the analyst can change node weights, and delete nodes from the initial plot plan. This allows the analyst to determine rapidly the effects on minimum paths of changes in the physical characteristics of a facility.

C.2 References

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

C.2 R. W. Floyd, "Algorithm 97, Shortest Path," Comm. ACM., Vol. 5, p. 345, 1962.

C.3 N. Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice-Hall, Englewood Cliffs, NJ, 1974.

C.4 E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs," Numer. Math., Vol. 1, pp. 269-271, 1959.

C.5 J. Y. Yen, "Finding the Lengths of All Shortest Paths in N-Node Nonnegative-Distance Complete Networks Using $(1/2)N^3$ Additions and N^3 Comparison," J. Assoc. Comput. Mach., Vol. 19, pp. 423-424, 1972.

C.6 T. A. Williams, and G. P. White, "A Note on Yen's Algorithm for Finding the Length of All Shortest Paths in N-Node Nonnegative-Distance Networks," J. Assoc. Comp. Mach., Vol. 20, pp. 389-390, 1973.

DISTRIBUTION:

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

W. H. Immerman (5)
Office of Nuclear Regulatory Research
Operational Support Branch
Washington, DC 20555

Department of Energy
Division of Safeguards and Security
Attn: H. E. Lyon
Washington, DC 20545

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

Los Alamos Scientific Laboratory
Attn: Roy Haarman, WX-8
Los Alamos, NM 87544

International Energy Associates, Ltd.
Attn: Dr. J. Mark Elliott
2600 Virginia Ave. NW
Washington, DC 20037

Dikewood Industries, Inc.
Attn: K. D. Granzow
1009 Bradbury Drive SE
University Research Park
Albuqucrque, NM 87106

Falcon Research and Development
Attn: D. M. Kunsman
2350 Alamo Ave. SE
Albuquerque, NM 87106

1230 W. L. Stevens
1233 R. E. Smith
1700 W. C. Myre
1730 C. H. Mauney
1739 J. D. Williams
1750 J. E. Steigler
1754 J. F. Ney
1758 C. E. Olson
1758 R. B. Worrell
1759 D. L. Mangan
1760 J. Jacobs
1760A M. N. Cravens
1760A J. M. deMontmollin
1761 T. A. Sellers
1761 J. L. Darby
1763 I. G. Waddoups
5120 G. J. Simmons
5122 L. F. Shampine
5122 B. L. Hulme (10)
5300 O. E. Jones
5400 A. W. Snyder
5410 D. J. McCloskey
5412 J. W. Hickman
5414 G. B. Varnado (10)
5414 S. L. Daniel (10)
5414 D. M. Ericson (10)
5430 R. M. Jefferson
5432 R. E. Luna
5700 J. H. Scott
5720 V. L. Dugan
5724 H. A. Bennett (10)
5724 L. D. Chapman
8320 T. S. Gold
8321 R. L. Rinne
8266 E. A. Aas
3141 T. L. Werner (5)
3151 W. L. Garner (3)
For: DOE/TIC
DOE/TIC (25)
(R. P. Campbell, 3172-3)