

NUREG/CR-0809
SAND79-0946
Unlimited Release

Fault Tree Analysis for Vital Area Identification

Bruce G. Varnado, Nestor R. Ortiz

Prepared by Sandia Laboratories, Albuquerque,
New Mexico 87115 and Livermore, California 94550
for the United States Nuclear Regulatory Commission
under DOE Contract AT(29-1)-789.

Printed June 1979



Sandia Laboratories

F 2900 017-731

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

8007280 012

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

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, nor the United States Nuclear Regulatory Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

NUREG/CR-0809
SAND79-0946
Unlimited Release

FAULT TREE ANALYSIS FOR VITAL AREA IDENTIFICATION

G. Bruce Varnado
Nuclear Facility Analysis Division 4414
Nestor R. Ortiz
Fuel Cycle Risk Analysis Division 4413

Printed June 1979

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

Prepared for
Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Interagency Agreement DOE 40-550-75
NRC FIN No. A1060

ABSTRACT

This paper discusses the use of fault tree analysis to identify those areas of nuclear fuel cycle facilities which must be protected to prevent acts of sabotage that could lead to significant release of radioactive material. By proper manipulation of the fault trees for a plant, an analyst can identify vital areas in a manner consistent with regulatory definitions. This paper discusses the general procedures used in the analysis of any nuclear facility. In addition, a structured, generic approach to the development of the fault trees for nuclear power reactors is presented along with selected results of the application of the generic approach to several plants.

CONTENTS

	<u>Page</u>
Introduction	9
Fault Tree Analysis Techniques	10
Vital Area Analysis	12
Generic Sabotage Fault Trees	14
Development of the Plant-Specific Sabotage Fault Tree	15
Results of the Vital Area Analysis	19
Conclusion	20
References	21

ILLUSTRATION'S

Figure

1	Top Portion of a Sabotage Fault Tree for a Pressurized Water Reactor (PWR)	12
2	Procedure to Identify Vital Areas and Event Sequences	15
3	Figure 1 (Repeated)	16
4	Continued Development of One Branch of the Sabotage Fault Tree	17
5	Generic Sabotage Fault Tree for an Open Loop without Pumping Power	18
6	Simplified Sabotage Fault Tree for Motor-Operated Valve	18

TABLES

Table

I	Symbols Used in the Graphical Representation of a Fault Tree	11
---	--	----

FAULT TREE ANALYSIS FOR VITAL AREA IDENTIFICATION

Introduction

The first step in designing or evaluating safeguards systems for a nuclear facility is the identification of the areas of the facility for which protection is required. The regulations governing commercial nuclear facilities define two types of areas which must be protected: material access areas and vital areas.¹ Procedures for identification of material access areas and for evaluation of the material control and accounting function related to these areas are discussed elsewhere.² This paper deals with the identification of vital areas with particular emphasis on vital area identification for nuclear power reactors.

A vital area is defined as any area which contains vital equipment. Vital equipment is defined as "any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital" (see Reference 1). The more stringent physical protection requirements in recently issued regulations,^{3,4} coupled with the redundant, safety-based design of nuclear facilities, imply significant economic and operational impacts if all areas containing safety-related equipment are required to have a high level of physical protection. The techniques discussed in this paper can be used to identify, in a structured, systematic manner, the areas of a plant that truly are vital and, therefore, must be protected against sabotage.

Facilities which use or process nuclear material are designed with redundant and diverse systems to prevent release of radioactive material. To determine the many possible combinations of events which could cause significant radioactive release usually requires the application of a systematic analytic method. In studies of sabotage vulnerability for several types of plants, fault tree analysis has been found

to be a useful tool for this purpose. First, fault tree analysis provides a means of stating and analyzing the problem in a very comprehensive manner. Second, the same general approach is applicable for any type of facility. In addition, there are computer codes and procedures for fault tree analysis which can be used to extract a great deal of information from the fault trees such as the most important vital areas and the combinations of areas that are the least costly to protect.

There are, however, a number of limitations on the use of fault tree analysis to study the potential for sabotage leading to radioactive release. In addition to having a detailed understanding of the plant systems, the analyst must be familiar with fault tree analysis techniques. The process is time-consuming, requiring several man-months for detailed analysis of a large nuclear facility. Furthermore, the results may be very analyst-dependent in that each analyst could overlook some failure modes or could develop the fault tree to a different level of detail.

The generic sabotage fault trees and procedures which are under development would largely overcome the limitations mentioned above. This paper briefly discusses the basic techniques of fault tree analysis, the mathematical concepts used to manipulate the fault trees, and the concept of generic sabotage fault trees for nuclear power reactors. Selected results of the application of the procedures to several reactor plants are presented to illustrate the utility of the approach.


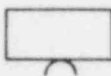

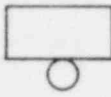

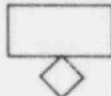

Fault Tree Analysis Techniques

A fault tree is a logic diagram which graphically represents the combinations of subsystem and component faults that can result in a specified undesired event. The undesired event of interest in this discussion is the release of significant quantities of radioactive material from a nuclear facility. In the analysis, this undesired event is successively developed into combinations of contributing events until primary events (individual sabotage acts such as disabling a pump, severing a pipe, etc.) terminate each branch of the tree. Table I defines the symbols commonly used in the fault trees. Figure 1 shows the top portion of a sabotage fault tree for a power reactor. Each gate in the tree represents the logical operation (AND or OR) by

which the inputs combine to produce an output. Each branch of the tree is developed by identifying the immediate, necessary, and sufficient conditions leading to each event.

TABLE I

Symbols Used in the Graphical Representation of a Fault Tree

<u>GATES</u>		<u>INTERMEDIATE EVENTS</u>	
AND GATE		INTERMEDIATE EVENT	
	THE COEXISTENCE OF ALL INPUT EVENTS IS REQUIRED FOR THE OUTPUT TO OCCUR.		A RECTANGLE ABOVE A GATE REPRESENTS THE OUTPUT EVENT PRODUCED BY THE GATE'S LOGIC.
OR GATE		BASIC EVENT	
	THE OUTPUT EVENT WILL OCCUR IF ONE OR MORE OF THE INPUT EVENTS OCCURS.		<u>PRIMARY EVENTS</u> THE RECTANGLE ABOVE A CIRCLE IDENTIFIES A BASIC EVENT. A BASIC EVENT IS ONE WHOSE CAUSES WILL NOT BE FURTHER IDENTIFIED.
TRANSFER IN		UNDEVELOPED EVENT	
TRANSFER OUT			THE RECTANGLE ABOVE A DIAMOND IDENTIFIES AN UNDEVELOPED EVENT WHOSE CAUSES HAVE NOT BEEN IDENTIFIED, OFTEN BECAUSE THERE IS A MORE ATTRACTIVE ALTERNATIVE.
	<u>TRANSFER SYMBOLS</u> 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.		

From a fault tree, an equivalent Boolean logic equation can be developed.^{5,6} Each gate or event is given a label as indicated in Figure 1. In the Boolean equation for the fault tree, these labels (or literals) are joined together by the logical operators \vee (OR) and \wedge (AND) as indicated by the gates. The Boolean equation for the top event in the tree shown in Figure 1 is

$$\text{RMR-PWR} = \text{RRCC} \vee \text{RSNFC} \vee \text{RFRADWSC} \quad (1)$$

The logical equivalent for each of the events on the right hand side of Equation 1 are substituted into the equation to develop the complete equation for the tree. The successive substitution of events lower in the tree for ones higher continues until the top event is represented solely in terms of primary events. Each combination of primary events sufficient to cause radioactive release from the plant appears as a term in the logic equation for the tree; thus, each term represents a "scenario" which must be prevented. The fault tree provides a means of cataloging the large number of combinations (typically there may be millions) in a structured manner.

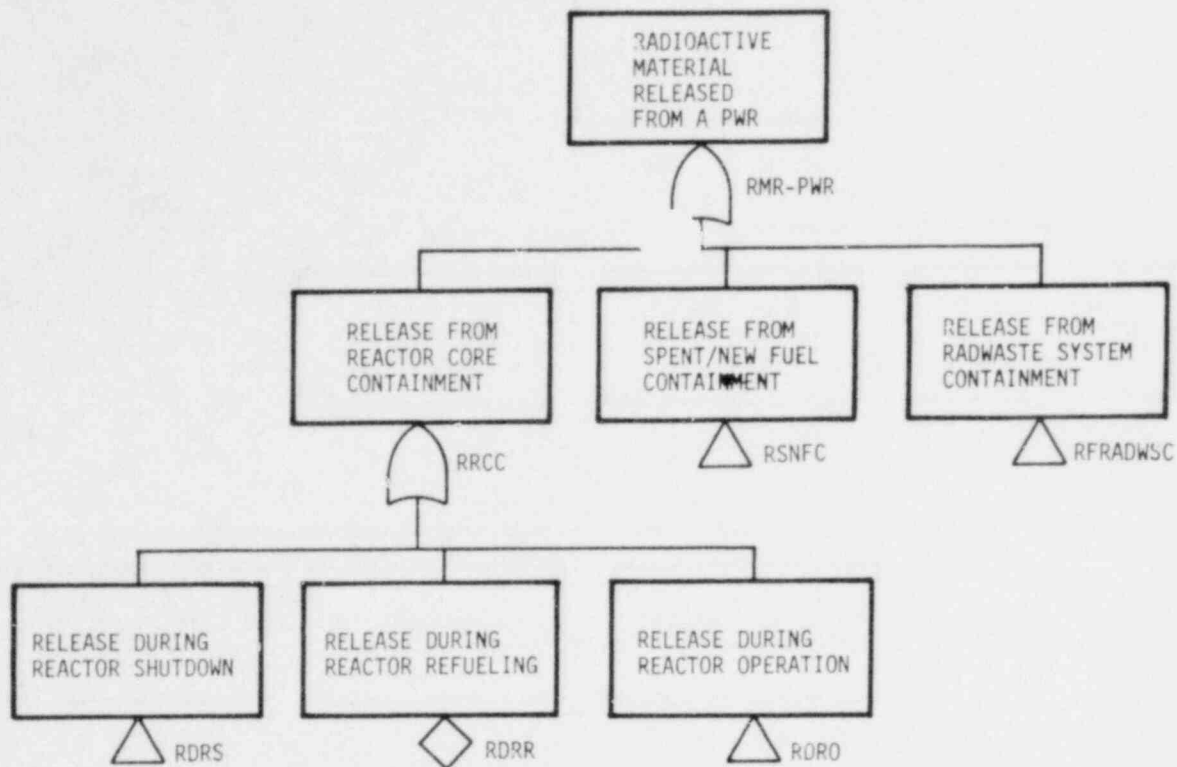


Figure 1. Top Portion of a Sabotage Fault Tree for a Pressurized Water Reactor (PWR)

Vital Area Analysis

The primary events in the fault tree 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. For some combinations of sabotage actions, the time sequence of occurrence (or the order in which areas must be entered) is important. However, this time-dependence is not considered in the definition of vital areas and is not presently addressed in the fault trees. The conservative assumption is made that the saboteur will perform the sabotage actions in the sequence which could cause a significant release.

In the vital area 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 on page 11 to obtain a location-equation for the undesired event. This location-equation represents the location or combinations of locations to which the adversary must gain access in order to cause a release of radioactive material. Each combination of locations (each term in the location-equation) may represent a single 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 a release. Because there are usually fewer locations than primary events, the location-equation is typically much simpler than the event-equation. While the event-equation is likely to contain millions of terms, the location-equation will typically have no more than about one hundred terms.

The output of the vital area analysis is a logic equation which identifies the combinations of areas to which an adversary must gain access in order to cause a release of radioactive material from the plant. The equation lists the single areas from which a set of events sufficient to cause release can be accomplished followed by the combinations of two, three, and so on. From this equation, the vital areas for the plant can be identified directly. It is also possible to list the combinations of events which could cause release for each combination of areas in the location-equation.

The location-equation can be processed further to identify a minimum set of locations, the protection of which will interrupt all possible sequences leading to radioactive release. This is done by taking the Boolean complement (logical NOT) of the location-equation. 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. For the locations, nonoccurrence implies that access has been denied. 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 measures (such as cost of protection or impact on normal operations) which can be associated with

each location. Using this approach, an analyst can determine minimum requirements for protection at a plant. Such information can be used to guide the design and evaluation of plant safeguards systems.

Generic Sabotage Fault Trees

All nuclear power reactors have a number of features in common. All have the same basic sources of radioactive material (core, fuel storage, radioactive waste) and the same general functions necessary for prevention of radioactive release (reactor shutdown, decay heat removal, etc.). Because of these common characteristics, fault trees for different power reactors will have very similar structure. A generic sabotage fault tree which applies to a broad spectrum of reactors has been developed for these common features.

From the broad spectrum generic sabotage fault tree, derivative generic fault trees for a particular type of nuclear power reactor (PWR, BWR, LMFBR) have been developed. These trees incorporate both the common features of reactors and the unique features of the reactor type. Even among plants of the same type and vintage, details of plant design and layout are usually not common. The systems used to provide the functions necessary to prevent radioactive release, the subsystems and components comprising these systems, and particularly the locations of components can vary significantly from plant to plant. Because of these plant-specific differences, the details of the sabotage fault trees and, thus, the number and locations of vital areas will be different for each individual reactor plant.

General procedures have been developed to aid the analyst in gathering the appropriate plant-specific information and assimilating that information into the generic trees to produce detailed sabotage fault trees for specific plants. Figure 2 represents the steps that will lead to a specific analysis of a particular plant. When the development of the plant-specific fault tree is completed by the analyst, the associated logic equations can be manipulated to identify the vital areas, as discussed in the previous section.

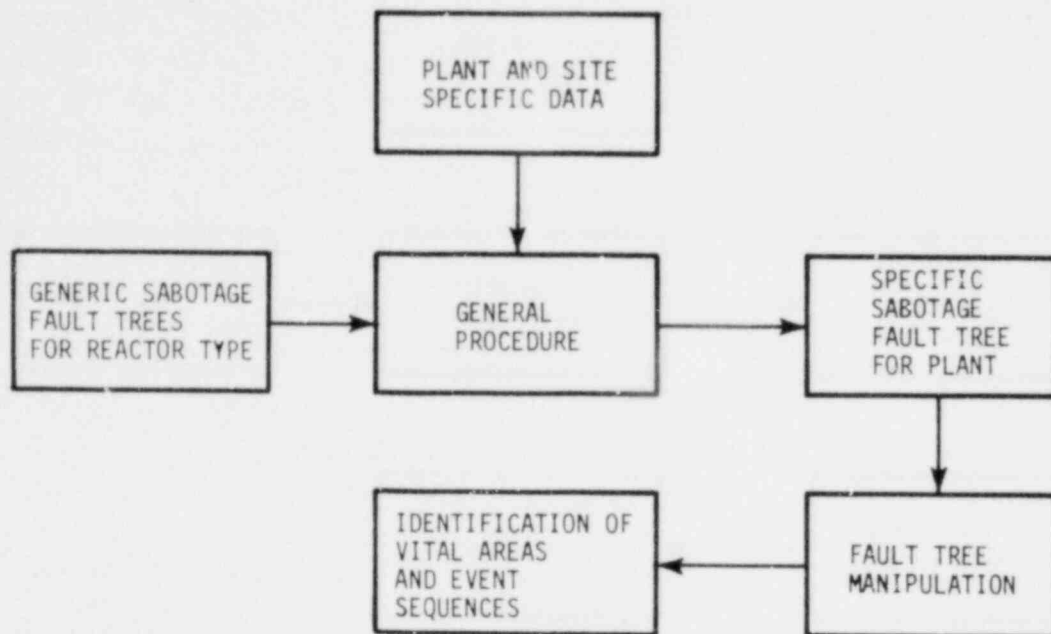


Figure 2. Procedure to Identify Vital Areas and Event Sequences

The generic sabotage fault trees and the general procedures overcome the limitations of fault tree analysis mentioned earlier. In particular, they (1) make it possible for someone with little knowledge of fault tree analysis to efficiently develop the detailed trees, (2) reduce the time required to develop the specific trees, and (3) make it unlikely that a sabotage event is overlooked in the development of sabotage fault trees for specific plants.

Development of the Plant-Specific Sabotage Fault Tree

The top of the generic sabotage fault tree is shown in Figure 3. To properly analyze the problem, it is necessary to specify the level of radioactive release that is of concern. A release in excess of the limits specified in 10CRF100⁷ is usually defined as the top event in the tree. The first level of development identifies the possible sources of radioactive material. If it can be shown that the release of all the radioactive material from one of these sources would not exceed the limits specified by the top event, then that source can be eliminated from the tree. For example, in some plants the radioactive waste system does not have to be considered as a source. The next level of the tree specifies the plant operating modes considered in

the analysis. Some of the equipment necessary to prevent release of radioactive material during power operation may not be required during a refueling outage; thus, it may be appropriate to define different sets of vital areas for the different modes of operation. The fault tree analysis provides a logical structure and detailed documentation which supports the selection of vital areas for the different operating modes.

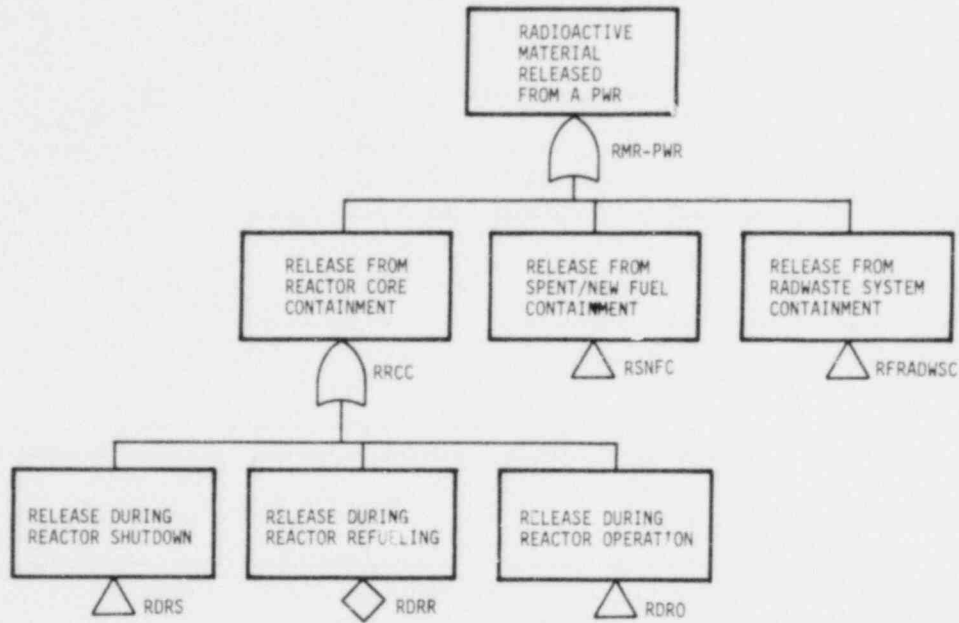
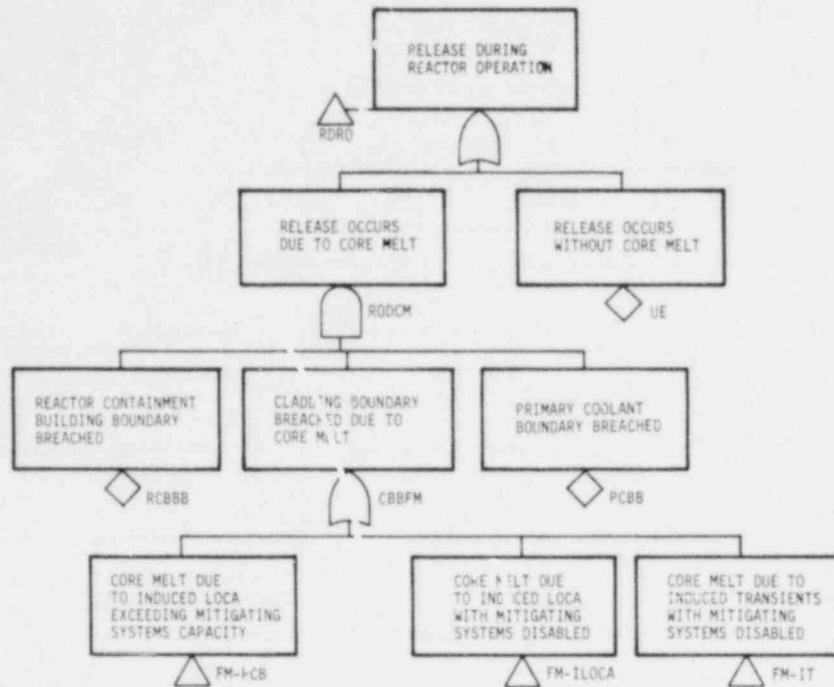


Figure 3. Figure 1 (Repeated)

The branch of the tree dealing with release from the core during reactor operation is developed further in Figure 4. As indicated by the AND gate labeled RODCM, three barriers must be breached if release is to occur. A conservative assumption often used in analyzing the trees is that core meltdown will breach all three barriers. Core melt can be caused in any of three ways, as shown by the OR gate labeled CBBFM: (1) by initiating a loss of coolant accident (LOCA) which exceeds the makeup capacity of the LOCA mitigating systems, (2) by initiating a LOCA and disabling the mitigating systems designed to respond to the LOCA, or (3) by causing a transient and disabling the appropriate transient mitigating systems. The development of these events depends upon the functional design and capacity of systems used to mitigate loss of coolant and transient incidents. It is at this point that plant-specific differences begin to appear in the trees. Generic subtrees



NOTE: LOCA = LOSS OF COOLANT ACCIDENT

Figure 4. Continued Development of One Branch of the Sabotage Fault Tree

representing commonly occurring system and component characteristics are used to develop the detailed sabotage fault trees from this point on.

At many places in the further development of the tree, events occur involving insufficient heat transfer in a heat-removal loop. The types of loops encountered in reactor systems have been classified according to common characteristics and fault trees developed for each type. An example of one such generic loop tree is shown in Figure 5. Within each class, the loop trees are made very general so as to cover possible variations in system design. The analyst must determine the type of loop he is analyzing and the appropriate labels for component identification and indicate any events that do not apply to the particular loop under study.

Eventually the analysis reaches the level of individual component failures. Common components such as valves and pumps have been classified according to type and subtrees developed for each. A typical valve subtree is shown in Figure 6. In the case of valves, the analyst must determine the type of valve, its normal state (open or closed), and its

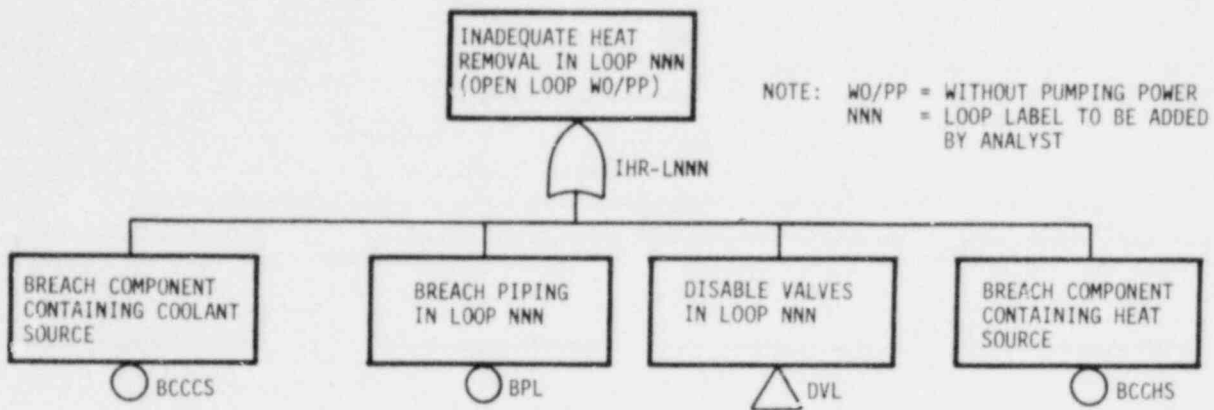


Figure 5. Generic Sabotage Fault Tree for an Open Loop without Pumping Power

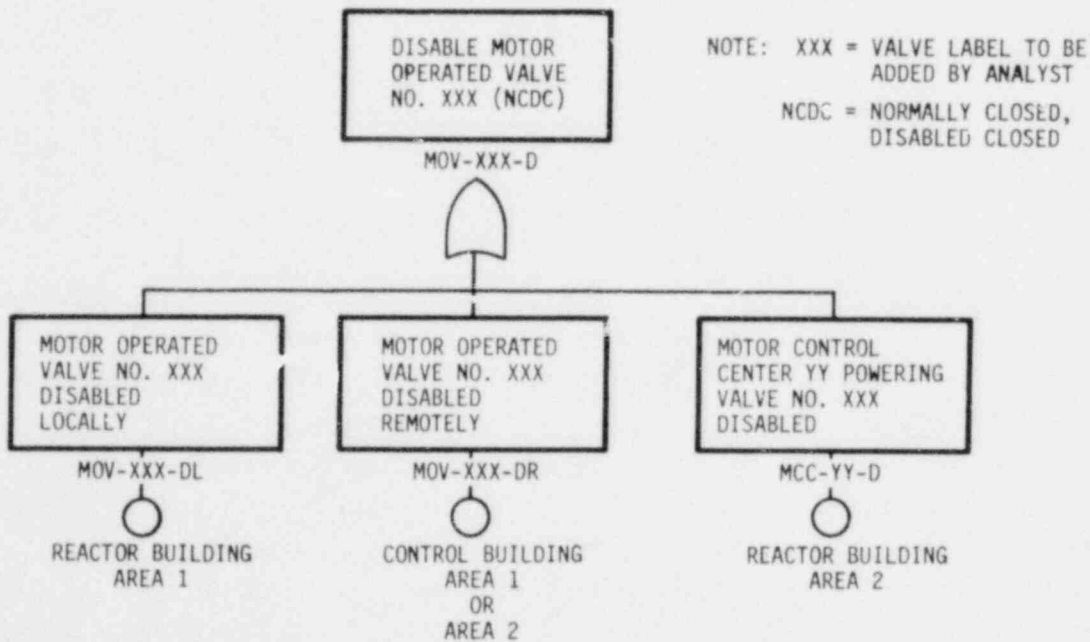


Figure 6. Simplified Sabotage Fault Tree for Motor-Operated Valve

disabled state. The disabled state is important because it could imply different sabotage actions depending upon the application of the valve. For example, the disabled state for an isolation valve would be open while the disabled state for a similar valve used in an injection system would be closed. The tree shown in Figure 6 describes the ways a saboteur could disable a motor-operated valve (MOV) which is normally closed and for which the disabled state is closed (that is, an MOV which must open in response to some abnormal system condition). As is the case for the loops, the analyst must add the appropriate labels for each component.

The generic sabotage fault trees are stored on computer files and can be called up on a computer graphics display system as the analyst selects the appropriate trees, adds the required labels, and deletes any branches not needed for the specific plant under study. As other types of equipment are classified and characterized, the resulting subtrees will be added to the library.

To complete the vital area analysis, the analyst must add the location information for each primary event in the tree. Example location assignments are shown below the primary events in Figure 6. Every location at which each event can be accomplished must be identified. For a detailed fault tree, it is usually a straightforward matter for someone familiar with the layout and operation of the plant to make the required location assignments.

The generic sabotage fault trees provide a means of quickly developing a detailed logic model of a complicated reactor plant. So far, these logic models have been used primarily to study sabotage vulnerability. There are other possible applications of these generic modeling approaches in the study of reactor safety problems as well. An expanding role for the basic techniques used for vital area analysis in the study of related reactor safety issues and the extension of the generic fault tree analysis procedures to other types of facilities is anticipated.

Results of the Vital Area Analysis

The vital area analysis procedures have been applied to several light-water reactor plants. The number of vital areas identified for

a plant ranged from 20 to 40. Of these vital areas, three to seven were Type I vital areas,⁸ i.e., single locations from which a saboteur could complete sufficient sabotage acts to cause release. The remainder were Type II vital areas,⁸ areas which must be visited in combinations of two or more. There were approximately 50 to 90 combinations of Type II vital areas from which radioactive release could be initiated and millions of combinations of sabotage acts which could lead to release. Using the generic sabotage fault tree procedures, an analyst can develop the detailed fault trees for a nuclear power reactor in a relatively short time. The large, complex fault trees produced in this process (as indicated by the millions of combinations of events in the reduced fault tree equation) can be analyzed efficiently using the SETS code.^{5,6} The entire process of tree development and analysis requires only a few weeks. Improvements being developed for the code will speed the analysis even more.

Conclusion

The vital area analysis procedures described in this paper provide a disciplined, logical, repeatable method for determining vital areas in nuclear facilities. The fault trees clearly document the assumptions made in the analysis and allow the analyst to examine the effect of different sets of assumptions on the number and location of vital areas. The results are consistent in form and level of details for every plant analyzed so that uniform criteria can be applied. Analytical procedures which identify the minimum set of areas which must be protected can help to reduce the costs of physical security while maintaining adequate protection of public health and safety.

The generic sabotage fault trees make it possible for an analyst with a minimum knowledge of fault tree analysis techniques to develop detailed fault trees for specific power reactor plants. The procedures described in this report provide an option a licensee can use for defining vital areas in his nuclear power plant. It is likely that vital area analysis procedures will gain greater acceptance within the regulatory process as more experience is gained in their use.

References

1. "Energy," Title 10, Part 73, The Code of Federal Regulations.
2. F. M. Gilman, H. E. Lambert, and J. J. Limm, "The Results of a Directed Graph-Fault Tree Assessment of an MC&A System," presented at the Institute of Nuclear Materials Management 19th Annual Meeting (June 1978).
3. "Energy," Title 10, Part 73.20, The Code of Federal Regulations (July 1977).
4. "Energy," Title 10, Part 73.55, The Code of Federal Regulations (April 1977).
5. R. B. Worrell, Set Equation Transformation System (SETS), SLA-73-0028A (Albuquerque: Sandia Laboratories, July 1973).
6. R. B. Worrell, "Using the Set Equation Transformation System in Fault Tree Analysis," Reliability and Fault Tree Analysis, R. E. Barlow, J. B. Fussel, and N. D. Singpurwalla, eds. (Philadelphia: SIAM, 1975), pp 165-185.
7. "Energy," Title 10, Part 100, The Code of Federal Regulations (January 1977).
8. "Definition of Vital Areas and Equipment," NRC Review Guideline 17 (January 1978).

DISTRIBUTION:

U. S. Nuclear Regulatory Commission (260)
Division of Document Control
Distribution Services Branch
7920 Norfolk Avenue
Bethesda, MD 20014

U. S. Nuclear Regulatory Commission (5)
M. S. 1130SS
Washington, DC 20555
Attn: R. Robinson

Los Alamos Scientific Laboratory
Los Alamos, NM 87544
Attn: D. G. Rose

Lawrence Livermore Laboratory
University of California
P. O. Box 808
Livermore, CA 94550
Attn: A. Maimoni

Peter R. Lobner
Science Applications, Inc.
1200 Prospect Street
P. O. Box 2351
La Jolla, CA 92038

Dr. J. Mark Elliott
International Energy Associates Limited
600 New Hampshire Avenue, NW
Washington, DC 20037

U. S. Nuclear Regulatory Commission (3)
M. S. 3106 MNNB
Washington, DC 20555
Attn: G. Edison
W. Vesely
J. Murphy

1230 W. L. Stevens
Attn: R. E. Smith, 1233
1700 W. C. Myre
1750 J. E. Stiegler
1754 I. G. Waddoups
1758 C. E. Olson
1758 D. D. Boozer
1760 J. Jacobs
1760A M. N. Cravens
1761 T. A. Sellers
1761 J. L. Darby
3145 W. R. Dameron
4400 A. W. Snyder
4410 D. J. McCloskey
4412 J. W. Hickman
4413 W. R. Ortiz (5)
4414 G. B. Varnado (10)
4416 L. D. Chapman
4420 J. V. Walker
4440 G. R. Otey

4442 W. A. Von Rieseemann
4443 D. A. Dahlgren
4510 W. D. Weart
4540 M. L. Kramm
4550 R. M. Jefferson
5640 G. J. Simmons
8266 E. A. Aas
3141 T. L. Werner (5)
3151 W. L. Garner (3)
for DOE/TIC
NRC/NTIS (25)
(R. P. Campbell, 3154-3)