1000-MWe LMFBR Accident Analysis
And
Safety System Design Study
— Phase I —
Fault Trees And Malfunction Catalog

December 1969

LEGAL NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy 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.

ANL Contract No. 31-109-38-2339
B&W Contract No. 847-0501

BABCOCK & WILCOX
Nuclear Power Generation Department
Power Generation Division
P. O. Box 1260
Lynchburg, Virginia 24505

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

THIS PAGE
WAS INTENTIONALLY
LEFT BLANK

CONTENTS

	Page
1. INTRODUCTION	1-1
1.1. General	1-1
1.2. Program Objectives and Scope	1-2
2. PHASE I SUMMARY AND RESULTS	2-1
2.1. Phase I Summary	2-1
2.2. Phase I Results	2-2
3. FAULT AND MALFUNCTION CATALOG	3-1
3.1. Description	3-1
3.2. Fault and Malfunction Catalogs	3-4
4. FAULT TREE DIAGRAMS	4-1
4.1. General	4-1
4.2. Fault Tree Presentation	4-1
4.3. Fault Tree Summaries	4-2
4.3.1. R/A Release to Environment in Excess of 10 CFR 100 Limits	4-3
4.3.2. Structural Failure of the Secondary Containment	4-3
4.3.3. Failure of Containment Isolation Components	4-4
4.3.4. Structural Breach in the Primary Tank Cover	4-4
4.3.5. Seal Leakage	4-5
4.3.6. Breach in the Primary Tank	4-5
4.3.7. Breach in Cavity Liner	4-6
4.3.8. High Pressure in Primary Tank	4-6
4.3.9. High-Temperature Primary Coolant Entering the Core	4-7
4.3.10. Inadequate Primary Coolant Flow	4-8
4.3.11. Failure of the Normal Decay Heat Removal System	4-8
4.3.12. Rundown Failure	4-9
4.3.13. Scram Failure	4-9
4.3.14. Fast Setback Failure	4-9
4.4. Pictorial Aids	4-9
APPENDIXES	
A. Fault Trees	A-1
B. Glossary	B-1

List of Tables

Table		Page
3-1.	Fault Catalog Headings	3-2
4-1.	Index of Fault Tree Numbers	4-11

List of Figures

Figure		
2-1.	Phase I Activity Flow Diagram	2-1
4-1.	Definition of Fault Tree Symbols	4-12
4-2.	Release of Radioactivity From Secondary Containment to the Environment	4-13
4-3.	Release of Radioactivity From Intermediate Coolant or Decay Heat Removal System to the Environment	4-14
4-4.	Release of Radioactivity Through Primary Tank Cover to Secondary Containment	4-15
4-5.	Release of Radioactivity From Primary Tank Cavity to Secondary Containment	4-16
4-6.	Release of Radioactivity From Intermediate Coolant or Decay Heat Removal System to Secondary Containment	4-17
A-1.	Radioactivity Release to Environment in Excess of 10 CFR 100 Limits	A-5
A-2.	Structural Failure of Secondary Containment	A-6
A-3.	Failure of Containment Isolation Components	A-7
A-4.	Structural Breach in Primary Tank Cover	A-8
A-5.	Seal Leakage	A-9
A-6.	Breach in Primary Tank	A-10
A-7.	Breach in Cavity Liner	A-11
A-8.	High Pressure in Primary Tank	A-12
A-9.	High-Temperature Primary Coolant Entering Core	A-13
A-10.	Inadequate Primary Coolant Flow	A-14
A-11.	Failure of Normal Decay Heat Removal System	A-15
A-12.	Rundown Failure	A-16
A-13.	Scram Failure	A-17
A-14.	Fast Setback Failure	A-18

1. INTRODUCTION

1.1. General

In recognition of the need for breeder reactors and the selection of the LMFBR to fulfill this need, the AEC has established the LMFBR program as its highest-priority power reactor development program. The overall objective of the program is to develop a safe, reliable, economical LMFBR power plant for the utility industry. Consistent with the foregoing priority and objective, the AEC implemented a series of plant design studies in 1967 to develop conceptual designs for 1000-MWe LMFBR plants. Babcock & Wilcox (B&W) participated in the 1000-MWe LMFBR Follow-On Study and completed the work late in 1968.

Although the follow-on study provided essential first-step information on the LMFBR conceptual designs favored by industry, the scope of the study was not sufficient. It provided neither in-depth resolution of many safety oriented problems nor detailed guidance for specific research and development requirements. As a result, B&W is undertaking more detailed evaluations of the reference 1000-MWe LMFBR design in an Accident Analysis and Safety System Design Study. This study, which includes investigations of several high-priority safety-related problem areas identified in Element 10 of the LMFBR program plan, involves the analysis of potential accidents that may determine the design basis for protective systems and safety features. Equally important, it includes the development of conceptual designs for the systems or features that are required in certain specified areas. Research and development programs will be developed to cover the necessary safety technology.

The study is being performed on a cost-sharing basis under ANL contract No. 31-109-38-2339. Utility companies are participating in the work under separate agreements with B&W. The Accident Analysis and Safety System Design Study was initiated on June 2, 1969. This document describes the results of the first phase of study.

1.2. Program Objectives and Scope

The basic objective of the study is to develop a better understanding of the influence of safety requirements on commercial LMFBR plants of large size. To achieve this objective, the work will be performed over a three-year period under a program definition phase and four time-oriented sequential work phases that end at clearly defined stages of work.

In Phase I, component and system faults and malfunctions associated with the B&W 1000-MWe LMFBR Follow-On Study reference design have been identified and catalogued. Fault trees were prepared to be used as an aid in identifying necessary protective systems and safety features.

Phase II concerns the definition of initiating conditions based on the faults and malfunctions identified in Phase I, and subsequent analysis of potential reactor accidents to establish functional requirements for selected protective systems and safety features. In parallel, candidate systems or features that have the potential to prevent or mitigate the consequences of accidents will be identified and evaluated before reference designs are selected at the end of Phase II.

In Phase III, conceptual designs will be developed for the protective systems and safety features selected in Phase II. Additional safety analyses will also be performed to verify the compatibility of the functional requirements and systems designs.

In Phase IV, safety-related information that is needed for the design, licensing, construction, and safe operation of pool-type LMFBRs will be specified, and, where meaningful, the effects of nonattainment or partial attainment of research and development goals will be assessed.

Several closely related activities are included in each of the four phases. In general, the activities in each phase are performed in parallel, but some that depend on information generated in earlier work are conducted in series.

2. PHASE I SUMMARY AND RESULTS

2.1. Phase I Summary

Phase I consists of six interrelated work activities. The general flow of information is shown in Figure 2-1.

Figure 2-1. Phase I Activity Flow Diagram

Activity 111 involves a detailed, systematic review of the 1000-MWe reference design to identify potential faults and malfunctions that might be relevant to reactor safety. Potential faults and malfunctions are defined as any conditions or events that represent a departure from the intended design or operational functions. Emphasis is placed on systems and equipment whose failure could significantly affect the primary and secondary containment.

In activity 112, many of the faults and malfunctions identified in the preceding activity are systematically grouped into a catalog. This

catalog is limited to faults and malfunctions that could lead to major accidents.

Activity 121 concerns the preparation of fault trees, which graphically display the principal fault paths, the interfaces of systems with respect to fault propagation, and the consequences of faults or groups of faults. The fault trees are carried to the point where critical faults and malfunctions that might lead to major accidents can be identified.

In activity 122 the fault trees and the analyses of the 1000-MWe reference design provide bases for the identification of necessary protective actions and passive protective devices which can ensure that basic faults and malfunctions will not develop into major accidents. In addition, the variables that may be monitored to initiate protective action are identified.

Engineered safety features that can mitigate the consequences of major accidents are identified in activity 123. The fault trees and previous analyses of the 1000-MWe reference design will once again serve as the bases.

2.2. Phase I Results

The results of Phase I are presented in two major categories: the fault and malfunction catalog and the fault trees. In addition to the faults and malfunctions, the fault and malfunction catalog includes possible protection, monitored variables, and engineered safety features. Thus, the catalogs actually include in tabular form the results of four activities: activities 111, 112, 122, and 123.

Fault trees are summarized and pictorial aids are presented in section 4. The actual fault trees are shown in Appendix A. The fault tree summaries are verbal descriptions that trace key failure paths and indicate important events along these paths. Because of the complexity of many of the systems and subsystems analyzed in the fault trees, a number of engineering sketches are included for explanation. These sketches, although not necessarily to scale, show the relative locations of different components and help to define many of the terms used in the fault trees.

A glossary of terms is given in Appendix B.

3. FAULT AND MALFUNCTION CATALOG

3.1. Description

The failure sequences that may ultimately result in the release of unacceptably large amounts of radioactive materials to the environment are characterized by a number of key failure events, which may result from a combination of basic failures and causal failure events. Basic failures receive no further development, whereas causal failure events will subsequently be described as the result of the other basic failures and causal failure events. These events form the headings for the fault and malfunction catalog. For example, failure events involving the primary and secondary containment and other basic failures may lead to the release of radioactivity to the environment. Similarly, reactivity insertions or abnormal coolant flow may lead to violent core disruption which can, in turn, lead to failure of the primary containment. Therefore, the general flow of the catalog is from failure events caused by basic failures to failure events that are largely the result of other (causal) failure events.

The fault and malfunction catalog is limited to the basic failures and failure events that may ultimately lead to the release of radioactive material. Special emphasis is placed on events that may cause violent core disruption. As a result, all of the faults and malfunctions identified in activity 111 are not presented in this catalog. The preparation of the fault and malfunction catalog is the task of activity 112. The catalogs are in essence verbal fault trees. In keeping with this philosophy, the failure events that form the headings in the catalog are in many cases the same as the titles of fault trees.

The failure events that form the headings in the fault catalog are listed in Table 3-1. The other failure event(s) to which a given failure event is input as a causal failure event are also identified.

Table 3-1. Fault Catalog Headings

Catalog No.	Catalog title	Input to Catalog Nos.
1	R/A Release to Environment in Excess of 10 CFR 100 Limits	
2	Loss of Secondary Containment Integrity	1
3	Structural Inadequacy	2, 5, 24, 27
4	Sodium or NaK Released to Secondary Con- tainment	2, 5
5	Breach in Primary Tank Cover	4, 23
6	Inadequate Heat Removal From Primary Tank Cover	5
7	Abnormal Force on Primary Tank Cover	5
8	High Pressure in Primary Tank	2, 7, 25, 28
9	Inadequate Decay Heat Removal Capability	8
10	Failure of Normal Decay Heat Removal System	9
11	Low Flow in Normal Decay Heat Removal Loop	10
12	Molten Fuel	2, 4, 7, 8, 15, 16, 22, 24, 25, 28
13	Power Transient Following Reactivity Inser- tions	12, 22
14	Overheating of a Single Assembly	12, 13
15	Non-Neutronic Void Propagation From a Single Assembly	12, 22
16	Inadequate Heat Removal Capability	12, 22
17	Inadequate Primary Coolant Flow	16
18	Primary Pump Malfunction	17
19	Loss of Electrical Power to a Primary Pump	17, 18
20	High-Temperature Primary Coolant Entering Core	16
21	Loss of Access to Heat Sink	20, 26
22	Nuclear Disassembly Following Large Reactivity Insertion	2, 4, 7, 8, 25, 28
23	R/A in the Secondary Containment	1
24	Breach in Primary Tank	23, 28
25	Abnormal Force on Primary Tank	4, 24
26	IHX Malfunction	25
27	Breach in Cavity Boundary	4, 23
28	Abnormal Force on Cavity	27

Included in the catalog under each failure event heading are the following:

1. Possible Causes — These are the basic failures and causal failure events which may lead to the failure event that forms the heading for the catalog. Causal failure events are identified by an asterisk and by a number that indicates where the failure event is developed. To show that the coexistence of certain basic failures and/or causal failure events is required to produce a given failure event, the word "and" is inserted between the coexisting events.

2. Possible Protection — Included in this category are the protective actions and passive protective devices that prevent or limit damage to the reactor core. Examples of protective action include scram and decay heat removal; devices to prevent flow blockage to an assembly or thick fuel assembly wrapper cans are examples of passive protective devices. The one or more basic failures and causal failure events that are affected by the suggested protection are identified.

3. Possible Monitored Variables — These are reactor or plant parameters whose variation might indicate the occurrence of a basic failure or causal failure event. In many cases monitoring the onset conditions may permit protective action before failure occurs. In each case the failure that perturbs the monitored variable is identified.

4. Possible Engineered Safety Features — Included in this category are features that prevent the occurrence of or mitigate the results of basic failures or failure events that could release radioactive materials to the environment. The emphasis is on failures outside the core, which may affect the public but which are not likely to affect the core. As in item 2, the features can be active (containment isolation) or passive (a meltdown pan). The failures that are affected by the engineered safety features are identified.

It can be seen that items 2 and 3 of the fault catalog present (in tabular form) the results of activity 122, i.e., the identification of protective actions and passive protection features. The results of activity 123, the identification of engineered safety features, are presented in item 4 under each failure event heading.

The protection and engineered safety features may act on several different levels in a given sequence of failure events. This is especially true in the case of causal failure events that serve as input to other failure events. Thus the protection or engineered safety features that are applicable to a given failure event may be identified both in the catalog where the causal failure event is input and in the catalog in which the causal failure event is developed. In other cases, they may be identified only in the catalog that describes the causal failure event. In this situation, the terms "protection at input level," "monitoring at input level," and the like are used where the causal failure is input.

The catalogs do not list malfunctions in the protection system and the reactivity control system which do not directly lead to accidents. It is assumed that the protective actions listed function as required. The protective systems and the engineered safety features will be developed and analyzed during Phases II and III.

3.2. Fault and Malfunction Catalogs

The 28 fault and malfunction catalogs are presented in this section; each catalog is identified by number.

1. R/A Release to the Environment in Excess of 10 CFR 100 Limits

1. Possible causes:

- a. R/A released from support systems outside the secondary containment (SC)
 - (1) Failure of shipping cask.
 - (2) Failure of decontamination cell.
 - (3) Failure of decontamination vessel.
- b. R/A released from SC
 - (1) Loss of SC integrity* 2.
and
 - (2) Radioactivity in SC*23.
- c. R/A released from intermediate coolant or DHRS outside SC
 - (1) Structural failure of the interface with primary coolant.
and
 - (2) Structural failure of system piping and isolation valves.
- d. R/A released from the rad waste disposal system
 - (1) Structural failure of components outside SC.
 - (2) Seal leakage.

- (3) Failure of filters.
- (4) Malfunction of plant effluent discharge control.
- 2. Possible protection (protects against):
- 3. Possible monitored variables (senses):
 - a. Radiation monitors (all).
- 4. Possible engineered safety features (mitigates results of):
 - a. Remote or underground siting (all).

2. Loss of Secondary Containment Integrity

- 1. Possible causes:
 - a. Structural inadequacy* 3
 - b. Abnormal pressure or temp in SC
 - (1) Na or NaK released to SC* 4.
 - and
 - (2) Fire in SC.
 - c. Abnormal external forces
 - (1) Airborne vehicle or missile crash.
 - (2) Acts of war.
 - (3) Explosion near containment.
 - (4) Ground vehicle crash.
 - d. Impact of equipment
 - e. Internal missiles
 - (1) Failure of component holddown.
 - and
 - (2) High pressure in primary tank* 8.
 - f. Acts of nature
 - (1) Flood.
 - (2) Meteorological phenomena.
 - (3) Earthquake.
 - g. Na or NaK released to SC* 4 and contacting SC liner
 - h. SC liner melted through by molten fuel
 - (1) Molten fuel* 12 in gross amounts on cavity liner.
 - (2) Nuclear disassembly following large reactivity insertion* 22, or molten fuel* 12-Na vapor explosion depositing fuel debris on cavity liner.
 - and
 - (3) Inadequate cooling of SC liner.
 - i. Containment building penetration failure
 - j. Isolation valve failure

2. Possible protection (protects against):
 - a. Scram (f-3).
 - b. Manually initiated shutdown (b, c, d, f).
 - c. Protection at input level (a, b, e, g, h).
3. Possible monitored variables (senses):
 - a. Inspection/operator (c, d, f).
 - b. Seismic shock (f-3).
4. Possible engineered safety features (mitigates results of):
 - a. Overdesign (a - f).
 - b. Remote or underground siting (c).
 - c. Armor plate or reinforcing (c, d, e).
 - d. Thermal shield (g).
 - e. Double seals (i).
 - f. Double isolation valve (j).
 - g. Meltdown pan and SC liner cooling (h).
 - h. Inert containment atmosphere (b).
 - i. Normal air at reduced pressure in SC (b).
 - j. Inert-atmosphere machinery dome (b).
 - k. Limited Na leakage and burning area (b).

3. Structural Inadequacy

1. Possible causes:
 - a. Inadequate safety factors
 - (1) Design error.
 - (2) Insufficient knowledge.
 - b. Faulty material and/or fabrication
 - c. Structural deterioration
 - (1) Excessive corrosion or erosion rate.
 - (2) Insufficient corrosion or erosion allowance.
2. Possible protection (protects against):
 - a. Inspection and quality assurance (b, c).
 - b. Periodic testing (b, c).
3. Possible monitored variables (senses):
 - a. Leakage (b, c).
4. Possible engineered safety features (mitigates results of):
 - a. Overdesign (all).

4. Na or NaK Released to Secondary Containment

1. Possible causes:
 - a. NaK released from DHRS
 - b. Na released from intermediate coolant system
 - c. Na escaping through primary tank cover
 - (1) Breach in primary tank cover*5.
and
 - (2) Nuclear disassembly following large reactivity insertion*22, or molten fuel*12-Na vapor explosion causes Na to impact on underside of primary tank cover.
 - d. Na escaping from cavity
 - (1) Breach in primary tank*25.
and
 - (2) Breach in cavity boundary*27.
and
 - (3) Nuclear disassembly following large reactivity insertion*22, or molten fuel*12-Na vapor explosion forces Na out.
2. Possible protection (protects against):
 - a. Scram or setback (a, b).
3. Possible monitored variables (senses):
 - a. Na or NaK detection in SC (all).
 - b. Na or NaK level in affected system (a, b).
 - c. Na or NaK flow in affected system (a, b).
4. Possible engineered safety features (mitigates results of):
 - a. Armor to protect against missiles or dropped equipment (a, b).
 - b. All Na or NaK piping placed in armored, inerted channels (a, b).
 - c. Programmed movement of heavy equipment to avoid areas where Na or NaK could be released (a, b).

5. Breach in Primary Tank Cover

1. Possible causes:
 - a. Structural inadequacy*3
 - b. Cover weakened by high temp
 - (1) Na or NaK released to SC*4 causing fire.
 - (2) Abnormal reactor heat load.
 - (3) Hot intermediate Na or NaK from DHRS on cover top.
 - (4) Inadequate heat removal from tank cover*6.
 - c. Abnormal force on primary tank cover*7
 - d. Seal leakage

2. Possible protective actions (protects against):
 - a. Scram or setback (b-1, 2, 3).
 - b. Fire prevention — see catalog 2 (b-1).
 3. Possible monitored variables (senses):
 - a. Primary coolant temp (b-2).
 - b. Cover structure temps (b).
 - c. R/A (all).
 4. Possible engineered safety features (mitigates results of):
 - a. Overdesign (a, b, c).
 - b. Inspection (d).
 - c. Containment (all).
 - d. Redundant seals (d).
6. Inadequate Heat Removal From Primary Tank Cover

1. Possible causes:
 - a. Improper cover cooling system performance
 - (1) Improper system control.
 - (2) Failure of system by missile.
 - (3) Structural failure of cover cooling system.
 - b. Cooling system capacity exceeded
 - (1) Inadequate design margins.
 - (2) Thermal insulation failure.
 - (3) Abnormal reactor heat load.
2. Possible protection (protects against):
 - a. Scram or runback (all).
3. Possible monitored variables (senses):
 - a. Cooling system parameters (all).
4. Possible engineered safety features (mitigates results of):
 - a. Overdesign (all).
 - b. Cooling system redundancy (a).
 - c. Missile shield for cooling system (a-2).

7. Abnormal Force on Primary Tank Cover

1. Possible causes:
 - a. High pressure in primary tank*8
 - b. High seismic forces
 - c. Abnormal thermal gradient
 - (1) Cover cooling system failure.
 - (2) Thermal insulation failure.
 - (3) Hot intermediate Na or NaK from DHRS on cover top.

- d. Impacting mass
 - (1) Large mass dropped on top of cover.
 - (2) Nuclear disassembly following large reactivity insertion*22, or molten fuel*12-Na vapor explosion generates missiles.
- 2. Possible protection (protects against):
 - a. Scram or setback (a, b, c, d-1).
- 3. Possible monitored variables (senses):
 - a. Primary tank pressure (a).
 - b. Seismic shock (b).
 - c. Temperatures (c).
 - d. Operator - sight and sound (d).
- 4. Possible engineered safety features (mitigates results of):
 - a. Missile barriers above and below cover (d).
 - b. Na or NaK drip shield (c-3).
 - c. Overdesign (all).

8. High Pressure in Primary Tank

- 1. Possible causes:
 - a. Na boiling
 - (1) Inadequate DHR capability*9.
 - (2) Heat generated from local recriticality after disassembly exceeds DHR capability.
 - b. Molten fuel*12-Na vapor explosion.
 - c. Nuclear disassembly following large reactivity insertion*22
- 2. Possible protection (protects against):
 - a. Separate, independent normal DHR systems (a-1).
- 3. Possible monitored variables (senses):
 - a. High temp or pressure in primary tank (all).
- 4. Possible engineered safety features (mitigates results of):
 - a. Emergency DHR system (a-2).
 - b. Emergency HP relief to Ar decay storage tank (all).
 - c. Designing to prevent recriticality (a-2).

9. Inadequate Decay Heat Removal Capability

- 1. Possible causes:
 - a. Inadequate thermal communication by natural convection between primary coolant in primary tank and the DHRS
 - b. Inadequate thermal communication between core and primary coolant in primary tank

- (1) Inadequate forced convection due to pump failure or flow blockage.
 - (2) Inadequate natural convection.
 - c. Total DHR failure
 - (1) Normal DHRS*10 failure.
 - (2) Emergency DHRS failure.
 - 2. Possible protection (protects against):
 - a. Design to enhance natural convection (a, b).
 - b. Redundant systems (b-1, c).
 - 3. Possible monitored variables (senses):
 - a. Temperatures (all).
 - b. Flows (all).
 - 4. Possible engineered safety features (mitigates results of):
 - a. Emergency cooling systems (all).
10. Failure of Normal Decay Heat Removal System
(requires failure of two independent systems)
- 1. Possible causes:
 - a. Loss of NaK in loop
 - (1) Pipe rupture.
 - (2) Na-NaK heat exchanger failure.
 - (3) Failure in NaK-air heat exchanger.
 - b. Low flow in normal DHR loop*11
 - c. Inadequate heat sink
 - (1) Tubes fouled on air side of heat exchanger.
 - (2) Fan failure.
 - (3) Variable air flow damper assembly failure.
 - d. Failure to actuate loop
 - e. NaK flow inadvertently switched to biological shield cooling coils
 - 2. Possible protection (protects against):
 - a. Redundant system or component (all).
 - 3. Possible monitored variables (senses):
 - a. Levels (a).
 - b. Flows (a-1, b, e).
 - c. Temperatures (all).
 - 4. Possible engineered safety features (mitigates results of):
 - a. Emergency cooling system (all).
 - b. Containment (all).

11. Low Flow in Normal Decay Heat Removal Loop

1. Possible causes:
 - a. Excessive pressure drop through loop
 - (1) Frozen NaK in NaK-air heat exchanger.
 - (2) Oxide deposits in tubing.
 - (3) Isolation or throttle valve closed.
 - (4) Pump discharge check valves fail to open (2 of 3 must fail).
 - b. Pump failure (2 of 3 must fail)
 - (1) Structural failure of pump.
 - (2) Winding, core, or stator failure.
 - (3) Loss of electrical power.
 - c. Incorrect alignment of valves in Na-NaK heat exchanger
2. Possible protection (protects against):
 - a. Redundant cooling system or component (all).
 - b. Overdesign (all).
3. Possible monitored variables (senses):
 - a. Temperatures (all).
 - b. Flows (all).
 - c. Valve position (a-3, a-4, c).
 - d. Pump power (all).
4. Possible engineered safety features (mitigates results of):
 - a. Emergency cooling systems (all).
 - b. Containment (all).

12. Molten Fuel

1. Possible causes:
 - a. Power transient following reactivity insertion*¹³
 - b. Non-neutronic void propagation from single assembly*¹⁵
 - c. Inadequate DHR capability*¹⁶
 - d. Overheating of a single assembly*¹⁴ followed by fuel melting
2. Possible protection (protects against):
 - a. Prevention at input level (all).
 - b. Decay heat cooling (all).
3. Possible monitored variables (senses):
 - a. Monitoring at input level (all).
4. Possible engineered safety features (mitigates results of):
 - a. Containment (all).
 - b. Emergency decay heat cooling (all).

13. Power Transient Following Reactivity Insertion

1. Possible causes:
 - a. Fuel movement to more reactive position
 - (1) Earthquake shock.
 - (2) Fuel assembly(s) bowing.
 - (3) Fuel assembly(s) movement.
 - (4) Collapse of ratcheted fuel.
 - b. Control rod withdrawal
 - (1) Single CR withdrawal at 1800"/min due to secondary motor failure.
 - (2) Withdrawal of up to 6 CRs at 15"/min due to control system or operator error.
 - c. Overheating*¹⁴ and voiding of a single assembly
2. Possible protection (protects against):
 - a. Single rod scram (b-1).
 - b. Scram (all).
 - c. Overdesign (a).
 - d. Prevention at input level (c).
3. Possible monitored variables (senses):
 - a. Flux-power range (all).
 - b. Positive or negative period - power, int. range (all).
 - c. Power/core flow ratio (all).
 - d. Seismic shock (a-1).
 - e. High source range count rate - source (a, b).
 - f. Power to CRD motors or shaft speed (b-1).
 - g. Reactivity (all).
 - h. Noise (all).
 - i. Rod position (b).
 - j. Assembly flow (c).

14. Overheating of a Single Assembly

1. Possible causes:
 - a. Misloaded fuel assembly
 - b. Inadequate primary coolant flow through affected assembly
 - (1) Debris or fission gas from failed fuel pin(s).
 - (2) Fuel pin(s) swelling or bowing.
 - (3) Flow blockage to assembly.
 - (4) Can wall failure.
 - (5) Fuel pin(s) spacer failure.
 - (6) Entrained cover gas bubbles in inlet coolant.
2. Possible protection (protects against):
 - a. Administrative procedures (a).
 - b. Different grapples required for each zone (a).
 - c. Keyed assemblies (a).

- d. Device to prevent flow blockage (b-3).
 - e. Limited burnup (b-2).
 - f. Overdesign (b-4, b-5).
 - g. Device to release entrained gases (b-6).
 - h. Canless assemblies (b).
 - i. Scram, setback, or rundown (all).
3. Possible monitored variables (senses):
- a. Assembly flow (all).
 - b. Assembly outlet temp (all).
 - c. Power tilt or local flux change (a).
 - d. Noise - if vapor bubble growth is slow (all).
 - e. Delayed neutron emitters in Na (a-1).

15. Non-Neutronic Void Propagation From a Single Assembly

1. Possible causes:
- a. Mechanical propagation
 - (1) Pressure pulse from flashing of superheated Na.
 - (2) Pressure pulse generated by molten fuel*12-Na vapor explosion.
 - b. Thermal void propagation
 - (1) Radial heat transfer causing boiling in adjacent assembly(s).
 - (2) Molten fuel*12 penetrates assembly wrapper can.
 - c. Na vapor bubble exiting from bottom of fuel assembly and entering adjacent assembly
2. Possible protection (protects against):
- a. Scram (all).
 - b. Thick assembly wrapper cans (a).
 - c. Refractory metal assembly wrapper cans (b-2).
 - d. Device to prevent backflow of bubble (c).
3. Possible monitored variables (senses):
- (See catalog 14.)

16. Inadequate Heat Removal Capability

1. Possible causes:
- a. Inadequate heat removal capability
 - (1) Cover gas bubbles entrained in primary coolant entering core.
 - (2) Inadequate primary coolant flow*17.
 - (3) High primary coolant temp entering core*20.
 - b. Primary coolant flow channels restricted by molten fuel*12-Na vapor explosion

2. Possible protection (protects against):
 - a. Thermal overdesign (all).
 - b. Thick assembly wrapper cans (b).
 - c. Setback (a).
 - d. Scram (a, b).
 - e. Primary pump inlet far enough below surface (a-1).
 - f. Device to release entrained gases (a-1).
 - g. Protection at input level (a-2, a-3, b).
3. Possible monitored variables (senses):
 - a. Core pressure drop (a-2).
 - b. High inlet temperature (a-3).
 - c. Noise (a-1, b).
 - d. Cover gas pressure (b).
 - e. Monitoring at input level (a-2, a-3, b).

17. Inadequate Primary Coolant Flow

1. Possible causes:
 - a. Bypass flow due to structural failure
 - (1) Major core vessel rupture.
 - (2) Major rupture of pump impeller housing.
 - (3) Major failure of seal between pump discharge and inlet pipes.
 - (4) Major primary inlet piping failure.
 - b. Primary pump malfunction^{*18}
 - c. Improper control of primary pumps
 - d. Flow blockage
 - (1) Pump inlet restriction.
 - (2) Primary inlet piping restriction.
 - e. Loss of electrical power to a primary pump^{*19}(all six)
2. Possible protection (protects against):
 - a. Scram or setback (all).
 - b. Standby pumps (b, c, d).
 - c. Device to prevent pump inlet blockage (d-1).
 - d. Hydraulic overdesign (all).
 - e. Mechanical overdesign (a).
3. Possible monitored variables (senses):
 - a. Primary coolant flow/core ΔP (all).
 - b. Power to primary pump (all).
 - c. Power/core flow ratio (all).
 - d. Loss of plant normal electrical power (d).

18. Primary Pump Malfunction

1. Possible causes:
 - a. Failure to deliver rated flow and head
 - (1) Rupture of pump impeller housing.
 - (2) Failure of seal between pump discharge and inlet.
 - b. Failure of primary pump drive motor
 - (1) Mechanical or electrical failure.
 - (2) Loss of electrical power to primary pump*19.
 - c. Failure of eddy-current coupling
 - (1) Mechanical or electrical failure.
 - (2) Loss of electrical power.
 - (3) Excessive slippage.
 - d. Shaft bearing seizure or impeller failure
 - e. Control system malfunction
2. Possible protection (protects against):
 - a. Fast setback (all).
 - b. Scram (all).
 - c. Guaranteed noninterruptible power source (c-2).
 - d. Energize pony motors—power must be reduced (b).
4. Possible monitored variables (senses):
 - a. Shaft rotation (d).
 - b. Power to eddy-current coupling (c-1, c-2).
 - c. Pump outlet pressure (all).
 - d. Primary coolant flow—core ΔP (all).
 - e. Pump power (all).

19. Loss of Electrical Power to Primary Pump

1. Possible causes:
 - a. Motor failure
 - (1) Motor cooling system failure.
 - (2) High temp in SC.
 - (3) Motor overload.
 - (4) Insulation breakdown.
 - (5) Relay failure.
 - b. Failure of normal power supply
 - c. Operator or control system error
2. Possible protection (protects against):
 - a. Scram or setback (all).
3. Possible monitored variables (senses):
 - a. Motor temp (a-1, a-2, a-3).
 - b. Power monitor (a, b).

20. High-Temperature Primary Coolant Entering Core

1. Possible causes:
 - a. Primary coolant flowing from outlet plenum to primary tank, by-passing IHX
 - (1) Leakage through fuel transfer ports.
 - (2) Structural failure of shield tank.
 - (3) Overflow over top of shield tank.
 - (4) Failure of IHX shutoff valve to close with IHX inoperative.
 - b. Loss of access to heat sink* 21
2. Possible protection (protects against):
 - a. Keep fuel transfer hole areas small (a-1).
 - b. Scram or setback (all).
 - c. Postshutdown cooling (b).
3. Possible monitored variables (senses):
 - a. Primary tank Na temp at pump inlets (all).
 - b. Device to sense overflow (a-3).
 - c. Na level (a).
 - d. IHX temp (all).
4. Possible engineered safety features (mitigates results of):
 - a. Structural overdesign (a-2).

21. Loss of Access to Heat Sink

1. Possible causes:
 - a. Loss of power to all intermediate pumps
 - b. Loss of flow in one intermediate loop
 - (1) Pipe rupture.
 - (2) Flow restriction.
 - (3) Loss of intermediate pump.
 - (4) Inadvertent Na dumping.
 - c. Increase in cold leg temp of intermediate loop
 - (1) Intermediate system throttle valve malfunction.
 - (2) Reheater malfunction.
 - (3) Steam generator malfunction.
 - d. Inadequate flow in IHX
 - (1) Structural failure of IHX shell or baffles.
 - (2) Internal flow obstruction.
 - (3) Malfunction in IHX shutoff valve.
 - (4) IHX malfunction.
2. Possible protection (protects against):
 - a. Scram or setback (all).
 - b. Postshutdown cooling (all).

3. Possible monitored variables (senses):
 - a. Loss of plant normal electrical power (a).
 - b. Power to intermediate pumps (a, b).
 - c. Intermediate coolant flow – each loop (a, b, d).
 - d. Cold leg temp in intermediate loop (all).
 - e. Valve position (a-4, c-1, d-3).

22. Nuclear Disassembly Following Large Reactivity Insertion

1. Possible causes:
 - a. Molten fuel^{*12} in gross amounts with slumping to more reactive configuration
 - b. Gross Na boiling in region of high positive worth
 - (1) Power transient following reactivity insertion^{*13}.
 - (2) Inadequate heat removal capability^{*16}.
 - c. Core compacted to more reactive configuration by molten fuel^{*12}-Na vapor explosion
 - d. Non-neutronic void propagation from single assembly^{*15}
2. Possible protection (protects against):
 - a. Scram (all).
 - b. Fuel spacers (a).
 - c. Thick fuel assembly wrapper cans (c, d).
3. Possible monitored variables (senses):
 - a. Power range level and rate (all).
 - b. Primary coolant core outlet temp (a, b).
 - c. Fuel assembly outlet temp (a, b, d).
 - d. Noise (b, c, d).

23. Reactivity in Secondary Containment

1. Possible causes:
 - a. R/A released from intermediate coolant or DHRS
 - (1) Structural failure of interface with primary coolant.
and
 - (2) Structural failure of system piping.
 - b. R/A released from rad waste disposal system
 - (1) Structural failure.
 - (2) Seal leakage.
 - c. R/A released from support system
 - d. R/A released from reactor coolant system
 - (1) Structural failure in reactor blanket gas subsystem.
 - (2) Structural failure in radioactive Na storage subsystem.
 - (3) Structural failure of Na purification subsystem.

- e. R/A released from CR drives
 - (1) Dynamic seal leakage.
 - and
 - (2) Structural failure of housing or housing seals.
- f. R/A released from primary tank cover
 - (1) Breach in primary tank cover*⁵.
 - (2) Seal leakage.
- g. R/A released from primary tank cavity
 - (1) Breach in primary tank*²⁴.
 - and
 - (2) Breach in cavity boundary*²⁷.
- 2. Possible protection (protects against):
None at present.
- 3. Possible monitored variables (senses):
a. Radiation (all).
- 4. Possible engineered safety features (mitigates results of):
a. Containment isolation (all).
b. Isolation valves (a - d).
c. Administrative procedures (b, c).
d. Shielding for CR drives (e).
e. Machinery dome (d - g).

24. Breach in Primary Tank

- 1. Possible causes:
 - a. Structural inadequacy*³
 - b. Melt-through of primary tank by molten fuel
 - (1) Molten fuel*¹² in gross amounts...
 - and
 - (2) Melt-through of meltdown pan and core vessel.
 - c. Abnormal force on primary tank*²⁵
- 2. Possible protection (protects against):
None at present.
- 3. Possible monitored variables (senses):
a. Primary tank temp (b).
b. Primary tank pressure (c).
c. Na in cavity (all).
- 4. Possible engineered safety features (mitigates results of):
a. Meltdown pan (b).
b. Containment isolation (all).
c. Cooling (b).
d. Inspection procedures (a).

25. Abnormal Force on Primary Tank

1. Possible causes:
 - a. High pressure in primary tank*8
 - b. High seismic forces
 - c. Abnormal thermal gradient
 - (1) IHX malfunction *26.
 - (2) Failure of vessel guard.
 - (3) Structural failure of shield tank.
 - d. Missiles in primary tank
 - (1) Molten fuel*12-Na vapor explosion.
 - (2) Nuclear disassembly following large reactivity insertion*22.
2. Possible protection (protects against):
 - a. Scram (a, b, c).
3. Possible monitored variables (senses):
 - a. Primary tank and cavity temp (c).
 - b. Primary tank pressure (a).
 - c. Seismic forces (b).
4. Possible engineered safety features (mitigates results of):
 - a. Containment isolation (all).
 - b. Missile barrier (d).

26. IHX Malfunction

1. Possible causes:
 - a. Failure of IHX bypass flow restriction
 - b. Structural failure
 - c. Loss of access to heat sink*21
 - d. IHX shutoff valve malfunction
 - (1) Structural failure.
 - (2) Drive failure.
 - (3) Operator error.
2. Possible protection (protects against):
 - a. Scram or setback (all).
3. Possible monitored variables (senses):
 - a. Temperature — especially intermediate cold leg or IHX outlet (all).
 - b. Flow (a, d).
 - c. Valve position (d).

27. Breach in Cavity Boundary

1. Possible causes:
 - a. Structural inadequacy*³
 - b. Melt-through of cavity liner by molten fuel
 - (1) Melt-through of primary tank.
and
 - (2) Insufficient cooling of cavity liner.
 - c. High temp in cavity
 - (1) Inadequate heat removal by closed loop Ar cooling subsystem.
 - (2) Excessive heat source.
 - d. Abnormal force on cavity boundary*²⁸
 - e. Failure of cover structure peripheral seal
 - f. Breach in Ar cooling system
2. Possible protection (protects against):
 - a. Scram or setback (c - f).
3. Possible monitored variables (senses):
 - a. Cavity temp (c).
 - b. Periodic leak tests (a, e, f).
 - c. Na in cavity (b).
4. Possible engineered safety features (mitigates results of):
 - a. Meltdown pan in cavity (b).
 - b. Redundancy (e, f).
 - c. Overdesign (a, d).
 - d. Tests (e, f).

28. Abnormal Force on Cavity

1. Possible causes:
 - a. Missiles generated by molten fuel*¹²-Na vapor explosion or nuclear disassembly following large reactivity insertion*²²
 - b. High seismic forces
 - c. Abnormal thermal gradient
 - (1) Closed loop Ar cooling system malfunction.
 - (2) Breach in primary tank*²⁴ releasing hot Na.
 - d. High pressure in cavity
 - (1) Breach in primary tank*²⁴.
and
 - (2) High pressure in primary tank*⁸.

2. Possible protection (protects against):
 - a. Scram or setback (b, c, d).
3. Possible monitored variables (senses):
 - a. Pressure in cavity (d).
 - b. Temp in cavity (c).
 - c. Seismic shock (b).
4. Possible engineered safety features (mitigates results of):
 - a. Containment isolation (all).
 - b. Missile barrier (a).
 - c. Thermal shield (c).
 - d. Cavity cooling (c).
 - e. Overdesign (b, c, d).

4. FAULT TREE DIAGRAMS

4.1. General

During Phase I, fault tree diagrams were generated to display the basic faults and show in graphic form the causes and interrelationships of failure events that could lead to core damage and, ultimately, to the release of radioactivity to the environment. The fault trees also display the principal fault paths and indicate the interfaces of systems and components within systems with respect to fault propagation.

These fault trees are qualitative in that no probabilities are assigned to the different basic failures and failure events. However, they are constructed in enough detail to allow assessment of the sequence of basic failures and failure events along the fault paths; to permit the identification of critical failures that might lead to major accidents; and to indicate where protective action, passive protective devices, and engineered safety features might be utilized.

4.2. Fault Tree Presentation

Fault tree diagrams are presented in Appendix A of this report and are numbered Figures A-1 through A-14. Figure A-1, "Radioactivity Release to the Environment in Excess of 10 CFR 100 Limits," is designated as the top of the overall tree; the remaining individual fault trees form its numerous fault branches. These individual fault trees are arranged in Appendix A by figure number in an order that diagrams the sequence and flow of the various possible initiating mechanical and structural basic failures or operational errors that can result in this type of accident.

Forming the base of the individual fault tree are the undeveloped basic failures or operator errors, e.g., loss of power, pipe rupture, etc., that can affect the safe and reliable operation of the reactor. These basic failures are diagrammed to show their possible results and influence on an operating system variable or a major component. If the

affected variable or component is monitored by the protection system, the fault trees denote the demand signal and the type of protective action that would be initiated to prevent propagation of the event. When this occurs, the trees incorporate an "And Gate" in the diagram indicating that coexistence of a protective system failure is required to produce the output event. This method of diagramming the individual fault trees is continued up the tree until the causal failure events terminate at the top in a single primary failure event. A numbered transfer symbol indicates that this information serves as input for one or more of the preceding fault trees. In addition, the individual fault trees may contain one or more subfault trees that provide input to other events occurring within the individual tree itself or transfer to another individual tree.

The triangular transfer symbol is used in two different ways in the fault tree diagrams. For the subfault trees, which are transferred within a fault tree or to another tree, the transfer symbol is located immediately below the culminating failure event on the subfault tree. For fault trees, the transfer symbol is immediately above the failure event at the top of the tree. In each case the description of the failure event to be transferred is repeated in a block immediately above the transfer symbol.

The fault trees utilize the standard fault tree nomenclature given by C. W. Griffin.* Figure 4-1 shows the standard fault tree symbols and defines their usage, and Table 4-1 is an index of the fault trees.

4.3. Fault Tree Summaries

The fault trees are summarized verbally in this section. In each case, key failures are indicated and the important fault paths are identified. The fault trees listed in Table 4-1 are all summarized, and the number of the summary paragraph corresponds to the figure number of the fault tree. Thus, summary 4.3.1 describes Figure A-1, summary 4.3.2 describes Figure A-2, etc. In the summaries the term "basic failure" indicates an undeveloped fault or malfunction, whereas a "failure event" is the result of one or more failures.

- - - - -

* Griffin, C. W., "Introducing the Fault Tree as a Tool for Nuclear Safety Analysis," Trans. ANS, Vol 9, No. 1, pp 157-159, June 1966.

4.3.1. Radioactivity Release to the Environment in Excess of 10 CFR 100 Limits

Four fault paths can lead to the primary failure event that heads this fault tree. Three of these paths involve the release of radioactivity (R/A) from systems which are, in part, outside the secondary containment. These are external support systems (spent fuel shipping and decontamination), the rad waste disposal system, and the intermediate coolant and decay heat removal systems. In the last of these three fault paths, the interface between the affected system and the primary coolant must also fail to cause the release of significant quantities of radioactive materials. Figure 4-3 illustrates this interface.

The fourth—and most important—fault path involves the release of radioactive materials from the secondary containment (see Figure 4-2). To cause such a release of R/A, the material must be present and the secondary containment or isolation components must have failed. These failures are described in sections 4.3.2 and 4.3.3, respectively.

Radioactive material can reach the secondary containment from the intermediate coolant or decay heat removal systems, the rad waste disposal system, and the support systems (Figure 4-6). In addition, failures in the reactor coolant system or in the reactivity control system drives can release fission gas, cover gas, and sodium to the the secondary containment. The most likely and potentially the most serious paths for the release of R/A to the secondary containment are through structural or seal failures in the primary tank cover or from the primary tank cavity (Figures 4-4 and 4-5). Leakage from the cavity can occur only after failure of the primary tank and the cavity boundary, both of which are described in subsequent sections.

4.3.2. Structural Failure of the Secondary Containment

Any one of four fault paths can cause the primary failure event that heads this fault tree. The first, structural inadequacy, implies that normal operating conditions may cause failure. Contributing factors include inadequate safety factors, faulty materials or poor workmanship not detected during inspection and testing, or deterioration

of the structure (possibly due to excessive corrosion or insufficient corrosion allowance). A large sodium or NaK fire could damage and ultimately rupture the containment liner. Similarly, molten fuel in contact with the liner where cooling is inadequate could melt through it.

The fourth and most complex of the fault paths leading to structural failure of the secondary containment is the application of abnormal force to the containment. Such force(s) can be created by acts of nature, missiles generated within the primary containment, equipment impacting against the inside of the containment, vehicles impacting against the outside, explosions, or thermal stress.

The containment could also be caused to fail by high internal pressure from a large liquid-metal fire in the primary tank (following failure of its cover) or in the secondary containment itself (as spray or pool burning after the release of primary or intermediate sodium or NaK). An inert containment atmosphere or one with a reduced oxygen concentration will prevent or reduce the severity of fires.

4.3.3. Failure of Containment Isolation Components

This primary failure event can result from either of two basic failures involving penetrations or from either of two fault paths. The first fault path, failure of ventilation system isolation valves, may occur if a valve fails or is not actuated. The second path involves failure of both personnel airlock doors, which can be a result of seal failure or failure of the interlock system to ensure that both doors are closed. These components are shown in Figure 4-2.

4.3.4. Structural Breach in Primary Tank Cover

Three fault paths can lead to this primary failure event; the first, structural inadequacy, is discussed in paragraph 4.3.2. The second fault path involves high temperatures, which can weaken the cover to the point of failure under normal loads. The two major branches of this fault path are abnormal heat sources and inadequate cover heat removal. The first includes such heat sources as a sodium or NaK fire in the secondary containment or abnormal reactor heat loads. Heat removal from the cover could be inadequate if the cooling system capacity

were exceeded or if it did not perform adequately. The latter can result from system failure, e.g., by missiles or improper system control.

The application of excessive forces can also cause the cover to fail. Abnormal force can result from several effects:

1. High pressure in the primary tank (see paragraph 4.3.8).
2. High seismic forces.
3. Abnormal thermal gradients (such as might result from the destruction of thermal insulation or the presence of hot sodium or NaK on the cover).
4. An impacting mass (such as a large object or a missile generated in the tank).

Figure 4-4 is a sketch of the primary tank cover.

4.3.5. Seal Leakage

Seal leakage may be a result of either of two fault paths. The first, seal or seal seat failure, entails the loss of seal purging gas pressure and the failure of both seals. The second fault path, failure of the retention device, can be caused by an abnormal force or by structural inadequacy.

4.3.6. Breach in the Primary Tank

This primary failure event can occur as a result of any of three fault paths: structural inadequacy, melt-through of the tank by molten fuel, or abnormal forces on the tank.

Structural inadequacy can result from deterioration, faulty materials or fabrication, or inadequate safety factors.

Molten fuel must be present and in contact with the tank to cause melt-through. To enable the presence of molten fuel, the core must have melted and penetrated the meltdown pan and core vessel; this can be prevented by adequate cooling of the intervening barriers.

Abnormal forces on the primary tank can be caused by high pressure in the tank, seismic forces, abnormal thermal gradients, or missiles generated by violent core disruption.

Figure 4-5 shows the location of the primary tank in relation to the primary tank cavity.

4.3.7. Breach in Cavity Liner

Four fault paths can cause this primary failure event. Structural inadequacy, the first of these, is described in paragraph 4.3.2. The second fault path, liner melt-through, requires molten fuel in contact with the liner and inadequate liner cooling.

High temperatures are the result of the third fault path leading to a breach in the cavity liner. Two failure events are required to produce such temperatures: a heat source and inadequate heat removal. These events are in turn the products of basic failures.

The last fault path terminates in abnormal forces, which can result from an impacting mass such as a missile, high seismic forces, abnormal thermal gradients, or high pressure within the cavity. These events are all products of basic failures and causal failure events.

The primary tank cavity is illustrated in Figure 4-5.

4.3.8. High Pressure in Primary Tank

Three fault paths — sodium boiling, a sodium-molten fuel vapor explosion, and nuclear disassembly — can lead to high pressure in the primary tank.

Sodium boiling will not produce the violent pressure pulses that might characterize the other two fault paths. Nevertheless, it is important because it could cause failure of the primary containment and force radioactive material through the break(s). Two key failure events could contribute to sodium boiling. If recriticality should occur after core disassembly, the heat removal capability of the decay heat removal system could be exceeded. Inadequate decay heat removal capability under normal decay heat loads could also cause sodium boiling. This inadequacy can result from failure of the normal and emergency decay heat removal systems or from inadequate thermal communication between the fuel and the decay heat removal systems.

A sodium-molten fuel vapor explosion can occur only if large quantities of fuel have melted in the absence of sodium, and the sodium has returned. Gross fuel melting can result from (1) a power transient following a reactivity insertion or (2) inadequate heat removal, both of which are protected against by scrams, or from (3) extensive void propagation, which may or may not be slow enough to be prevented

by a scram. Fuel movement, absorber movement, or the voiding of a single assembly can all cause power transients. Similarly, inadequate flow of primary coolant or the entry of high-temperature primary coolant into the core are failure events that can lead to inadequate heat removal capability. Extensive void propagation implies the non-neutronic propagation of a void from a single assembly to adjacent ones with the consequent loss of heat transport away from the fuel.

Nuclear disassembly is the violent disruption of the core by a power transient which is fast enough and large enough to vaporize significant amounts of fuel, steel, and sodium. For disassembly to occur, a large reactivity insertion is required. Gross sodium voiding which can be caused by extensive void propagation, a slow power transient, or a high sodium outlet temperature can result in very large reactivity insertions. If void propagation is slow enough, protective action can prevent its becoming excessive. A power transient and high sodium outlet temperature can be prevented by scram.

Another possible source of a large reactivity insertion is the gross compaction of fuel to a more reactive configuration. This may result from fuel slumping following gross melting or from compaction by a sodium vapor-molten fuel explosion.

4.3.9. High-Temperature Primary Coolant Entering the Core

This primary failure event can be caused by four fault paths: one involves the primary coolant's by-passing the IHXs and three (plus one basic failure) are concerned with conditions in and beyond the intermediate loops. Primary coolant can by-pass the IHXs by leaking through the fuel transfer ports, by passing through a breach in the shield tank, by overflowing the top of the shield tank, or by flowing through an inoperative IHX.

Flow in the intermediate loops can be reduced by one or more pumps losing electrical power or by flow restrictions or structural failures within the loop(s) or the IHX(s). The cold leg temperature in the intermediate loops will increase if failures occur in the steam generators, reheaters, or bypass valves.

4.3.10. Inadequate Primary Coolant Flow

This primary failure event, which is protected against by a scram, can result from any one of four basic failures in the primary coolant structure or from one of four fault paths. The fault paths are loss of electrical power to all six primary pumps (which is protected against by scram), flow blockage to or from the pump(s), improper control of the pumps, and primary pump malfunction (which is protected against by a fast setback).

The first three of these fault paths are relatively simple and require little explanation, but primary pump malfunction can be caused by any one of five failure events. Two of these events involve mechanical failure of the pump impeller or drive shaft, and two result in loss of the power train that drives the pump. The latter two events are failure of the primary pump drive motor and of the eddy-current coupling, either of which can fail due to loss of electrical power or mechanical or electrical failure. (It should be noted that the reference design utilizes eddy-current couplings powered by a guaranteed non-interruptible power supply.) The fifth failure event that could lead to primary pump malfunction is a reduction in pumping head.

4.3.11. Failure of the Normal Decay Heat Removal System

Two independent normal DHR systems must fail simultaneously to produce this primary failure event. The failure of both loops would follow essentially the same path; hence, for this summary the failure of a single loop will be treated as a primary failure event. The four failure events that feed into this primary event, then, are the termination points of fault paths.

Loss of flow in the loop is the first fault path; it is caused by several basic failures involving ruptures in various loop components and a consequent loss of NaK. The second fault path, low flow in the loop, can result from excessive loop pressure drop due to frozen NaK in the system, from oxide deposits in the loop, from valve failure, or from inadequate pump discharge. The third fault path, inadequate heat sink, is the result of failures involving the NaK-air heat exchanger; included are tube fouling, blower failure, and failure of the variable air

flow damper assembly. The final fault path is failure to actuate the system; to cause this, both the operator and the protection system must fail.

4.3.12. Rundown Failure

Rundown is a protective action in which up to six control rods are inserted at shim speed until the reactor reaches a predetermined power level. Failure of this action can be caused by failure of the rods to move in on signal, insufficient rod worth or excessive time delay, or failure of the protection system to provide a rundown signal. There are three rundown signals.

4.3.13. Scram Failure

Scram failure can be caused by (1) failure of the control rods to enter the core following a scram signal due to failure of the magnetic coupling to release or to distortion of the core, (2) ineffective scram due to excessive time delay or insufficient rod worth, or (3) failure of the protection system to provide a signal. Ten scram input signals are used.

4.3.14. Fast Setback Failure

This fault tree is similar to 4.3.13 except that it depends on the control rod drive motor to cause insertion at fast follow-in speed (1800 in. per minute) rather than on the magnetic coupling. Setback signals are provided by less severe failures than those which call for scram.

4.4. Pictorial Aids

Figures 4-2 through 4-6 are included to help the user of the fault categories or fault tree diagrams to locate and identify some of the complicated system or component failures. They are simplified engineering sketches showing only the information required to establish the component location, boundary conditions, and failure sequence. The sketches are described briefly below:

Figure 4-2 — This sketch shows the leak paths that can result from structural, seal, or valve failures inside or outside the secondary containment and, as a consequence, permit radioactive leakage to the environment.

Figure 4-3—This sketch shows the location of the components, the boundary conditions, and the failure sequences that must occur before R/A is released to the environment from these systems. The order in which the failures occur is indicated by number.

Figure 4-4—Shown in this sketch are the structural or seal failures that must occur before R/A is released through the primary tank cover into the secondary containment.

Figure 4-5—This sketch identifies the primary tank cavity boundary and the failure sequence that must occur before R/A from the cavity is released to the secondary containment. The failure sequence is indicated by number.

Figure 4-6—This sketch shows the location of the components, the boundary conditions, and the failure sequences that must occur before R/A is released to the secondary containment from these systems. The failure sequence is indicated by number.

Table 4-1. Index of Fault Tree Diagrams

<u>Fault tree title</u>	<u>Diagram figure No.</u>
Radioactivity Release to the Environment in Excess of 10 CFR 100 Limits	A-1
Structural Failure of Secondary Containment	A-2
Failure of Containment Isolation Components	A-3
Structural Breach in Primary Tank Cover	A-4
Seal Leakage	A-5
Breach in Primary Tank	A-6
Breach in Cavity Liner	A-7
High Pressure in Primary Tank	A-8
High-Temperature Primary Coolant Entering Core	A-9
Inadequate Primary Coolant Flow	A-10
Failure of Normal Decay Heat Removal System	A-11
Rundown Failure	A-12
Scram Failure	A-13
Fast Setback Failure	A-14

Figure 4-1. Definition of Fault Tree Symbols

EVENT PRESENTATION:

The RECTANGLE identifies an event, usually a malfunction, that results from the combination of fault events through the logic gates.

The RECTANGLE is also used to describe conditional inputs to INHIBIT GATES. It indicates a condition that is presumed to exist for the life of the system. The CIRCLE describes a basic fault event that requires no further development. This category includes component failures whose frequency and mode of failure are derived through laboratory testing.

The DIAMOND describes a fault event that is considered basic in a given fault tree; however, the causes of the event have not been developed either because the event is an insufficient consequence or the necessary information is unavailable.

The OVAL is used to record the conditional input to an inhibit gate. It defines a state of the system that permits an event sequence to occur, and may be either normal to the system or be the result of equipment failures.

The HOUSE indicates an event that is normally expected to occur. For example, it may be used to represent the event, "Timing Pulses Present." (Used strictly for description, i.e., What is going on? .. in ground rules of effects.)

The TRIANGLES indicate transfer symbols. A line from the apex of the triangle denotes a transfer-in and a line from the side denotes a transfer-out. This refers to a whole sub-fault-tree repeated elsewhere.

LOGIC OPERATIONS

The AND Gate describes the logical operation whereby the coexistence of all input events is required to produce the output event.

The PRIORITY AND GATE performs the same logic function as the AND GATE, with the additional stipulation that sequence as well as coexistence is required.

The AND/OR GATE defines the situation whereby the output event will exist if any or all of the input events are present.

The INHIBIT GATES describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system that permits the fault sequence to occur, and may be either normal to the system or be the result of equipment failures.

Figure 4-2. Release of Radioactivity From Secondary Containment to the Environment

Figure 4-3. Release of Radioactivity From Intermediate Coolant or Decay Heat Removal System to the Environment

Figure 4-4. Release of Radioactivity Through Primary Tank Cover to Secondary Containment

Figure 4-5. Release of Radioactivity From Primary Tank Cavity to Secondary Containment

Figure 4-6. Release of Radioactivity From Intermediate Coolant or Decay Heat Removal System to Secondary Containment

APPENDIX A
Fault Trees

Index of Fault Tree Transfer Symbol Numbers

<u>Fault tree title</u>	<u>Transfer symbol</u>	<u>Diagram figure No.</u>	<u>Diagram used as input to these figures</u>
R/A release to the environment in excess of 10 CFR 100 limits	None	A-1	None
Structural failure of secondary containment	1	A-2	A-1
Failure of containment isolation components	2	A-3	A-1, 2
Structural breach in primary tank cover	3	A-4	A-1, 2
Seal leakage	4	A-5	A-1, 2, 3
Breach in primary tank	5	A-6	A-1, 7
Breach in cavity liner	6	A-7	A-1
High pressure in primary tank	7	A-8	A-2, 6, 7
High-temperature primary coolant entering core	8	A-9	A-8
Inadequate primary coolant flow	9	A-10	A-8
Failure of normal decay heat removal system	10	A-11	A-8
Sodium-molten fuel vapor explosion	11	A-8	A-2, 4, 6, 7, 8
Rundown failure	12	A-12	A-8
Scram failure	13	A-13	A-8, 9, 10
Fast setback failure	14	A-14	A-9, 10
Failure of first seal and/or seat	15	A-5	A-5
Structural inadequacy	16	A-2	A-4, 5, 6, 7
Inadequate heat removal capability	17	A-8	A-8
Inadequate heat sink for the IHX due to loss of flow	18	A-9	A-6
Inadequate heat sink for the IHX due to high temperature	19	A-9	A-6
Nuclear disassembly	20	A-8	A-2, 4, 6, 7, 8
Loss of flow in the loop	21	A-11	A-11

Fault tree title	Transfer symbol	Diagram figure No.	Diagram used as input to these figures
Low flow in the loop	22	A-11	A-11
Inadequate heat sink	23	A-11	A-11
Bearing failure	24	A-10	A-10
Shaft seizure	25	A-10	A-10
Insufficient or improper inspection	26	A-10	A-10
Failure of primary tank cover	27	A-2	A-2
Sodium or NaK released to secondary containment	28	A-2	A-2
Sodium or NaK fire in secondary containment	29	A-2	A-2, 4
Ground vehicle crashing into secondary containment	30	A-2	A-2
Melt-through of primary tank	31	A-6	A-7
NaK released from decay heat removal system	32	A-2	A-4
Sodium released from intermediate coolant systems	33	A-2	A-4
Cover cooling system failure	34	A-4	A-4
Melt-through of cavity liner	35	A-7	A-2
Gross fuel melting	36	A-8	A-6, 8
Power generation following core disassembly	37	A-8	A-6
Inadequate decay heat removal	38	A-8	A-6
Loss of electrical power	39	A-10	A-10
Single assembly voiding	40	A-8	A-8
Reactivity insertion	41	A-8	A-8
Extensive void propagation	42	A-8	A-8

Figure A-1. Radioactivity Release to Environment in Excess of 10 CFR 100 Limits

Figure A-2. Structural Failure of Secondary Containment

Figure A-3. Failure of Containment Isolation Components

Figure A-4. Structural Breach in Primary Tank Cover

Figure A-5. Seal Leakage

Figure A-6. Breach in Primary Tank

Figure A-7. Breach in Cavity Liner

1

Figure A-9. High-Temperature Primary Coolant Entering Core

Figure A-10. Inadequate Primary Coolant Flow

Figure A-11. Failure of Normal Decay Heat Removal System

Figure A-12. Rundown Failure

Figure A-13. Scram Failure

Figure A-14. Fast Setback Failure

APPENDIX B
Glossary

Basic failure—an undeveloped fault or malfunction.

Causal failure event—a failure event at the head of a subfault tree or fault catalog which serves as an input to another failure event by means of a transfer symbol.

Containment, primary—the system or complex immediately surrounding the primary system, which constitutes the first external barrier to the release of energy, missiles, and radioactivity. For this study the primary tank cover and the boundary of the primary tank cavity form the primary containment (see Figures 4-4 and 4-5).

Containment, secondary (SC)—the ultimate consequence-limiting barrier in protection of the public. For this study the reactor building forms the secondary containment (see Figure 4-2).

Control rod—an assembly containing neutron-absorbing material that is used to control the core power level.

Core—the active core plus the radial and axial blankets.

Core, active—the portion of the core that is initially fueled with plutonium.

DHRS—decay heat removal system.

Engineered safety features—systems or devices whose prime function is to mitigate and control the consequences of accidents that might otherwise endanger the public. The emphasis is on failures outside the core which are not likely to affect the core.

Engineered safety features actuation system—this system is similar to the protection system except that it generates trip signals associated with the actuation of engineered safety features.

Failure event—an intermediate event which is the termination of one or more sequences of initiating events.

Fast setback—a reactor trip comprising controlled insertion of all control rods except the safety rods; a fast setback need not terminate in a full shutdown.

Fault or malfunction—abnormal behavior or failure of components, systems, or reactor parts that may have safety significance.

Fault path—a fragment of a fault tree which terminates in a failure event immediately below the primary failure event heading the fault tree. The terminating failure event provides the name for the fault path.

HP—high pressure.

LP—low pressure.

Primary failure event—the failure event that heads a fault tree.

Protection—the act of preventing or limiting the extent of damage to the core; see "protective system or device."

Protection system—all electrical and mechanical devices and circuitry (from and including sensors to actuation device input terminals) involved in generating the trip signals that actuate the protective systems.

Protective system or device—a system or device capable of preventing or limiting the extent of core damage that might result from nuclear excursions or other accidents. It may be either active or passive.

R/A—radioactivity.

Reactor trip—a reduction of core power level initiated by the protection system and comprising the insertion of control rods into the core.

Regulating rods—control rods which are used to control the power level of the critical reactor.

Rundown—a reactor trip involving the controlled insertion of regulating rods, which reduces core power level at a rate commensurate with the normal maneuvering limits of the reactor plant; a rundown need not terminate in a full shutdown.

Safety rod—control rods which are fully withdrawn from the core during all operating modes except shutdown; they are capable of shutting down the core from any operating mode.

Scram—a maximum-capability reactor trip to accomplish complete and irreversible insertion of all control rods at the fastest possible speed.

Subfault tree—a fragment of a fault tree which culminates in a causal failure event.