LA-UR -85-558

CONF-850723--1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W 7405-ENG-36

LA-UR--85-558

DE85 007665

TITLE: VITAL AREAS AT NUCLEAR POWER PLANTS

AUTHOR(S): D. F. Cameron

SUBMITTED TO: 7th International System Safety Conference
San Jose, CA, July 25-28, 1985.

DISCLAIMER

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

DRAFT

Vital Areas at Nuclear Power Plants

D. F. Cameron, PE; Los Alamos National Laboratory; Los Alamos, NM

Abstract

Vital area analysis of nuclear power plants has been performed for the Nuclear Regulatory Commission by the Los Alamos National Laboratory from the late 1970's through the present. The Los Alamos Vital Area Study uses a fault-tree modeling technique to identify vital areas and equipment at nuclear power plants to determine their vulnerability. This technique has been applied to all operating plants and approximately one-half of those under construction in the US. All saboteur-induced loss-of-coolant accidents and transients and the systems needed to mitigate them are considered. As a result of this effort, security programs at nuclear power plants now include vulnerability studies that identify targets in a systematic manner, and thus unnecessary protection has been minimized.

Introduction

In the early 1970's, the Nuclear Regulatory Commission (NRC) initiated security research in anticipation of new security requirements for nuclear power plants. When Title 10 of the Code of Federal Regulations Part 73.55 (10 CFR 73.55) came into effect in March 1977, all nuclear power plants were required to submit amended security plans. Los Alamos participated in the review of these amended security plans, which included a list of the vital areas at each plant. Sandia National Laboratories, Albuquerque (SNLA),[1] developed a method for identifying these areas for the NRC's Office of Nuclear Regulatory Research (RES). Two nuclear power plants were analyzed with this new methodology in 1976. A fault-tree approach is used to systematically identify system interrelationships and equipment locations in plants. Early in 1978, the NRC decided to use this analysis approach for all power reactors. Los Alamos has applied it to specific plants for the Office of Nuclear Reactor Regulation (NRR) and, most recently, for Nuclear Material Safety and Safeguards (NMSS). Since the Vital Area Analysis Program's (VAAP) inception, Los Alamos engineers have visited all of the operating reactors and approximately 25 plants undergoing their operating license review. The fault-tree approach has proved to be an excellent tool for performing detailed and systematic vital area analyses of complex plants.

The development of fault trees is central to the vital area program, and the accurate representation of a plant in the trees is essential for reliable results. Development begins with combining generic subtrees that have been modified to show the specific details of the plant under review. The SETS[2] (Set Equation Transformation System) computer code is used to solve the resulting massive fault trees and to provide the results in a usable format.

The fault trees used in these analyses differ from safety fault trees in an important way: failure modes cannot be eliminated because they have a low probability of occurrence. In sabotage fault trees, an adversary is not limited to damaging equipment in a manner corresponding to a likely random fault. This has led to the inclusion of complex scenarios in the fault trees

that require a different set of assumptions than might be needed on a safety fault tree. Because most light-water reactor safety analysis work has been done assuming that single-failure criteria and necessary system interactions are not always well understood, there has been some uncertainty in developing the trees. Generally, the uncertainty is in the area of determining the system or combination of systems that is required to mitigate various saboteur-initiated incidents. This has resulted in a tendency to use conservative assumptions in the sabotage trees. These fault trees will not include credit for incident recovery modes that have not been reviewed and approved by the NRC. Therefore, it is entirely possible that a licensee may be required to overprotect certain areas of a plant in some instances. The case of "better too many than not enough" may satisfy the objectives of security; however, when plant operations are considered, care must be taken not to affect plant safety adversely.

Vital Area Analysis

Background: 10 CFR 73.55 came into effect in March 1977 to provide better protection of nuclear power reactors against industrial sabotage. Los Alamos participated in the review of the amended security plans that were required from every NRC licensed nuclear power reactor. Some of the items reviewed were

1. access control,
2. intrusion detection,
3. contraband interception, and
4. the plant's identification of vital areas.

During the review, we realized that a better way to identify vital areas was needed. Nuclear power plants are large, complex facilities that both are costly to build and have the potential for significant radiological releases. In early 1978, the NRC decided to use the SNLA-developed fault-tree methodology to assure that all vital areas were identified and to identify areas that were not considered vital and did not require such a high level of protection. In the anayses, vital area and vital equipment are defined as follows.

> Vital Area. Any area in which successful sabotage can be accomplished by compromising or destroying the vital systems or components located within this area. A vital area must be constructed substantially, have locked doors, and be provided with access control measures.
>
> Vital Equipment. Any equipment, system, device, or material whose failure, destruction, or release could directly or indirectly endanger public health and safety by exposure to radiation.

Nuclear Power Plants: A power plant requires a heat source heating a working fluid, such as water, that in turn produces steam to drive a turbine-generator that produces electricity. The heat source varies. In the United States, electricity is produced from coal (44%), oil (17%), gas (17%), nuclear (12%), and other sources, such as wood, wind, and hydro (10%). There are about 305 operational nuclear power reactors throughout the world, and about 220 are under construction in 22 countries. The US has the most of any one

country--90 operational power reactors and 40 under construction. There have been no new orders in the US since 1978, and 40 have been cancelled. These numbers change as time goes on.

Figure 1 shows the relative size of these plants. A plant site usually is an area of about two acres. The containment structure is ~170 ft high and ~70 ft in diameter. Cooling towers vary but can be as much as 400--500 ft tall. Each plant has complex water, steam, electrical, and nuclear systems. The systems all have redundancies built into them so that no single component failure would result in a catastrophic failure.

Vital Area Analysis: A vital area analysis pinpoints sabotage-sensitive targets in nuclear power plants. This is done using an engineering study of plant systems to determine which systems are needed for a safe shutdown, an analysis of possible saboteur actions, and a determination of the plant operator's actions. Using site-specific information, an analyst constructs a fault tree using "AND" and "OR" gates. For example, if one event depends on two other events occurring, an "AND" gate is used. If an event depends on just one of many events occurring, an "OR" gate is used. The SETS computer code then is used to solve the fault trees

The study of a specific plant begins with a 1-week study of all information available on it. The primary document used is the plant's Final Safety Analysis Report (FSAR). A 1-week site visit by two Los Alamos engineers follows the initial study. At the site, meetings are held with plant management and knowledgeable operators and engineers. Transient and loss-of-coolant accident (LOCA) failure criteria are discussed, as are the required mitigating systems. Failure modes and equipment locations also are identified. All this information is marked on plant drawings that are taken back to the Laboratory for further study and input to the SETS code. The plant then is toured to verify data obtained from the discussions and drawings, such as the locations of pumps, valves, control panels, electrical switchgear, and so forth. When the engineers return to Los Alamos, it takes about 4 weeks for an engineer and a data analyst to prepare the data for the computer program. During this time, the Los Alamos engineer usually contacts the plant engineers by telephone to clarify information not obtained during the site visit. Many details must be studied, and the information must be accurate. Another 4 weeks are required for the computer analysis and correction of any errors. A quality assurance review by another knowledgeable Los Alamos engineer, which takes about a week, is required before a final report is submitted to the NRC. The NRC uses this report as part of their input data to determine that the plant has protected essential targets adequately. The report also discloses areas and equipment that may not require a high level of protection. Table I shows a time table for an average vital area analysis.

Vital Area Analysis Computer Output Report: The major sections of the Vital Area Analysis Computer Output Report are shown in Fig. 2. I will discuss only the set equations and the end product--the location solution. The set equations (Fig. 3) describe the fault tree mathematically, and they are solved by the SETS program. The set equations also transform the sabotage events into locations. A typical location solution is shown in Fig. 4. The first six

DRAFT

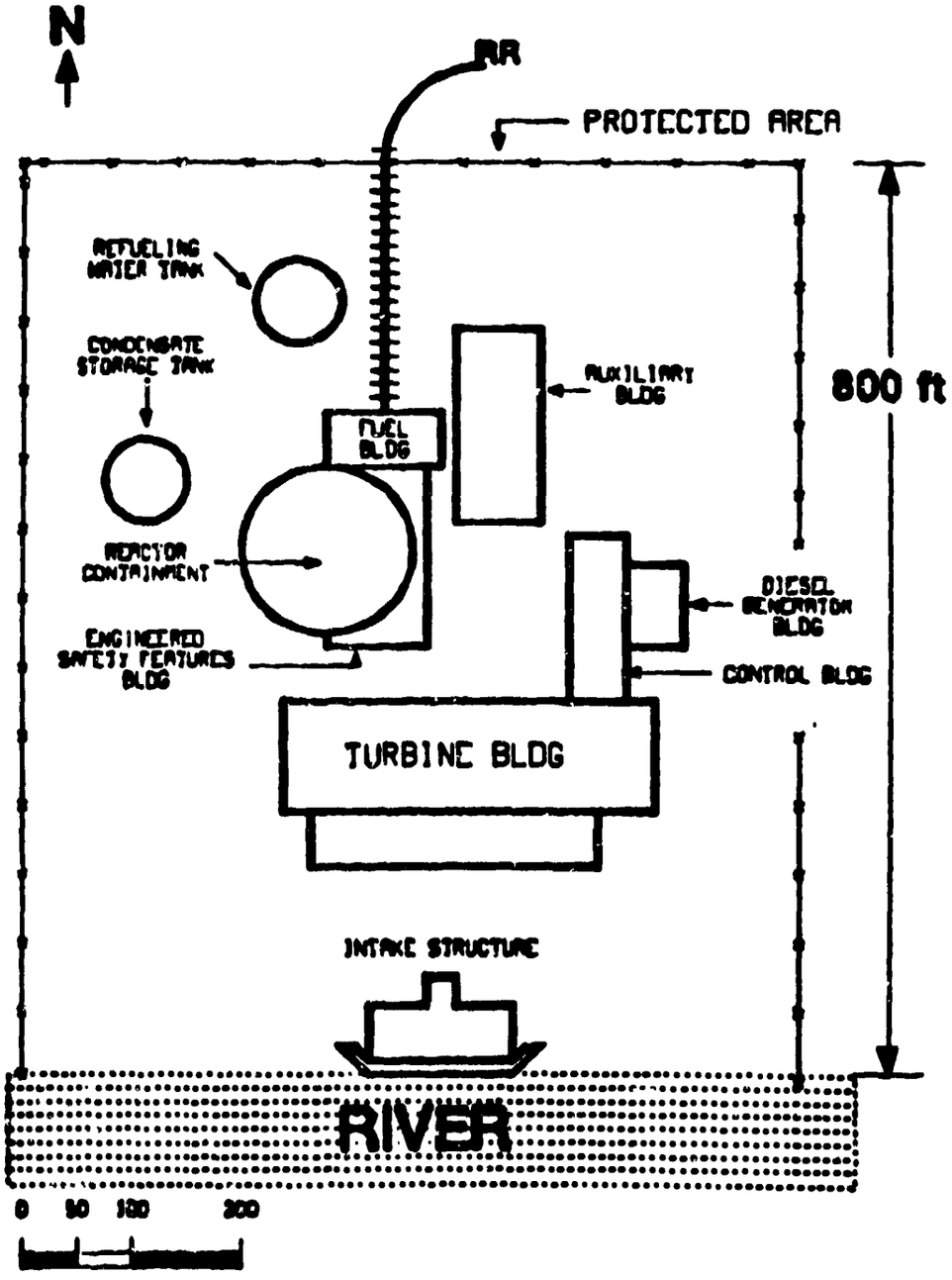

Fig. 1.
Typical nuclear power plant.

VITAL AREA ANALYSIS OUTPUT

- Event Locations
- Locmap
- Fault Tree Event Table - TREE
- Set Equations
  1-Events, 2-Omega/Phi, 3-Locations
- Location Solution
- Location Minimum Protection Set
- Event-Location Analysis
- Keys to Abbreviations

2.2-6-5

Fig. 2.
Summary of vital area analysis output.

Set equations are the mathematical description of the fault tree. These equations are solved by SETS. Set equations also transform the sabotage events into locations.

DG - DG1 - FUEL = DG1RM

Fig. 3.
Typical set equation.

1 - 45TB089

2 - CR

3 - 45TB090

4 - 45TBFAC

5 - 93FB281

6 - CX

7 - CST & 45AB164

8 - CST & 63CB038

Fig.4.
Location solution from computer output.

TABLE I

TIME TABLE

Event	Time Involved
(1) Site visit preparation	1 week
(2) Site visit	1 week
(3) Conversion of raw data into computer input	4 weeks
(4) Computer analysis	4 weeks
(5) Quality assurance review	1 week
(6) Submit report to NRC	

items are abbreviations for single vital areas. (45TB089 means the 45 ft elevation of the Turbine building room number 089; CR means Control Room; and so forth.) The seventh and eighth items are double vital areas (CST means condensate storage tank and 45AB164 means the 45 ft elevation of the auxiliary building room number 164); that is, the saboteur would have to go to two areas and commit an act of sabotage in each to cause a radiological release.

Simplified generic sabotage fault trees for light-water reactors are shown in Figs. 5, 6, and 8. Figure 5 is a typical fault tree in that the top event is a radiological release from a plant. Below this top event is an "OR" gate with inputs. Any one of these inputs can cause a release. The three inputs are fission products released from the spent fuel storage area, fission products released from the containment because of a fuel melt, and fission products released from radwaste systems. These subtrees are developed elsewhere on the fault tree. Figure 6 illustrates a simplified development of the release from a containment fuel melt. The inputs to the top of Fig. 6 are fuel melt from a LOCA and the mitigating systems disabled (LOC-MIT) OR fuel melt from an induced transient and the mitigating systems disabled (TRANS-MIT). Notice that under both LOC-MIT and TRANS-MIT there is an "AND" gate. This means that under LOC-MIT the LOCA must be induced AND the mitigating systems disabled for the gate to open. The same logic applies under TRANS-MIT.

Figure 7 a simplified piping diagram of a typical reactor coolant system. The diagram indicates a coolant source, pumps, valves, and piping routes. This coolant system is partially modeled in Fig. 8 as a generic subfault tree. Note that loss of flow from coolant sources, loss of flow through the pump, or loss of flow from the pumps' discharges will open the gate at the top of the subfault tree. The triangle means that this event is developed elsewhere; the circle indicates a basic event, which means the end of a branch of the tree. The areas where this event could occur would be listed under it.

Spinoffs from the Program: This program has other applications beside verifying that all the vital areas in a plant are protected. The analysis reports are used in assessing any communicated threat against a nuclear power reactor; the Los Alamos engineers working on this program are trained in threat assessment. This methodology also has been used in facility vulnerability studies for NASA's space transportation system and can be adapted readily to vulnerability studies for industry and the military.

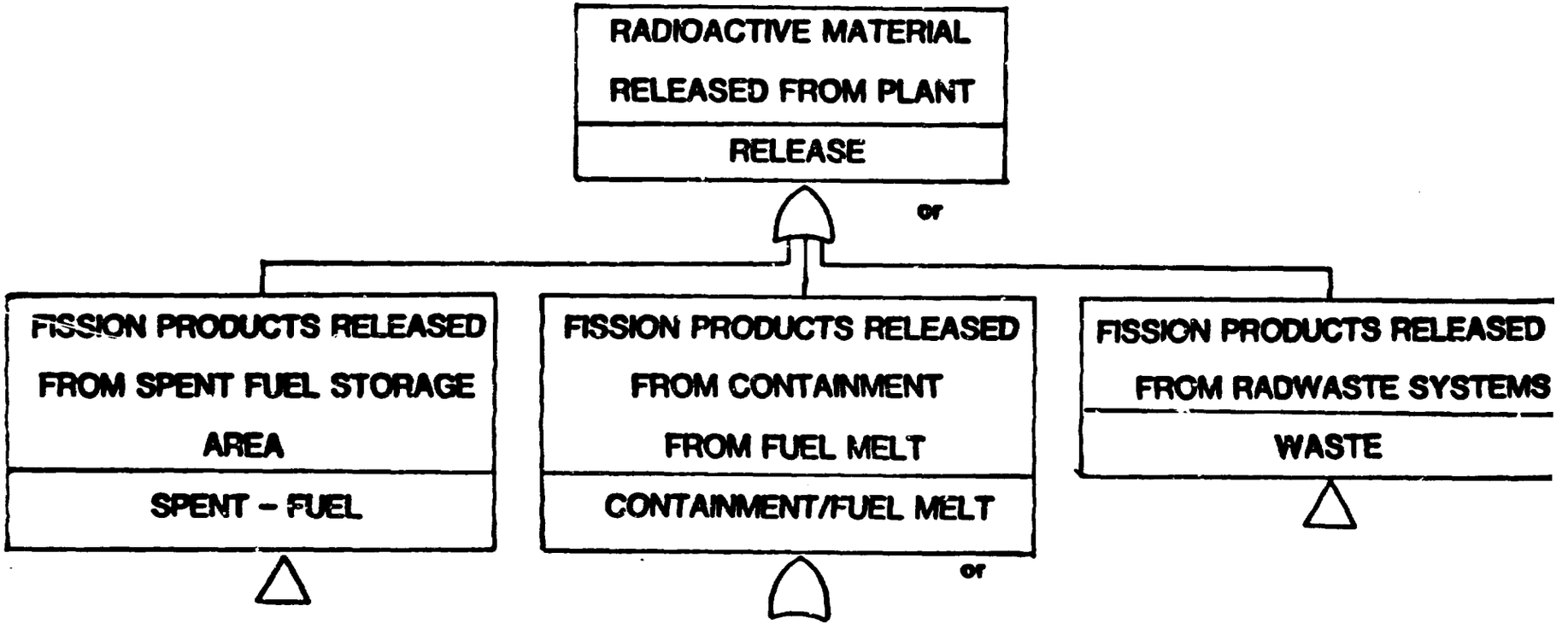

Fig. 5.
Simplified generic sabotage fault tree for light-water reactors.

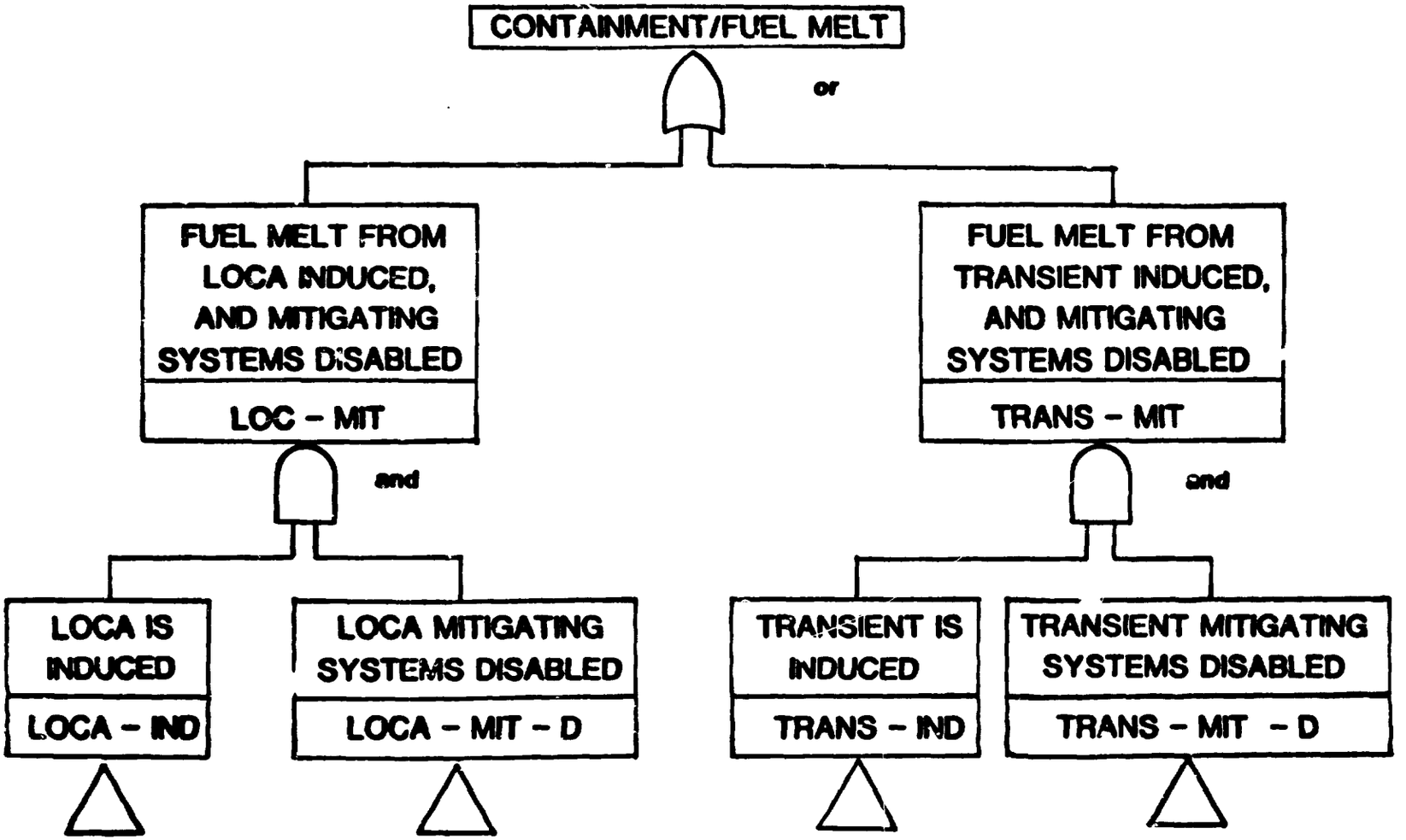

Fig. 6.
Further development of simplified generic sabotage fault tree.

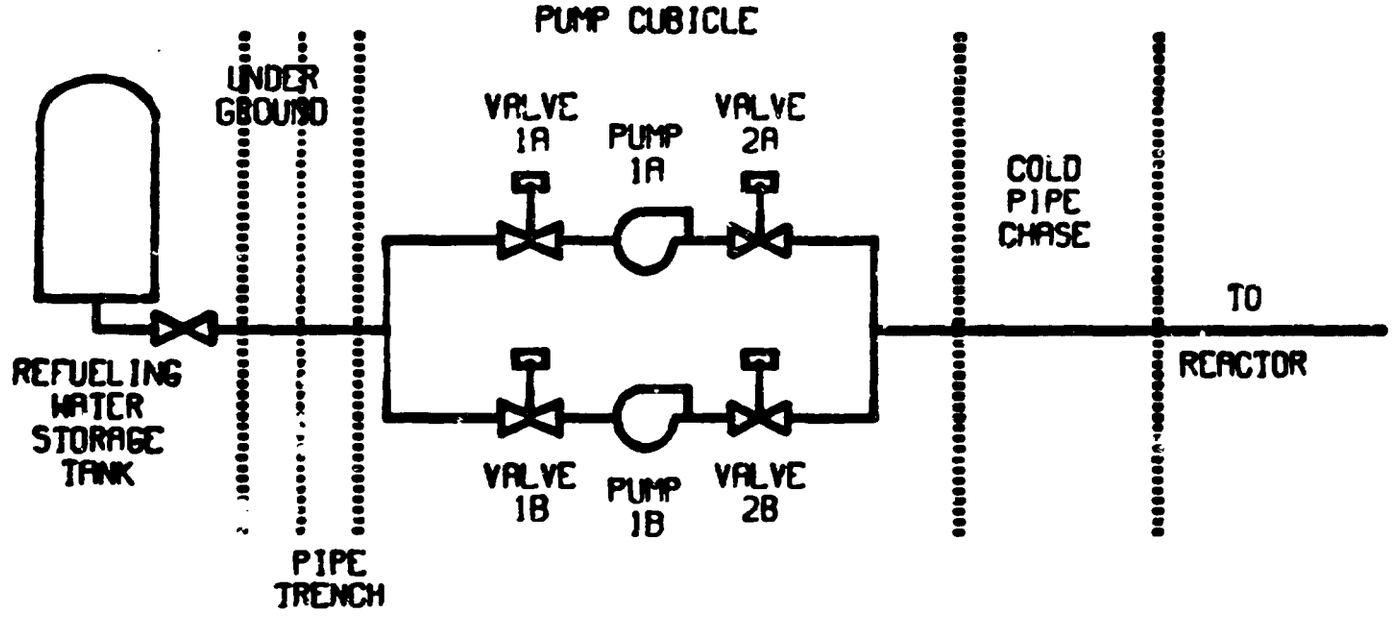

Fig. 7.
Simplified piping diagram for the coolant system.

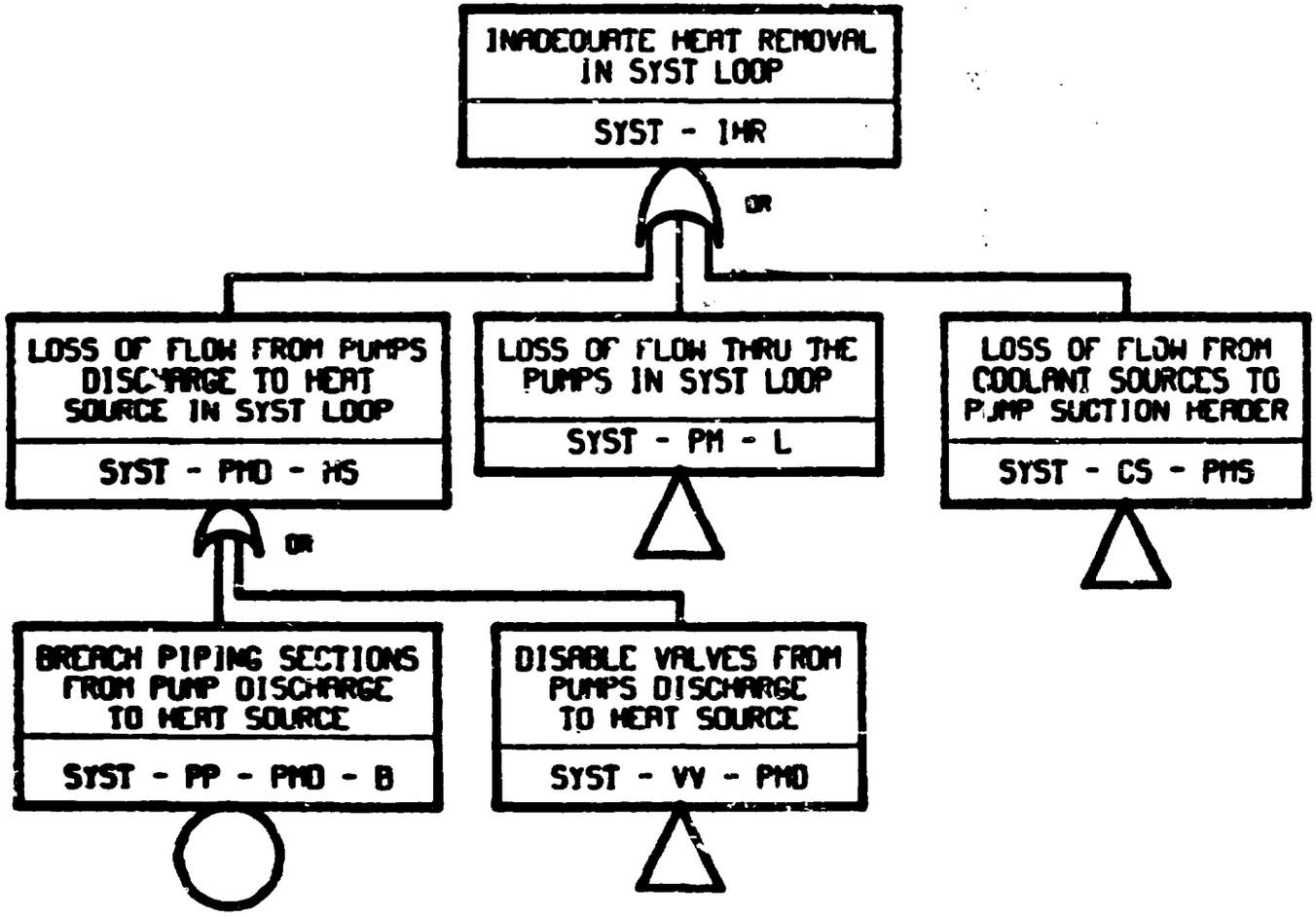

Fig. 8.
Simplified generic subfault tree for the coolant system.

Summary and Conclusions

Using a fault-tree modeling technique, the Los Alamos vital area analysis program analyzed all operating nuclear power plants and about half of those under construction. The result of this effort is that the security programs at nuclear power plants now include vulnerability studies that identify vital targets in a systematic manner, and thus unnecessary protection has been minimized. Expertise has been developed that can use this vulnerability modeling technique for any industrial or military application.

Reference

1. D. J. McCloskey, S. V. Asselin, J. W. Hickman, G. B. Varnado, and J. A. Milloy, "Protection of Nuclear Power Plants Against Sabotage," Sandia National Laboratories report SAND77-01163 (October 1977).

Biography

Donald F. Cameron, PE
Los Alamos National Laboratory, Group Q-6
Box 1663, MS K557
Los Alamos, New Mexico 87545 USA

Donald F. Cameron, PE, is the Principal Investigator of the nuclear power plant Vital Area Analysis Project in the Safety Assessment Group, Energy Division, of the Los Alamos National Laboratory. Since receiving a B.S. in Civil Engineering from the College of the City of New York in 1954, Mr. Cameron has worked in various areas of engineering in the Army, the Los Alamos National Laboratory, and industry. His work during the last decade has involved applying computer fault-tree modeling techniques to determine vital areas to be protected against sabotage in all types of commerical nuclear power plants.