11B

BNWL-874
UC-2

2 -
5-69

PRELIMINARY FAULT TREE ANALYSIS
FOR THE FFTF

May 1969

AEC RESEARCH &
DEVELOPMENT REPORT

ROUTE TO	P. R. NO.	LOCATION	FILED BY DATE
<i>Archives</i>	<i>60013</i>	<i>271-26</i>	<i>SEP 5 1969</i>
<i>M. L. Oliver</i>	<i>60982</i>	<i>202A</i>	<i>SEP 5 1969</i>

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

PACIFIC NORTHWEST LABORATORY

RICHLAND, WASHINGTON

operated by

BATTELLE MEMORIAL INSTITUTE

for the

UNITED STATES ATOMIC ENERGY COMMISSION UNDER CONTRACT AT(45-1)-1830

3 3679 00061 1626

BNWL-874

UC-2, General,
Miscellaneous,
and Progress Reports

PRELIMINARY FAULT TREE ANALYSIS FOR THE FFTF

By

M. A. McLaughlin

Systems Engineering Department
Physics and Engineering Division

May 1969

NOT REPRODUCED
DISTRIBUTION

BATTELLE MEMORIAL INSTITUTE
PACIFIC NORTHWEST LABORATORY
RICHLAND, WASHINGTON 99352

BNWL-874

Printed in the United States of America
Available from
Clearinghouse for Federal Scientific and Technical Information
National Bureau of Standards, U.S. Department of Commerce
Springfield, Virginia 22151
Price: Printed Copy \$3.00; Microfiche \$0.65

PRELIMINARY FAULT TREE ANALYSIS FOR THE FFTF

M. A. McLaughlin

ABSTRACT

A preliminary fault tree analysis for the Fast Flux Test Facility is presented. The fault tree is a logic diagram showing all ^{conceivable} ~~possible~~ failures leading to the FFTF postulated maximum accident, release of radioactivity outside the containment. Probabilities of occurrence of the failure sequences were not calculated due to the preliminary state of the system design. It is concluded that the design of the FFTF safety system meets the established criteria in that multiple simultaneous faults are required to allow anything more serious than a minor accident.

CONTENTS

ABSTRACT	iii
LIST OF FIGURES	vii
INTRODUCTION	1
SYSTEM SAFETY ANALYSIS	2
FAILURE MODE AND EFFECT ANALYSIS (FMEA)	3
FAULT TREE ANALYSIS	4
RESULTS	6
FFTF Fault Tree	6
Protective System Failure	7
RECOMMENDATIONS	8
REFERENCES	17
DISTRIBUTION	19

LIST OF FIGURES

1	Steps in Fault Tree Analysis	9
2	Definition of Symbols for Fault Tree Analysis	10
3	Fault Tree Analysis - FFTF Maximum Accident: Reactivity Insertion	11
4	Fault Tree Analysis - FFTF Maximum Accident: Power/Heat Removal Imbalance	12
5	Fault Tree Analysis - FFTF Maximum Accident: Radioactivity Release Outside Containment	14
6	FFTF System Fault Tree Structure	15
7	Fault Tree Analysis - FFTF Maximum Accident: Protective System Failure	16

PRELIMINARY FAULT TREE ANALYSIS FOR THE FFTF

M. A. McLaughlin

INTRODUCTION

This report presents a preliminary fault tree analysis of the Fast Flux Test Facility. It is preliminary because it is based on a conceptual system design, and therefore does not contain details related to system hardware required in a final analysis.

There are several reasons for publishing the fault tree at this time, in its preliminary form. The first purpose is to provide supporting data for maximum accident studies for the FFTF.⁽¹⁾ A second purpose is to illustrate the application of system safety analysis techniques to the FFTF.

When a complex system has been designed with careful attention to reliability in each stage of its development, it is a difficult task to identify the most probable causes or combinations of causes leading to a particular failure event in the system. Such a failure event may take many forms, depending on the type of system under study. In a missile system, for example, it may mean a premature launch, or a missed target. For this study, the undesired event has been defined as the release of radioactivity outside the FFTF containment. The fault tree is a logic tool used here to identify causes which may lead to release of radioactivity outside the containment. Maximum accident studies may then be based upon analysis of the various postulated failure sequences, followed by a determination of those yielding the maximum work energy release. The maximum accident, that accident determining the design criteria for the containment

system, is so chosen that no accident is expected to exceed its severity in terms of release of radionuclides to the environment.

SYSTEM SAFETY ANALYSIS

System Safety Analysis, a relatively new discipline in the study of system failures, was developed as a result of the extremely high reliability and safety requirements demanded by the aerospace industry. As aircraft and missile systems became increasingly complex and costly, the necessity of a new approach in finding and eliminating system faults at the design stage also became apparent. It was not practical any longer to follow the traditional cycle of design, build, test, and redesign. The result of this situation, therefore, was the development of the systems approach to safety.

During each phase of design, a system is examined from the safety standpoint. The effects of any failures on system operation are evaluated to determine the principal design defects requiring correction.

System Safety Analysis is not merely a new phrase used to describe the old techniques. It includes the important new tool of Fault Tree Analysis. A fault tree analysis considers an undesired failure event and traces back through the system to find all possible causes. It is not the only approach to safety analysis, however. Another method, known as Failure Mode and Effect Analysis, starts from the opposite direction. All possible failure modes of a component are identified, and the effects of these on system operation are evaluated.

A comprehensive summary of all the methods developed for analyzing system safety is not intended here. However, some additional explanation of Failure Mode and Effect Analysis is

given to show, principally, why this method was not chosen for the FFTF safety analysis.

FAILURE MODE AND EFFECT ANALYSIS (FMEA)

Failure or malfunction of each component is considered, in the failure mode and effect method, along with the mode of failure. For example, a valve may stick open or closed, or it may become partially restricted by debris in the system. Each of these occurrences is a failure mode. The effects of each type of failure are traced through the system, and the resulting effect on system performance is evaluated. FMEA is fairly straightforward, assuming the analyst knows the system thoroughly. However, there are some limitations to FMEA which should be noted.

1 Since only one failure mode and only one component are
normally considered at a time, some possibilities can be easily
2 overlooked. Also, it happens often that concurrent fail-
ures of more than one component can result in more serious
3 consequences than those for a single isolated failure. When
all combinations of components in a complex system must be
evaluated for all failure modes, the analysis becomes prohibi-
tive in scope. Even the consideration of single failures in
a very complex system can be an impractical job. For these
reasons, use of a fault tree in the safety analysis of the FFTF
system is preferable to the FMEA.

FAULT TREE ANALYSIS

The technique of Fault Tree Analysis was first developed at Bell Laboratories in 1962 and proved successful in the safety analysis of the Air Force Minuteman ICBM program.⁽²⁾ It is essentially a method for studying the probability of occurrence of certain undesired events. A fault tree study is a combination of logical design, symbolic logic, Boolean algebra, reliability analysis, and probability theory.

Fault tree studies are dependent, for completeness, upon access to complete source materials. Logic and schematic diagrams are required for preliminary analysis and failure analysis. Details of physical layout and operating and maintenance instructions must be known in determining all possible interactions between parts of a system and lengths of time possible for system faults to remain undetected. Figure 1 shows the sequence of steps required for a complete fault tree analysis.⁽²⁾ The solid lines indicate steps which are covered in the present analysis. The remaining items could not be completed due to the preliminary status of the FFTF system design. For example, system hardware has not yet been selected and, therefore, data are not available to calculate reliabilities of individual components or subsystems.

Two different techniques of fault tree analysis have been developed. The analysis may consider only primary failures, or may include secondary effects as well. A "primary" failure may be defined as one that occurs while the system or component is operating normally, that is, within its intended design function. On the other hand, a "secondary" failure occurs when the component fails because it is subjected to stresses outside its normal environment induced, for example, by failure of a related component.

If only primary failures are considered, construction of a fault tree is a fairly straightforward process. An undesired failure event is selected, and all the possible happenings which can contribute to the event are diagrammed in the form of a tree. The branches of the tree are developed downward to those independent component failures which will directly produce the failure event. Probabilities are determined for the independent events and, after developing a mathematical model, the probability of the undesired event can be computed and the most likely sequence leading to the undesired failure event can be identified.

When secondary failures are considered, the fault tree analysis becomes more complex. The interactions between failed components and the effects of multiple failures add an additional dimension to the analysis. The analysis continues beyond the component failure level to the point where the effect of all possible related component failures on each component has been diagrammed. Construction of the fault tree is the same for both analytical techniques. Only in analyzing the causes of component failure are the two techniques different.

The definitions of symbols used in a fault tree diagram are shown in Figure 2. Two types of symbols are defined. The rectangle and diamond, for example, are simply used to present a failure event, while others, such as the "and" gate, define the connecting logic for the fault tree. A set of mathematical relationships corresponding to the logic symbols in the diagram is used in developing a mathematical model of the fault tree. Haasl⁽³⁾ gives a complete treatment of this aspect of fault tree analysis.

RESULTS

FFTF FAULT TREE

The approach taken by PNL in evaluating the severity of the postulated maximum accident for the FFTF was to analyze various failure mechanisms and determine those failure sequences which would yield the maximum work energy release.⁽¹⁾ The postulated accident results in a nuclear excursion initiated by a hypothetical series of failures and terminated by explosive disassembly of the core. In order to investigate the course of events leading to such an accident, a system fault tree showing all the possible failure sequences which could lead to release of radioactivity outside the containment was constructed for the FFTF. Initial fault tree studies related to this work were performed by A. V. Campise of Atomics International.⁽⁴⁾

The fault tree was used to show all the failure mechanisms which could lead to the maximum accident.^{only} However, the magnitude of the work-energy release, not a function of fault tree analysis, had to be arrived at independently in each case. A fault tree would be used to establish the probability that each of the events would occur. However, the FFTF system hardware is not well enough defined at this stage of preliminary design to allow the determination of reliabilities for each of the subsystems. No attempt was made, therefore, to estimate, either on an absolute or on a relative basis, the occurrence probabilities of all the combinations of failure events.

The FFTF fault tree shows that core collapse and disassembly can be initiated by failure events leading to any one of the following:

- Large, rapid reactivity insertions
- Slow reactivity insertions with a simultaneous failure of the protective system.
- Gross loss of sodium flow.

The system fault tree is presented in three segments. Figure 3 shows the "Reactivity Insertion" sequences and Figure 4, the case of "Power/Heat Removal Imbalance." Figure 5, "Radio-activity Release Outside Containment," shows the possible sequence of events after a failure has progressed through the steps in either "Power/Heat Removal Imbalance" or "Reactivity Insertion." The way in which all three of the fault tree segments fit together to form the complete system fault tree is shown diagrammatically in Figure 6.

PROTECTIVE SYSTEM FAILURE

A separate fault tree was constructed for the FFTF protective system (Figure 7). Two distinct possibilities must be considered in assessing protective system failures. First, the protective system could fail with no serious consequences. The protective system fault tree does not, by itself, consider the consequences of any of the failures shown but simply displays the various modes of system failure.

A potentially more serious situation arises, however, if the protective system fails in conjunction with another failure. A fault allowed to progress beyond its original level of consequence could possibly result in a major accident.

Failures of the protective system are entered on the overall FFTF system fault tree in a number of locations. The various scram signal inputs to the protective system fault tree have been designated by a number. On the main system fault tree, wherever a protective system failure is shown as the result of "no scram signal," the particular scram signal input number is called out in order to enhance the usefulness of the fault tree for tracing the causes of any accidents in the system after it is operational.

The design safety criteria for the FFTF require a multiplicity of simultaneous faults to allow anything more serious than a minor accident. The consequences of a single unlikely fault, accompanied by an independent failure of a protective device, will be limited to a major accident. Two simultaneous and independent unlikely faults, or a single such fault along with failure of two protective devices, will have consequences limited to the level of a disruptive accident. The postulated maximum accident would require a multiplicity of failures representing an upper limit for a disruptive accident.

One of the primary objectives for the FFTF fault tree analysis has been to show that accidents severe enough to result in core disassembly would require simultaneous failures equivalent to those for a disruptive accident. An examination of the FFTF fault tree shows the conceptual design for the FFTF system to be consistent with the preceding design safety criteria adopted for the FFTF.

RECOMMENDATIONS

The FFTF fault tree is in a preliminary stage at this time because it is based on a conceptual system design. During the successive preliminary and final design phases for the FFTF, the fault tree should be expanded and revised to reflect the current status of the system design. More specific orientation to system hardware is needed to complete the study.

Expansion of the fault tree would take the form of a downward extension of each of the branches to the point where only individual component failures would be considered. Such information on the system logic, combined with reliabilities of individual components, would enable the probability of events leading to the postulated maximum accident to be calculated.

FIGURE 1. Steps in Fault Tree Analysis

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.

The DOUBLE DIAMOND is used in the simplification of the fault tree for numerical evaluation. The event described results from causes that have been developed but are not shown on a particular version of the fault tree.

LOGIC OPERATIONS

Output

Inputs

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

Output

Inputs

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.

Output

Inputs

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

Output

Inputs

The priority EXCLUSIVE OR GATE functions as an OR GATE with the restriction that specified inputs cannot co-exist.

Output

Input

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. It is represented by an oval if it describes a specific failure mode, or a rectangle if it describes a condition which may exist for the life of the system. It could contain probability numbers which are either inherent to the system or are functions of effects.

Input

FIGURE 2. Definition of Symbols for Fault Tree Analysis

FIGURE 3. Fault Tree Analysis - FTF Maximum Accident: Reactivity Insertion

BNWL-874

FIGURE 4. Fault Tree Analysis - FTF Maximum Accident: Power/Heat Removal Imbalance

13 & 14

FIGURE 6. FFTF System Fault Tree Structure

FIGURE 7. Fault Tree Analysis - FTFF Maximum Accident: Protective System Failure

REFERENCES

1. D. E. Simpson et al. Preliminary Analysis of Postulated Maximum Accidents for the FFTF, BNWL-760. Pacific Northwest Laboratory, Richland, Washington, November 1968.
2. A. B. Mearns. "Fault Tree Analysis: The Study of Unlikely Events in Complex Systems," System Safety Symposium. University of Washington and the Boeing Company, Seattle, Washington, June 1965.
3. D. F. Haasl. Advanced Concepts in Fault Tree Analysis, System Safety Symposium, University of Washington and the Boeing Company, Seattle, Washington, June 1965.
4. A. V. Campise. FFTF Maximum Energy Release Containment Study. Atomics International, May 1966.

DISTRIBUTION

No. of
Copies

OFFSITE

1	<u>AEC CHICAGO PATENT GROUP</u> G. H. Lee, Chief
30	<u>AEC Division of Reactor Development and Technology</u> M. Shaw, Director, RDT Asst Dir for Nuclear Safety Analysis & Evaluation Br, RDT:NS Environmental & Sanitary Engrg Br, RDT:NS Research & Development Br, RDT:NS Asst Dir for Plant Engrg, RDT Facilities Br, RDT:PE Components Br, RDT:PE Instrumentation & Control Br, RDT:PE Liquid Metal Systems Br, RDT:PE Asst Dir for Program Analysis, RDT Asst Dir for Project Mgmt, RDT Liquid Metals Projects Br, RDT:PM FFTF Project Manager, RDT:PM (3) Asst Dir for Reactor Engrg, RDT Control Mechanisms Br, RDT:RE Core Design Br, RDT:RE (2) Fuel Engineering Br, RDT:RE Fuel Handling Br, RDT:RE Reactor Vessels Br, RDT:RE Asst Dir for Reactor Tech, RDT Coolant Chemistry Br, RDT:RT Fuel Recycle Br, RDT:RT Fuels & Materials Br, RDT:RT Reactor Physics Br, RDT:RT Special Technology Br, RDT:RT Asst Dir for Engrg Standards, RDT
223	<u>AEC Division of Technical Information Extension</u>
1	<u>AEC Idaho Operations Office</u> <u>Nuclear Technology Division</u> C. W. Bills, Director
1	<u>AEC San Francisco Operations Office</u> <u>Director, Reactor Division</u>

No. of
Copies

✓ 4	<u>AEC Site Representatives</u> Argonne National Laboratory Atomics International Atomic Power Development Assoc. General Electric Co.
✓ 3	<u>Argonne National Laboratory</u> R. A. Jaross LMFBR Program Office N. J. Swanson
✓ 1	<u>Atomic Power Development Assoc.</u> Document Librarian
✓ 7	<u>Atomics International</u> D. J. Cockeram (5) Liquid Metal Information Center J. J. Droher (2)
✓ 2	<u>Babcock & Wilcox Co.</u> <u>Atomic Energy Division</u> S. H. Esleeck G. B. Garton
8	<u>Bechtel Corporation</u> J. J. Teachnor, Project Administrator, FFTF
✓ 1	<u>BNW Representative</u> N. A. Hill (ZPR III)
✓ 1	<u>Combustion Engineering</u> <u>1000 MWe Follow-On Study</u> W. P. Staker, Project Manager
✓ 5	<u>General Electric Co.</u> <u>Advanced Products Operation</u> Karl Cohen (3) Bertram Wolfe Nuclear Systems Programs D. H. Ahmann
✓ 2	<u>Gulf General Atomic Inc.</u> <u>General Atomic Division</u> D. Coburn

No. of
Copies

- ✓ 1 Idaho Nuclear Corporation
D. R. deBoisblanc
- ✓ 1 Oak Ridge National Laboratory
W. O. Harms
- ✓ 1 Stanford University
Nuclear Division
Division of Mechanical Engrg
R. Sher
- ✓ 1 United Nuclear Corporation
Research and Engineering Center
R. F. DeAngelis
- ✓ 10 Westinghouse Electric Corp
Atomic Power Division
Advanced Reactor Systems
J. C. R. Kelly (10)

ONSITE-HANFORD

- ✓ 1 AEC Chicago Patent Group
R. K. Sharp (Richland)
- ✓ 4 AEC RDT Site Representative
P. G. Holsted
- ✓ 3 AEC Richland Operations Office
J. M. Shivley (3)
- ✓ 3 Battelle Memorial Institute
- ✓ 1 Bechtel Corporation
D. H. Weiss (Richland)
- ✓ 1 Westinghouse Electric Corp.
R. Strzelecki (Richland)

No. of
Copies

72

Battelle-Northwest

W. G. Albert	P. L. Hofmann
J. M. Batch	E. M. Johnston
A. L. Bement	✓ B. Mann
D. C. Boyd	W. B. McDonald
C. P. Cabell	J. S. McMahon
J. J. Cadwell	M. A. McLaughlin (10)
A. C. Callen	M. H. Meuser
J. C. Cochran	J. M. Norris
D. L. Condotta	L. T. Pederson
G. M. Dalen	J. A. Perry
D. R. Doman	H. G. Powers
F. G. Dawson	J. M. Seehuus
E. A. Evans	D. E. Simpson
J. C. Fox	R. J. Squires
V. W. Gustafson	D. D. Stepnewski
F. C. Gronemeyer	N. G. Wittenbrock
J. P. Hale	FFTF Files (10)
K. M. Harmon	Technical Information (5)
R. A. Harvey (10)	Technical Publications (2)
	FFTF Technical Reports Office