

#21

Revision 1
12-10-80
1990F

INTERIM RELIABILITY EVALUATION PROGRAM
BROWNS FERRY TEAM FAULT TREE GUIDE

Milan E. Stewart

4.	Translation of system event into path events	10
5.	Enumerating component fault modes and interfacing events on conventional fault tree	12
6.	Basic fault events shown by code name only	15
7.	Abbreviated fault tree logic gates	19
8.	Required conditions incorporated as inverted inputs to AND gate	26
9.	Mutually exclusive conditions	28
10.	Classifying faults using the house	29
11.	System boundaries	40
12.	Typical two-train safety system	41
13.	Two-train system fault tree	42

TABLES

1.	Fault Summary	14
2.	Secondary Event Type Codes	24
3.	Common Cause Events on Fault Summary	33

INTERIM RELIABILITY EVALUATION PROGRAM
BROWNS FERRY TEAM FAULT TREE GUIDE

1. INTRODUCTION

Fault trees will be used to fault model systems in the Interim Reliability Evaluation Program (IREP). A modified and abbreviated version of the fault tree method is used to determine system failure probabilities where the system, in turn, is related to the overall public risks associated with the nuclear plant. Fault tree analysis is a systematic procedure used to identify and record the various combinations of component fault states that can result in a predefined, undesired state of a system. Unlike the familiar inductive method of first postulating a component failure mode and then determining its effect on the system, fault tree analysis is an opposite deductive approach whereby the analyst first defines an undesired system effect and then identifies all the component failure modes that can, by themselves or in combination with other component failure modes, produce that predefined system effect. A fault tree, as opposed to fault tree analysis, is a result of the fault tree analysis and is a graphic display of all the component fault modes and the combinatorial AND and OR logic that relates those fault modes to the predefined, undesired state of the system. It is a fault model of the system which, when expressed in its non-redundant Boolean form, can be used as a probabilistic model to determine a probability of the system failing in that predefined state, based on known, or easily computed, probability values for individual events shown on the tree. A complete treatise on fault trees is contained in the fault tree handbook¹.

This guide describes the abbreviated fault tree method to be used by the Browns Ferry team in IREP. To facilitate description and understanding of the abbreviated methodology, it is first necessary that the conventional approach be described briefly. Essentially, the abbreviated method is the same as the conventional method except that basic fault events are shown on the tree by code name only, and the basic event statements are shown in a fault summary table. A few rules are presented for handling other kinds of events, such as interfacing system events and common cause events, human

2. SYSTEM FAILURE DEFINITION AND UNDESIRED EVENT

Fault tree analysis begins with a statement of the undesired event. Embodied in that statement must be the conditions which constitute failure of the system. For example, the undesired event, "insufficient coolant flow through the reactor core when the reactor is generating heat" is considered. This event statement is a complete logic statement specifying the requirements for reactor coolant. If a fault tree were to be developed about the undesired event, the analyst would examine all systems, normal operating and emergency systems, which deliver coolant to the reactor vessel. The analyst may define a more restrictive undesired event, for example, "insufficient emergency coolant flow when normal flow is lost," for which a fault tree is developed for the auxiliary coolant systems only. In any case, the top event, including conditions, must be compatible with the event tree sequence for which it pertains.

The undesired event examples previously presented are stated rather generally which, in most cases, is perfectly acceptable. For example, the word "insufficient," implies that below some flow value, the system will have failed. Where redundancy has been provided, however, the generalized statement must be translated into a statement more specific in order to account for the redundant capabilities of the system. For example, the statement, "insufficient coolant flow . . . ," might be translated into the more specific statement, "less than two-pump coolant flow . . . ," where more than two pumps have been provided.

The fault tree will be developed about the selected undesired event, and only events which relate logically to the occurrence of that undesired event will be identified. Component failures that produce other undesired events (for example, inadvertent operation of the system) when loss of flow is of concern will not be identified unless the particular component failures relate to the occurrence of both undesired events.

The undesired event and all subsequent events shown on the fault tree are binary. That is, if the event, as stated, occurs, the system (or component, in more detailed parts of the tree) has failed; if the event does

3. FAULT TREE CONSTRUCTION

Once an undesired event has been defined, a fault tree can be constructed about that undesired event. To illustrate the procedure, a PWR high pressure injection system will be used as an example. First, the top tiers of the fault tree will be constructed using the conventional method; then, the tree will be restructured using an abbreviated approach.

Figure 1 is a simplified schematic of the high pressure injection system (HPIS). It is used to provide emergency coolant to the reactor vessel in the event of a small loss of coolant accident where the reactor coolant system (RCS) is not depressurized sufficiently for core flood or for low pressure coolant injection. The HPIS is initiated automatically by an engineered safeguards actuation system (ESAS) upon 1500 psig decreasing RCS pressure or 4 psig increasing containment pressure. Upon receipt of an ESAS signal, the three pumps start, refueling water storage tank (RWST) valve 6 opens (RWST valve 5 is normally open), and injection valves 1, 2, 3, and 4 open. All valves (not shown) in connecting piping are assumed to be closed for this example.

3.1 Conventional Fault Tree Construction

The undesired event selected for the HPIS must be compatible with the event tree sequence for which it applies. Suppose, for example, that a relief valve sticks open, heat removal through the power conversion system is lost, and it is incumbent upon the HPIS to provide emergency coolant to the reactor vessel. Suppose too, that one-pump HPIS flow through any path shown will suffice. An undesired, or top, event selected for the fault tree might be "less than one-pump HPIS flow to the reactor coolant system (RCS) given a stuck-open relief valve, no heat removal through the power conversion system." Other top events would have been selected for other accident initiators and sequences, but this will be the top event used to illustrate the method. Since the "given" part of the undesired event statement specifies the conditions under which the fault events to be defined by the fault tree produce system failure (see Section 8), the top undesired event, as shown in the top rectangle, Figure 2, is translated into the two

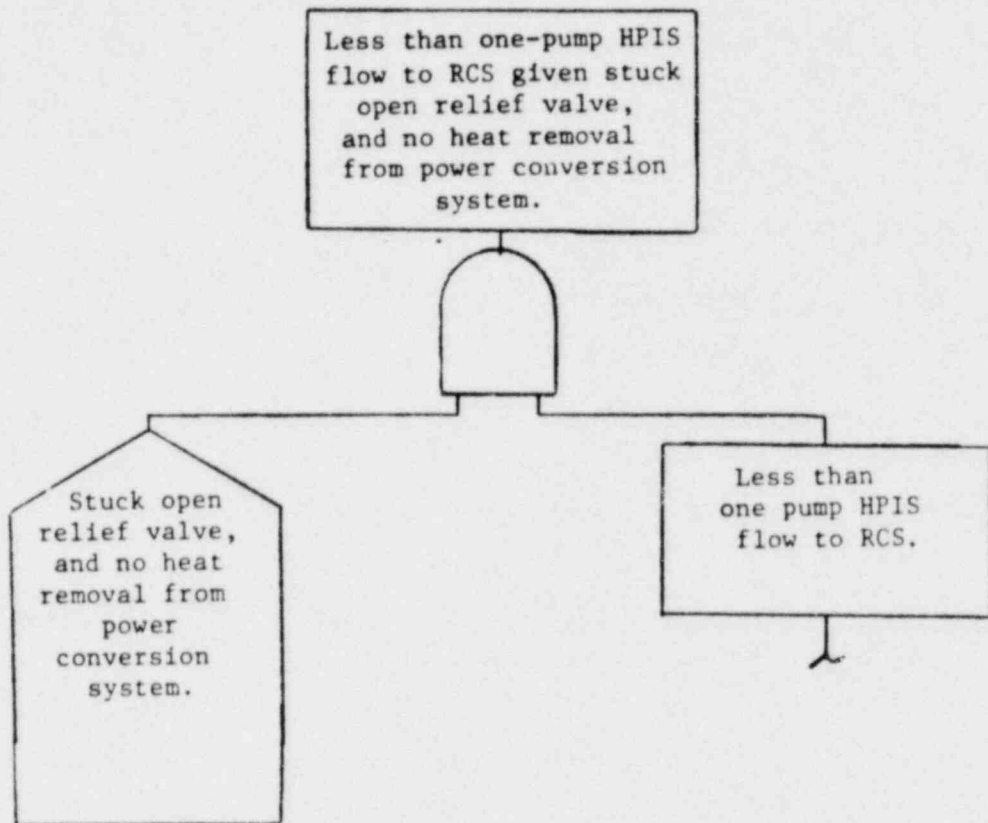


Figure 2
Top Two Fault Tree Tiers

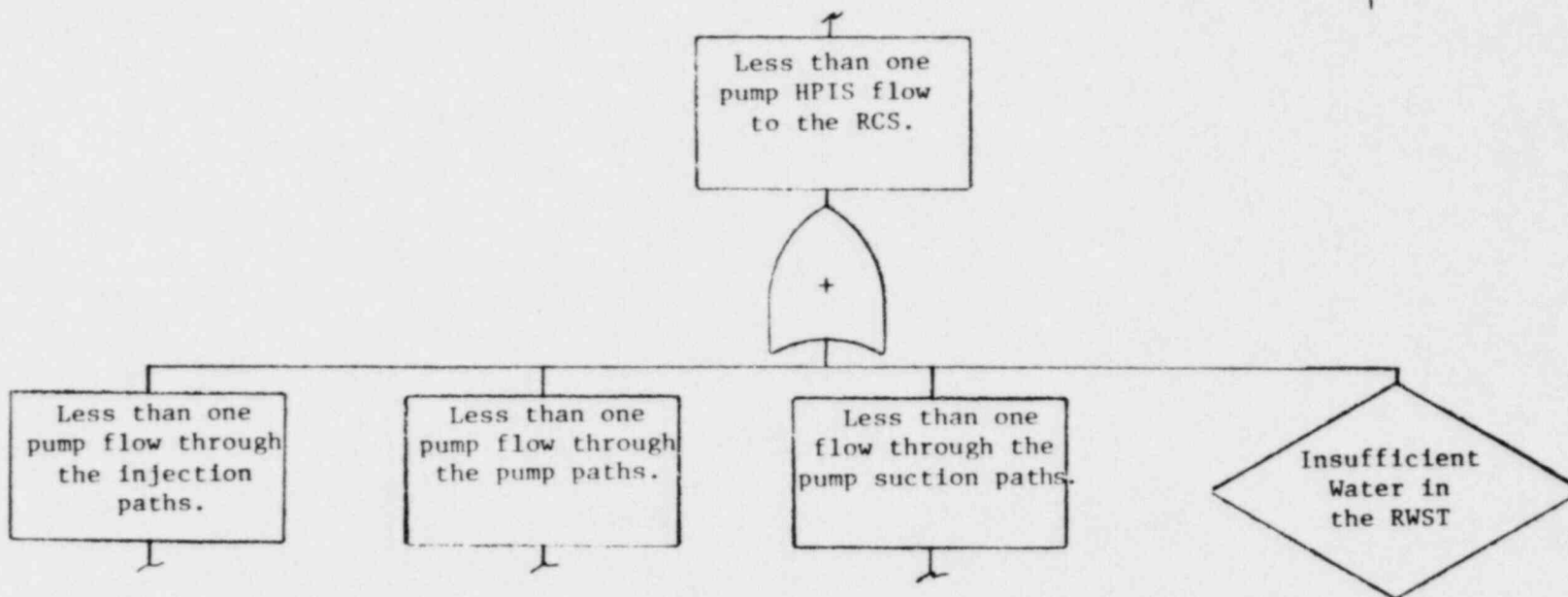


Figure 3
 Translation of System Event
 Into Subsystem Events

The development of the fault tree, thus far, has been a restatement of each event to increasing levels of resolution: from system, to subsystems, and to paths. The top logic for the fault tree has been established, and the next step is to enumerate all the component fault modes, as well as the fault modes of support systems which may interface with those individual path components. The top logic and the interfacing system events generally determine the degree of redundancy inherent in a particular safety system function. This is not always true, however, and the fault tree should be developed into the interfacing systems and into the control and power circuits to identify the more subtle, but important, contributions to risk. Also, some component fault modes will appear in more than one path, thus reducing redundancy for that particular fault mode. For example, rupture of any pipe downstream of the pumps and upstream of the injection valves (shown in Figure 1) will appear as faults in the fault tree development for each path. This is to say that when the fault tree is converted to its simplest Boolean form (see Section 9 below), the pipe rupture event will be a single fault. Knowing this is the case, the top fault tree logic could be changed to reflect pipe rupture as a single event.

Figure 5 shows the conventional method for enumerating component fault modes and interfacing events. Each of the events shown within a circle is a basic component failure for which failure rate data are expected to be available. The events shown within diamonds are basic events that are not expanded either because the event is judged not to be important, insufficient information is available, or the analyst merely wishes to postpone development. In any case, the event is given a name (see Section 7 below) and is accountable in the Boolean expression for the fault tree. The events shown within rectangles are interface events that will be expanded during the course of evaluating the interfacing systems (not evaluated herein).

The fault tree is developed in the preceding manner until all components of the system are identified in their basic fault states. The result is a binary model of the system which can be reduced to its simplest Boolean form. Failure rates, human error rates, and appropriate time intervals can be assigned to determine probability values for the components, subsystems,

and the system. The quantification process involves the naming of events and the transferring of all the information contained on the fault tree to event tables and coding sheets for ease in the assignment of data to events and for computer processing.

3.2 Abbreviated Fault Tree Construction

Since all basic fault event statements on the conventional fault tree are subsequently transferred to tables, one way to reduce the fault tree analysis effort is to not put those statements on the fault tree in the first place. The first step in the abbreviated method, then, is to enter all basic fault statements directly into fault summary tables (a portion of a fault summary table is shown in Table 1). Only the event code name, described in Section 7, is shown on the fault tree.

The second step in the procedure is to define a new logic gate, the tabulation OR gate (described in Section 5), to facilitate the listing of event names on the tree rather than to show named individual event statements within event type symbols as is conventionally done. Typically, systems which are evaluated contain a large number of events that are logically in series when reduced. For example, the fault tree development for the two injection path components connected in series (shown in Figure 5) is considered. This development can be restructured as shown in Figure 6, where the code names for basic input events are listed under a tabulation OR gate, inputs to a component can be shown under the tabulation OR as shown; otherwise, they can be expanded into their respective causes. The same treatment can be applied to any number of components logically in series. A completed fault tree for a system would be typically depicted by a top undesired event, basic fault events listed by code name under one or more tabulation OR gates, a few input events identified within rectangles which are inputs to chains of components and inputs to the system, a few house events, and the logic AND and OR gates used to relate the events. All the other information is contained in the fault summary table.

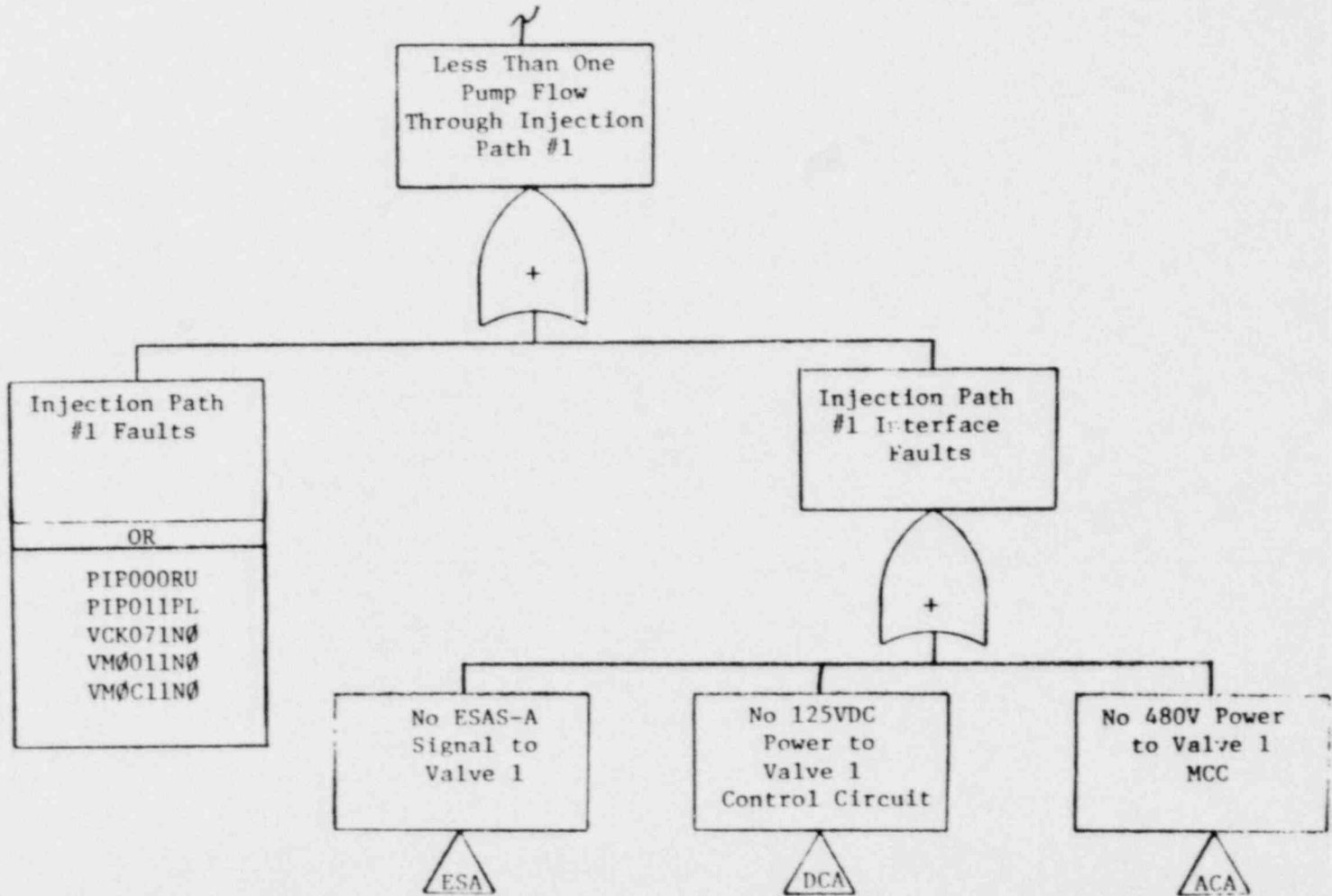
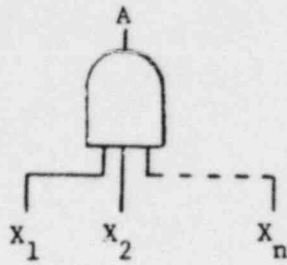


Figure 6
Basic Fault Events
Shown by Code Name Only

4. COMPONENT FAULT STATES

A component can transfer to a fault state due to any one of three categories of causes: primary failure, secondary failure, and command transition. A primary failure is the so-called "random" failure found in the reliability literature and refers to failure from no known external causes. A secondary fault results when a component is exposed to an operational or environmental condition which exceeds the design rating of that component. A command transition does not involve actual component failure. It simply means that the component is in the wrong state at the time of interest because it was commanded to that faulted state by another faulted component, a human error, or, in some cases, by an environmental condition.

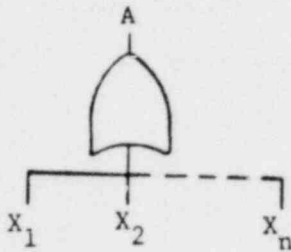
Most of the data available on nuclear components embody both primary and secondary causes for failure; therefore, the distinction between the two types of failure is not made on the fault tree except for the case in which a secondary cause results in multiple component failures, and the distinction is made in code only. A procedure for screening secondary failures for common cause failures is discussed in Section 10.



AND GATE

The output event A occurs when input events X_1 and X_2 and X_n coexist.

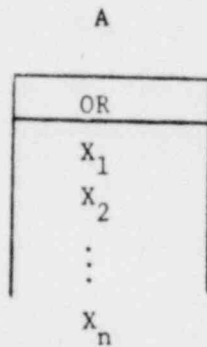
$$A = X_1 X_2 \dots X_n \text{ (all input events independent)}$$



OR GATE

The output event A occurs when any one or more input events X_1, X_2, \dots, X_n exist.

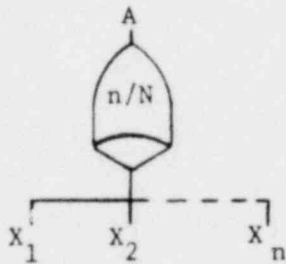
$$A \sim X_1 + X_2 + \dots + X_n \text{ (all input events independent)}$$



TABULATION OR GATE

The output event A occurs when any one or more input events X_1, X_2, \dots, X_n exist.

$$A \sim X_1 + X_2 + \dots + X_n \text{ (all input events independent)}$$



COMBINATION GATE

The output event A occurs when any subset of n of the N input events coexist. For example, if $n = 2$ and $N = 3$:

$$A = X_1 X_2 + X_2 X_3 + X_3 X_1$$

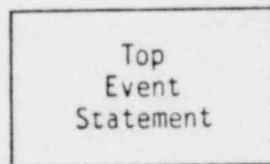
Figure 7
Abbreviated Fault Tree Logic Gates

7. EVENT NAMING

In order to facilitate the computer handling of events, and as discussed earlier, to simplify fault tree construction, each non-expanded event on the tree is given a code name. This includes "house" events, interfacing systems events, basic component events, and secondary events having common cause failure potential. The top event is also given a code name to facilitate future storage and retrieval of the fault tree. These event naming codes are described as follows:

7.1 Top Event

A three-character system code is used to identify each system fault tree. This code is obtained from Table A-1A, attached, for the Browns Ferry fault trees. The code name will be placed near the bottom of the top event on each fault tree and also at the top of each page of the associated fault summary. Where more than one fault tree is constructed for a system, the system code will be followed by the top "house" event code; for example:



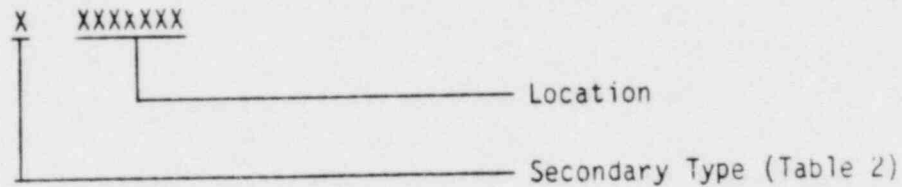
CBB-H2

7.2 House Events

A two- or three-character code name is used to identify each house event on a fault tree; for example:

7.4 Secondary Events

Secondary events which are expected to have significant effect on component failure and are suspect of affecting multiple components (common cause) are given a different eight-character name from that described previously. This secondary event code is characterized by the type of secondary event and location:



The potential secondary event location is best identified by building, room number within facility, and cabinet number, if applicable. If all rooms within the facility are uniquely numbered, the building number is not needed.

All events which are unique in the system must be given a unique name. An event may appear in more than one place on the model or on multiple models but, if it is the same event, it must be given the same name.

8. REQUIRED CONDITIONS

A system can assume a variety of possible off, standby, or normal operational states depending on plant conditions and operational requirements. For example, a water pump may be off if the water level in a tank is high but on if the water level is low, a diesel generator may be required to start if the offsite power fails, or a valve may be required to close if a fault has occurred in a downstream component. In fault modeling, inclusion by the analyst of the conditions upon which a system or component is required in the analysis is important. A system fault is not considered a fault unless the system is required. For example, failure of a diesel to start at any time other than when the diesel is needed is not a fault insofar as the analysis is concerned.

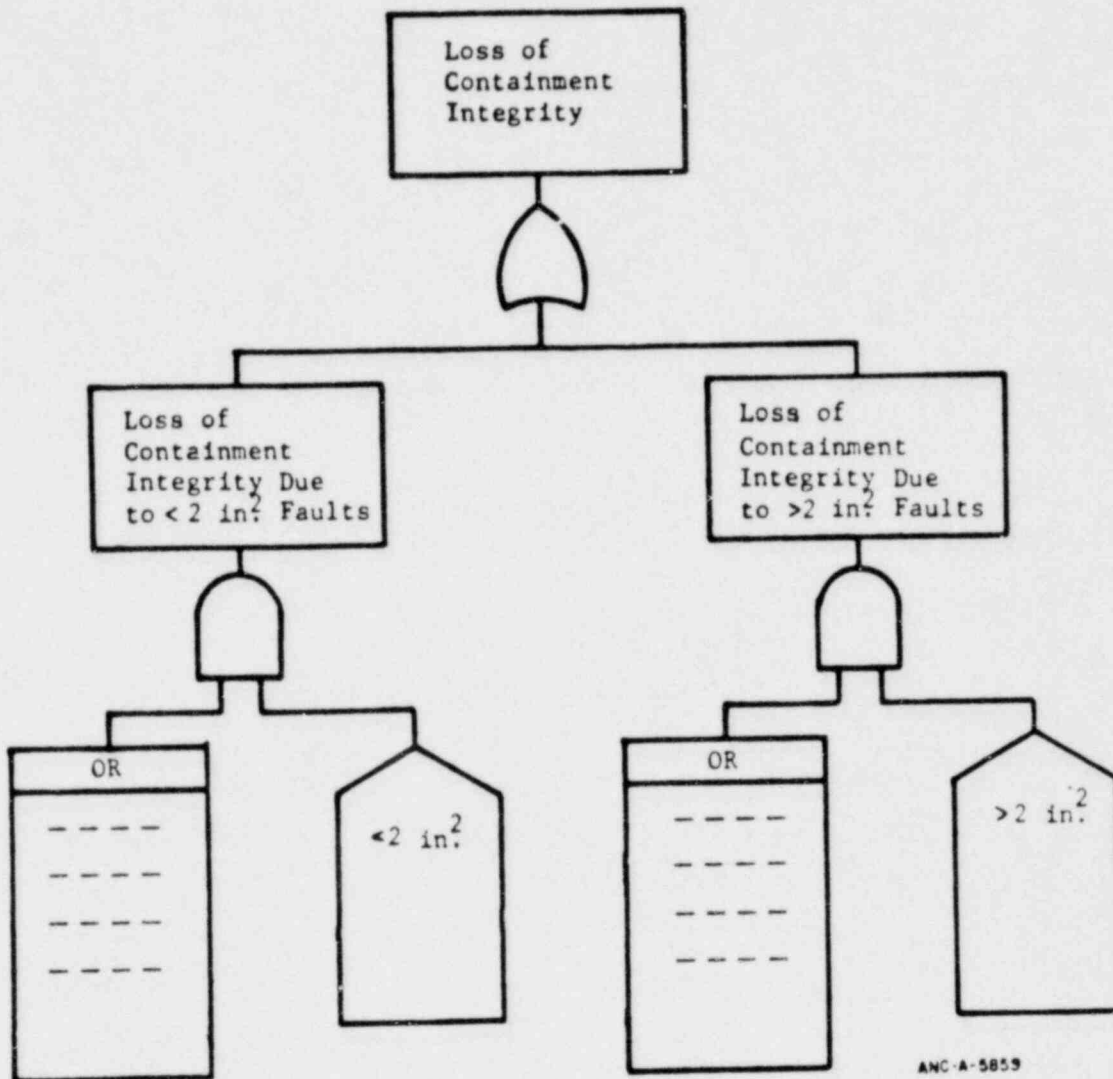
Required conditions in a fault tree analysis can be in the form of explicit assumptions and the fault tree constructed accordingly, or the required conditions can be incorporated directly in the fault model. The latter is preferred because it provides versatility in the use of the model. When incorporated into the model, required conditions are shown within the "house" symbol. The "house" serves as a switch to turn on those events which are faults when the required conditions exist and off when the required conditions do not exist. The "house" is input into one input of an AND gate, and the subtree of faults is input into other inputs of the AND gate as shown in Figure 2.

In some situations, to turn on or off subtrees by connecting the "house" to the input of an OR gate is desirable before going to an AND gate as shown in Figure 8. In this case, the required condition is inverted (stated negatively) such that when the "house" statement is true, the AND gate is enabled; when the "house" statement is false, only the existence of faults described by the associated subtree enable the gate. Typically, this inverted logic arrangement is used in fault modeling standby redundancy.

The house is also used to describe mutually exclusive faults, in which case, two "houses," as shown in Figure 9, are used--one or the other house can be on but not both at the same time.

The house is also frequently used to classify faults for which each fault classification results in a different consequence. For example, in the evaluation of a reactor containment classification of breach areas (faults) according to size may be desirable, as shown in Figure 10. In the computer evaluation of this fault tree, either or both houses may be turned on depending on whether the analyst is interested in faults $< 2 \text{ in.}^2$, $> 2 \text{ in.}^2$, or all faults, respectively, where the faults in each category are listed under the tabulation OR gate.

Any other conditions which are pertinent to the analysis and which should affect the analyst's thinking about the evaluation should also be specified. For example, knowing that a large LOCA has occurred and that suddenly large loads are to be placed on the electrical system should guide the analysis of the electrical system. That is, the analyst should concentrate his evaluation on those components (e.g., overload trips) which are vulnerable to transient loading. Turbine trip also occurs, and those components most likely to be effected by turbine trip should be examined.



ANC-A-5859

Figure 10
Classifying Faults Using the House

$$\begin{aligned}
A &= A_2 \cdot A_3 \\
&= (A_1 + X_1) \cdot (X_1 + X_3) \\
&= (X_1 X_2 + X_1) \cdot (X_1 + X_3) \\
&= X_1 X_1 X_2 + X_1 X_1 + X_1 X_2 X_3 + X_1 X_2
\end{aligned}
\tag{1}$$

The preceding algebraic expression contains "AND" and "OR" redundancies which can be removed by using the following idempotent relations:

$$A \cdot A = A \tag{2}$$

$$A + A = A \tag{3}$$

$$A + AB = A \tag{4}$$

By application of these relations to algebraic Expression (1), the model reduces to $A = X_1$. In this example, the analyst would not expand X_2 and X_3 into their respective causes of failure because the models represented by those variables would disappear in the end result.

cause event. That is, the event D0000211 would appropriately affect the nonredundant form of the Boolean expression resulting from one or more trees containing the event.

12. TEST AND MAINTENANCE

System outages due to tests and maintenance and the human errors which can accompany test and maintenance activities can be important contributors to the risks of nuclear plants. Some systems and components associated with nuclear plants are tested and maintenance is performed when the reactor is shut down; therefore, test and maintenance outage, as such, is not an important risk factor. However, where on-line testing and maintenance has been provided in the design, a system which is redundant can change to a nonredundant system during the time tests and maintenance are performed unless override features have also been provided in the design.

Outage due to test or maintenance is treated on the abbreviated fault model by showing an additional component fault event on the fault tree and on the fault summary for any subsystem or portion thereof which is unavailable during test and maintenance. Although not a failure in the strict sense of the word, outage is treated as a basic component fault with a mode designation "test" or "maintenance" and a fault mode code designation "T." Unless each component is tested or maintained separately and at different times, only the component requiring the longest outage time is shown as a fault time. If each component is tested or maintained separately and at different times, each component should be treated as a test and maintenance fault.

If a valve or other component can be left in the wrong state as a result of a test or maintenance error, the fault is also shown on the fault tree and is treated as a human error as discussed in Section 11.

14. SYSTEMS FAILURE ANALYSIS

The reliability of a typical nuclear safety system is dependent on the degree of redundancy in the system and its support systems and on the reliability of individual components in those systems. The redundant elements in those systems must be independent, and the individual components must be reliably mature for the expected operational and environmental demands on them. The failure analysis of a safety system, for the most part, requires that the analyst determine the degree of redundancy based on system requirements, that he verify the independence of those redundant elements by examination of individual component fault modes, and that he verify that components have been properly selected for the expected operation and environment. Fault tree analysis permits this failure evaluation of a system to take place systematically.

The failure evaluation of any system requires first that the analyst establish the physical boundaries of the system to be analyzed. These boundaries can be rather arbitrary, but they are usually about the same as those defined by the designer. Typically, the system, as defined, will have one or more outputs and one or more inputs (see Figure 11). The first task in evaluating that system will be to break the system down into redundant elements which must be done on the basis of the requirements of the system. This is to say that one accident may require that two of three pumps operate; another accident may require that only one of three pumps respond. For a two-train safety system which provides a single output function, the system broken down into its two redundant trains might be represented by the two "black boxes" as shown in Figure 12. The inputs to each redundant train, or subsystem, are also separated as shown. The abbreviated fault tree representing the two subsystems is shown in Figure 13.

The failure evaluation of systems in IREP will be conducted much as just presented, first for the front line systems and then for the support systems. The requirements for support systems, of course, are based on the requirements for the front line systems. The enumeration of individual

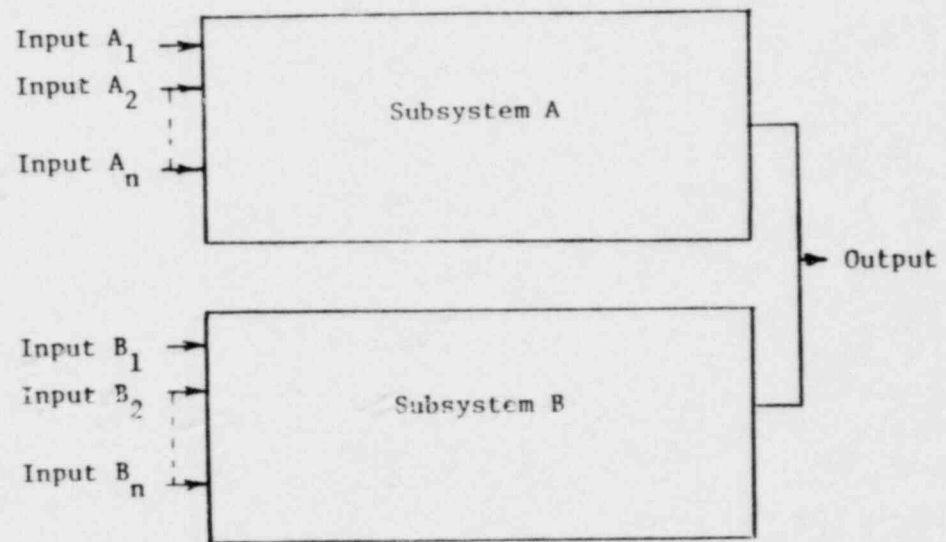


Figure 12
Typical Two-Train Safety System

faults under the OR gates will be deferred according to the discussion about staging in Section 12.

Failure analyses are usually performed to the component level of resolution where a component is defined as the largest entity of hardware for which experience data are expected to be available. A component is usually an off-the-shelf item which the designer uses as building blocks for his system. Sometimes it is necessary for the analyst to examine components, however, in order to determine how component inputs relate logically to the component output.

When examining component fault modes, the analyst should think not only about how each of those fault modes may affect the system being analyzed, but he should also concern himself about how those fault modes may affect other systems. For example, a timer in a residual heat removal pump circuit which is used to stagger the load application to emergency buses could actually trip a circuit breaker in the electrical power system if it becomes faulted. A leaky valve in a recirculation loop could result in fission product leakage to the atmosphere even though leakage may not affect recirculation performance.

10. Parent tree--A fault tree developed to a subsystem level only and which defines the top logic and which identifies the various interface faults with other systems.
11. Daughter tree--That part of a fault tree which enumerates the various component faults in a subsystem.

Sandia National Laboratories

Albuquerque, New Mexico 87185

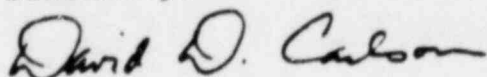
October 21, 1980

Mr. Joseph A. Murphy
Division of Systems and Reliability
Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Joe:

Enclosed is our draft proposal for human reliability modeling for IREP. Any comments you might have would be appreciated. I assume that this will be among the topics for discussion at the methods meeting on the 28th. See you then.

Sincerely,



David D. Carlson
Nuclear Fuel Cycle Systems
Safety Division 4412

DDC:4412:ep

Copy to:

EI	Jon Young
INEL	Jack Trainer
SAI	Paul Bleiweis
SAI	Abel Garcia
SAI	Cliff Gerstenhaber
USNRC	Frank Rowsome
1223	B. J. Bell
1223	H. E. Guttmann
1223	A. D. Swain
4410	D. J. McCloskey
4412	J. W. Hickman
4412	A. M. Kolaczowski
4412	G. J. Kolb
4414	G. B. Varnado
4414	D. W. Stack
4414	R. B. Worrell
4412	D. D. Carlson

Human Reliability Modeling for IREP

The treatment of human reliability is a very important aspect of any risk assessment. Past risk assessments have shown that the human plays an important role in at least some of the dominant accident sequences. Actual operating experience reflected in Licensee Event Reports and accidents such as those at Three Mile Island and Browns Ferry attest to the importance of operator action.

The treatment of human reliability in nuclear power plant operation is a complex task. The purpose of this paper is to present a systematic approach for identifying human error susceptibilities for incorporation into the IREP models and to propose an approach which will identify and quantify those susceptibilities important to risk. This discussion will serve as a guideline for handling most of the operator actions of importance to IREP. Nevertheless, a particular plant may have specific design or operational considerations which are unique and which require case-specific human error considerations. These can be handled only on a case-by-case basis, perhaps using this discussion for some general guidelines.

Incorporation of Human Errors into Logic Models

For the purposes of this discussion, human errors in two situations are considered: test and maintenance operations and transient or accident response situations. Both are important and must be addressed in the IREP study.

Unavailability Due to Test and Maintenance

A system may be unavailable as a result of test or maintenance activities if (1) the system is undergoing test or maintenance at the time it is required to operate or (2) the system is left in an inoperable state by test and maintenance personnel. The latter would constitute a human error. An example of such an error is failing to reopen manual valves which were closed to allow maintenance on a pump.

System unavailability during testing and maintenance and human errors committed in performing these activities are independent of any particular accident sequence. Therefore, they should be modeled explicitly on each system fault tree by developing the test and maintenance fault logic associated with each affected component.

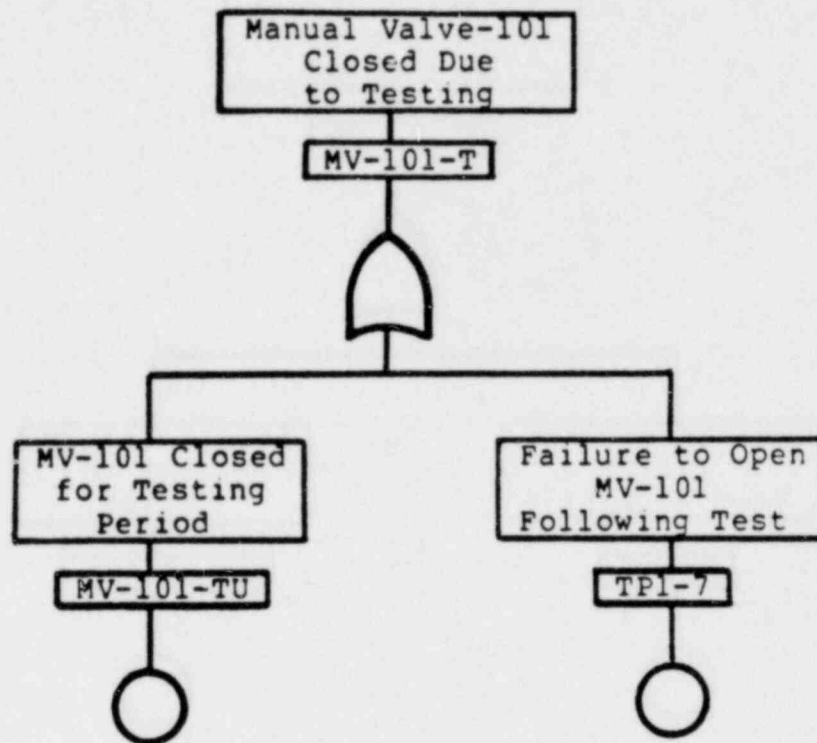
This may be done as follows. The analyst for each system reviews the testing requirements and testing procedures for the system. These should be placed in the system description notebook. For each procedure, he constructs a table of actions performed on components in the system. The table has the following form:

<u>Procedure</u>	<u>Step</u>	<u>Component</u>	<u>Action</u>	<u>Comments</u>
Test Procedure 1	1	Manual Valve-101	Close	Normally Locked Open
	7	Manual Valve-101	Open	

From this table, the analyst can identify which components in the system are affected by actions associated with the test. In general,

it will be assumed that the only components affected by the test are those associated with the procedure - that is, that the operator does not manipulate any components not involved in the procedure. However, if the analyst believes that such an action is probable, he should include this in the fault logic for the system affected. (For example, the analyst may ascertain that three valves are colocated in the plant, but only one is to be manually manipulated by the operator for a given test. It may be fairly probable the operator would turn the wrong valve. Such an error would appear in two places in the fault tree: as an error of omission for the system undergoing test, and as an error of commission for the affected system.) Although such exceptions may exist, generally the only errors to be considered are those in which an operator fails to perform a given step in a procedure properly, or in which he omits a step altogether. Human factors specialists suggest these constitute the majority of human errors which might fail a component.

For each affected component in this system, the fault logic associated with the test of the system will be developed explicitly. A "component unavailable during testing" event and events associated with human errors which would cause the component to fail, can be modeled as inputs to the OR gate representing the causes of component failures. For the example above, if "Manual Valve-101 closed due to the testing" is the fault event, the logic would appear as follows:



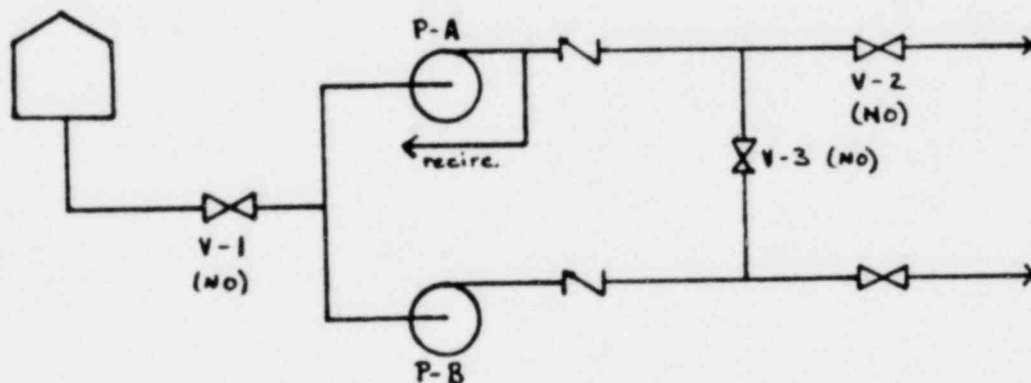
The event MV-101-TU reflects the unavailability during the test - it is assumed that the test procedure is performed correctly. The other event, TPI-7, reflects the human error which leaves the component in the failed state.

There could, of course, be other events in the development of a "manual valve-101 closed" event reflecting hardware failures, other human errors (discussed below), or other errors involved in testing the system. It is important that each component failure in the tree be given a label indicating the particular procedure and step in the procedure. In the above example, the label "TPI 7" indicates that the error was that of performing step 7 in Test Procedure 1 improperly. If several components are affected by the same procedural step, it is important that the same label be affixed to each, since performance of operations on these components may

be dependent. That is, if test procedure 2, step 3, calls for valves A and B to be opened, the events "operator fails to open valve A in test 2" and "operator fails to open valve B in test 2" should both be labeled "TP2-3" and treated as a single event.

The unavailability and human errors associated with maintenance activities are treated in the same manner as those of testing. That is, maintenance procedures for the system are reviewed, a table of procedures and components is constructed, and appropriate faults are included in the system fault tree development.

As another example, consider the system illustrated below.



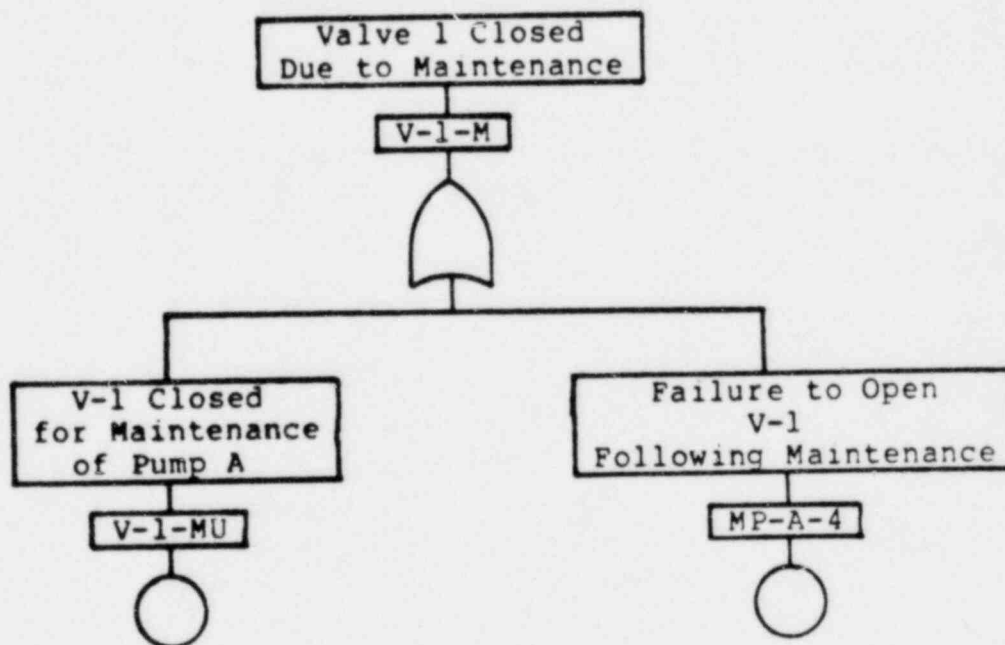
Testing of Pump A requires the following steps:

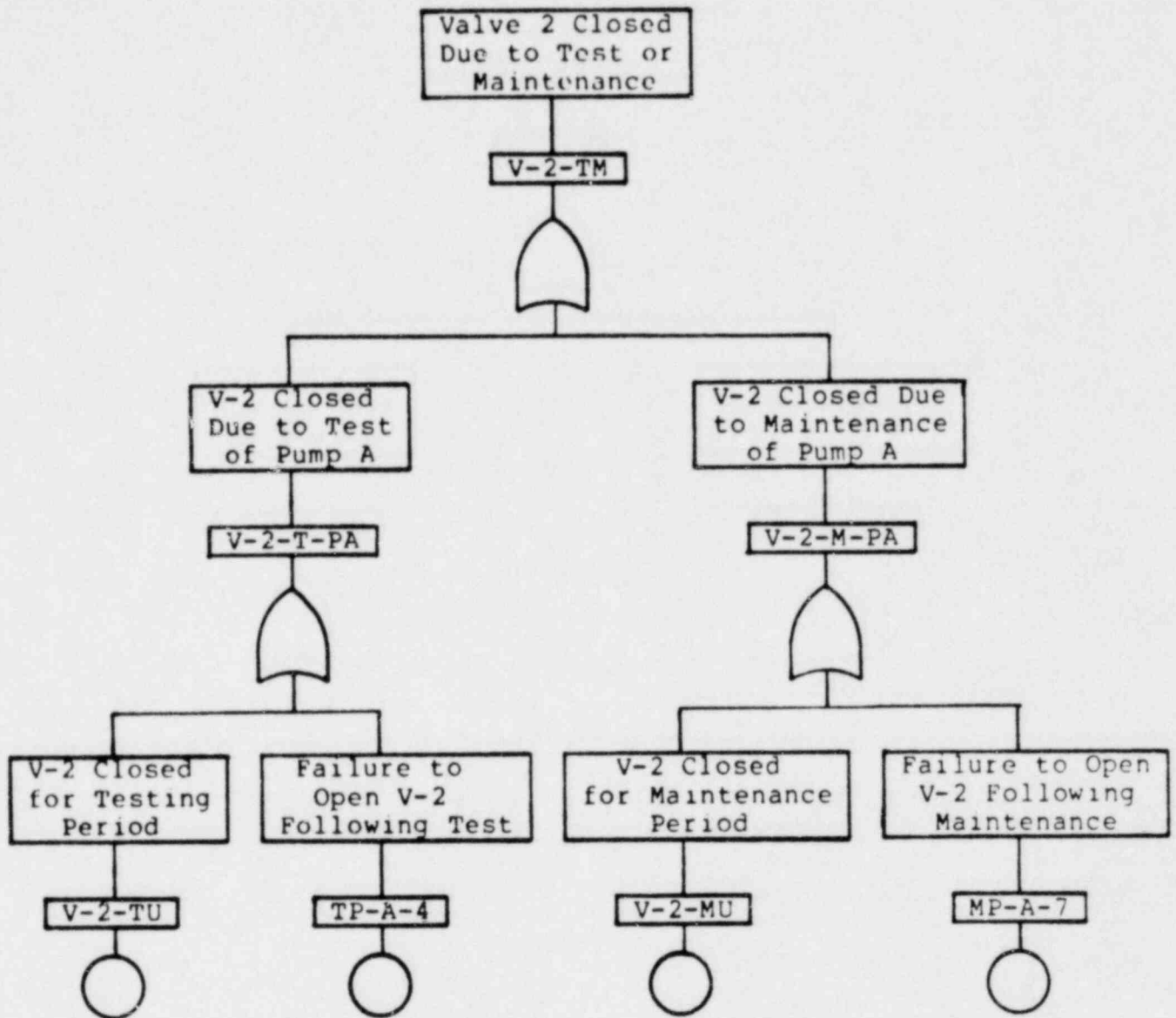
<u>Procedure</u>	<u>Step</u>	<u>Component</u>	<u>Action</u>
TP-A	1	V-2, V-3	Close
	2	P-A	Turn On
	3	P-A	Turn Off
	4	V-2, V-3	Open

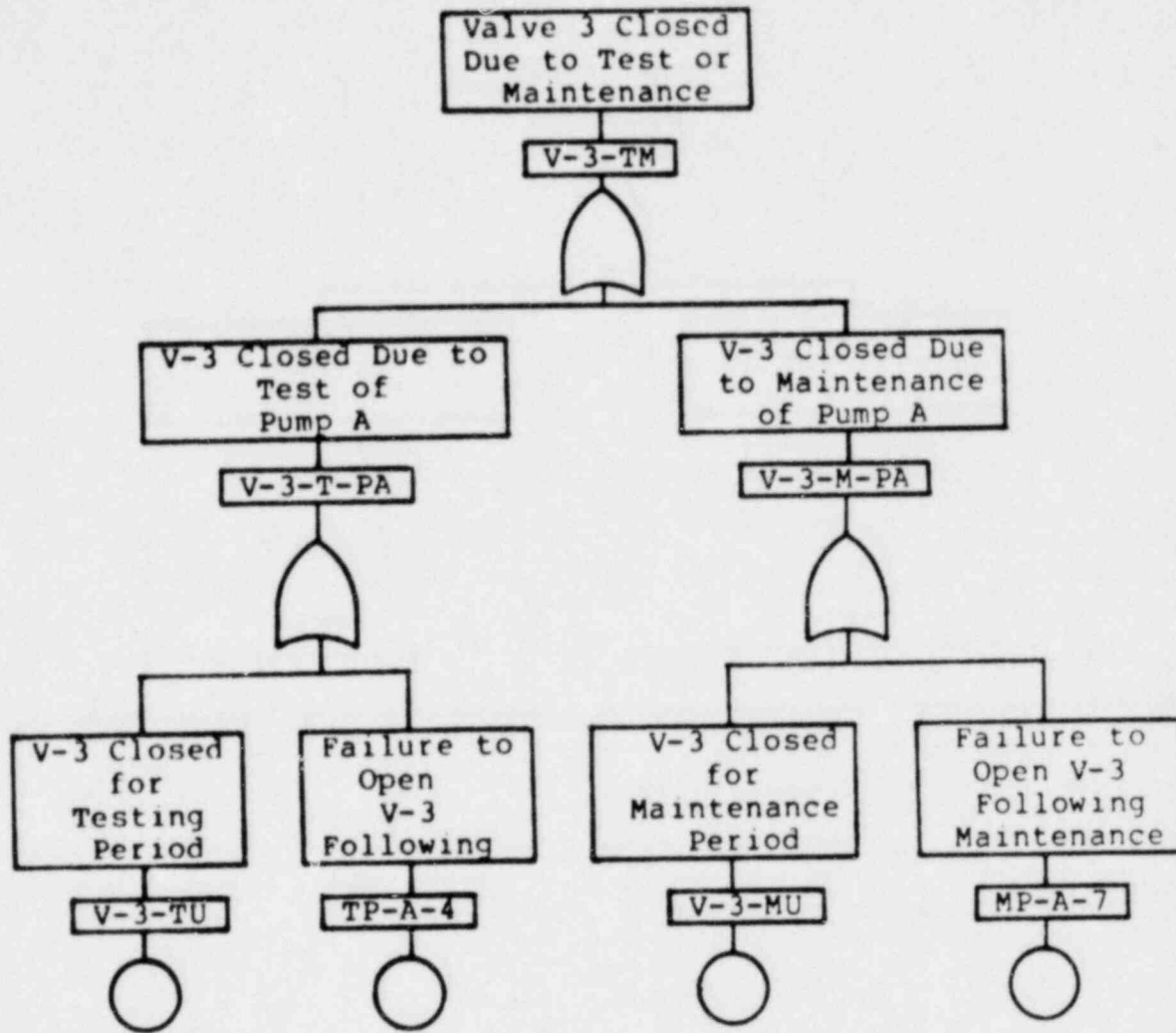
Maintenance on Pump A requires the following steps:

<u>Procedure</u>	<u>Step</u>	<u>Component</u>	<u>Action</u>
MP-A	1	V-1,V-2,V-3	Close
	2	P-A	Remove From Service
	3	P-A	Return to Service
	4	V-1	Open
	5	P-A	Turn On
	6	P-A	Turn Off
	7	V-2,V-3	Open

Fault logic for the unavailability of valves 1, 2, and 3 as a result of test and maintenance would appear as follows:







In each case, unavailabilities and human errors for valves 1, 2, and 3 are modeled as part of the valves' pipe sections even though the test or maintenance activities are associated with pump A in a different pipe section.

Errors in Responding to an Accident

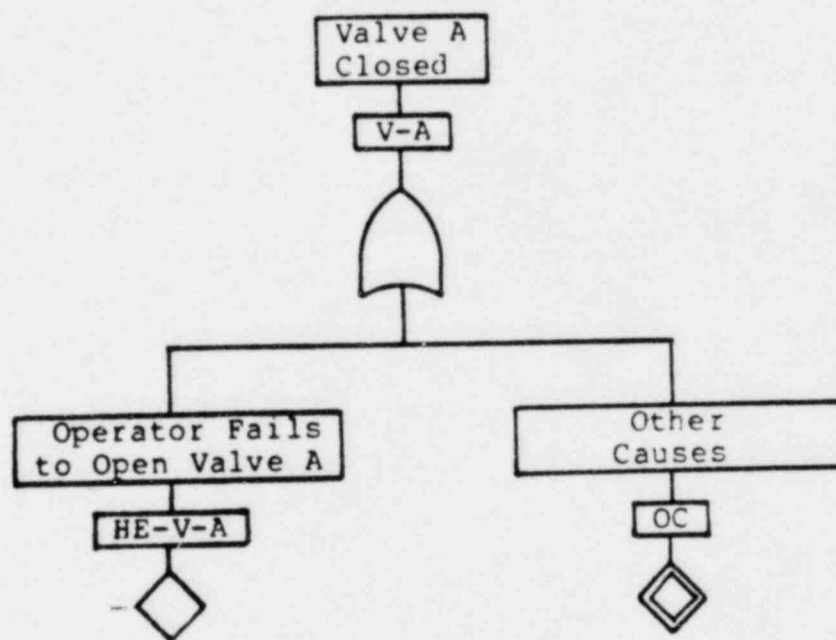
The treatment of potential human errors under accident conditions is somewhat more difficult than the treatment of errors during test and maintenance. A major difficulty in including these errors explicitly in the fault logic is that operator actions are dependent upon the particular accident sequence. Thus, one logic development may not apply to all situations. Only errors of commission and errors of omission associated with the carrying out of particular procedures will be considered. Human factors specialists suggest extraneous actions are generally so infrequent that they may be disregarded.

This analysis begins, as in the case of test and maintenance errors, with a review of the procedures, such as the Emergency Operating during test and maintenance. A major difficulty in including Procedures which the operators would use in responding to a transient or accident. To identify the components susceptible to human error during an accident a table is constructed of the following form:

<u>Procedure</u>	<u>Step</u>	<u>Component</u>	<u>Action</u>	<u>Comments</u>
EOP-1	1	Valves A, B	Open	
	4	Pump C	Turn On	
	9	Valve D	Regulate	
EOP-2	3	Valve A	Open	
	4	Pump E	Turn On	
	7	Valve F	Close	

This table includes those steps in the procedures in which the operator is called upon to change the state of a component.

From the completed table, a list is compiled of all components susceptible to human error by performing a procedure incorrectly in responding to an accident. For this example, the list includes: valves A, B, D, and F, and pumps C and E. Wherever these events appear in the fault tree, one cause of failure is "human error under accident conditions." This event is not further developed explicitly in the tree, but is labeled with a human error identifier. That is, the development of event "valve A closed" is as follows:



At this stage in the logic development, all potential human errors associated with carrying out the emergency procedures improperly have been included in the tree. However, for a given accident sequence not all such errors are applicable, since not

all procedures are implemented for each accident sequence. Thus, the analysis from this point forward is accident sequence dependent.

To proceed, the analyst must identify which procedures the operator is expected to use in responding to each accident sequence in the event tree. The utility representative on each team should be of great assistance in this regard. Again, a table containing this information is constructed as follows:

<u>Accident Sequence</u>	<u>Designator</u>	<u>Procedures Used</u>
Large Loca-10	ACD	EOP-1, EOP-2
Small LOCA-34	S ₁ C	EOP-1

Given this table and the preceding one (relating components to procedures), a set of Boolean equations representing potential human errors for each accident sequence is constructed. For sequence ACD, such a set of equations includes:

$$HE-V-A = EOP-1-1 + EOP-2-3$$

$$HE-V-B = EOP-1-1$$

$$HE-P-C = EOP-1-4$$

$$HE-V-D = EOP-1-9$$

$$HE-P-E = EOP-2-4$$

$$HE-V-F = EOP-2-7$$

The set of equations relating the human error events to particular procedural steps is constructed for each accident sequence. Again, it is important that multiple components affected by the same procedural step be assigned the same label.

An alternative approach would be to develop each human error event explicitly for each accident sequence. Such an approach

does not seem as desirable as constructing a set of transformation equations, since the fault trees would be different for each accident sequence.

The proposed approach assumes that the operator is attempting to follow the proper procedure in responding to each accident sequence. This assumes a proper diagnosis of the situation. However, if the operator diagnoses the situation incorrectly, he will be using an incorrect set of procedures. Further, even if he diagnosed the accident correctly, there is a possibility that he will inadvertently choose the wrong procedure. In terms of system consequences, neither of the above errors may be significant because of many factors. The symptomatic similarity of some accident sequences calls for their having similar response requirements; there may be no actions called for in the incorrect procedure that would actually degrade system performance. In many accident situations, critical responses are required to be performed within a period of time that is sufficient for the arrival (if not already present) of a shift supervisor and two reactor operators. Although there may be some degree of dependence between the personnel, there is a recovery factor of human redundancy which may compensate for this. Finally, in any sequence to which the operator is responding incorrectly, there will be numerous indications to that effect. Even if the operator should concentrate on a particular subsystem to the exclusion of other, perhaps more critical, indications, the factors of time, additional personnel, and feedback offer some chance of recovery. These factors would need to be considered individually and collectively for each accident sequence. However, the state-of-the-art of human

reliability analysis does not allow for quantification of these interactions. Therefore, these potential errors will be disregarded. Specific instances may be considered in the latter stages of this project.

Treatment of Human Errors in the Screening Process

Quantification of the accident sequences for IREP will take place in two stages: an initial screening process to identify candidate dominant accident sequences and refined quantification to arrive at a final set of dominant accident sequences. This section discusses the treatment of human errors during the initial screening process.

Test and Maintenance Unavailability

As discussed previously, the unavailability of a component due to test and maintenance and the potential human errors associated with testing and maintenance are developed explicitly in the system fault trees. For each of these events, an unavailability or probability of failure is assigned.

For component unavailability, the standard unavailability calculation is performed:

$$Q = \frac{\text{mean duration time for test or maintenance}}{\text{mean test or maintenance interval}}$$

Data for these calculations may be found in the IREP Data Guide, Wash-1400, or in some cases, may be obtained from the plant.

Data for human errors during test or maintenance may be found in NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Each analysis team

is encouraged to utilize this reference and arrive at numbers on its own. However, should problems arise in using the handbook, human factors specialists at Sandia National Laboratories will be available to provide assistance.

Errors in Responding to an Accident

The quantification of human errors in response to an accident is not as straightforward as that associated with test and maintenance. Although the human reliability handbook provides a wealth of information, there are many variables during an accident which influence human reliability and the selection of a probability value for a given error. Some of these include operator training, stress, and control room design. To quantify a given human error accurately, these and other factors must be considered. However, to perform such an assessment on each potential human error for each accident sequence would be an unmanageable task. Rather, the IREP team must employ a coarser quantification scheme for the initial screening process which will permit identification of those human errors which might contribute to dominant accident sequences. Only these human errors will be accurately quantified.

The previous discussion led to the generation for each accident sequence of transformation equations which represent the potential human errors associated with procedures to be followed during that accident. In the initial quantification of sequences, these equations are to be substituted for the appropriate fault tree events. Those human error events which do not apply to the particular accident sequence are set to ϕ .

In addition to performing this substitution, probability values are assigned to each event. For the initial screening process, coarse values are chosen for the human error events for reasons discussed previously. These coarse values should represent upper bounds -- one does not want to underestimate probabilities at this stage, or some important terms may be discarded during the screening. Human factors specialists suggest that assigning a probability of 0.1 to an error in a given procedural step would represent a reasonable upper bound in most cases. This number is not assigned to the human error event, but rather to each event in the transformation equation. That is, for the equation $HE-V-A = EOP-1-1 + EOP-2-3$, a value of 0.1 is assigned to events EOP-1-1 and EOP-2-3. For the initial screening process, errors within a single procedural step are assumed to be completely dependent. Actions performed in different procedural steps are generally independent, and this assumption is made. If the analyst believes he has identified an exception, appropriate probability values should be assigned.

The computation and screening criteria are described in the IREP quantification guide and will not be discussed in detail here. Briefly, however, each accident sequence is analyzed to determine the minimal cut sets (with illogical cut sets removed). The human errors in these cut sets are recognized by their labels. For the examples cited above, test errors appear as terms such as TP1-7, maintenance errors as terms such as MP3-4, and errors in responding to accidents as terms such as EOP-1-1.

Candidate dominant accident sequences are chosen probabilistically based on the probabilities and criteria used in the initial screening

process. Only these sequences are analyzed further. The cut sets and events for each of these sequences are ranked to aid in the final quantification process.

Final Quantification of Human Errors

The IREP quantification guide discusses final quantification of accident sequences in detail. In brief, each candidate dominant accident sequence is analyzed to ensure that it is properly quantified. The probabilities are scrutinized and, perhaps, modified to reflect plant specific data. The analyst attempts to ensure that all common modes have been considered, and the potential for recovery is assessed.

For those sequences containing human errors, the probabilities must be examined. Values for test and maintenance errors should be reviewed. Plant specific data pertaining to test and maintenance errors may need to be included. Errors made in responding to an accident have not yet been adequately quantified in this process. For those human errors in the candidate dominant sequences, actual probabilities must be inserted (rather than the 0.1 value used for screening). These values are obtained from the human reliability handbook. The analyst should use his best judgment in choosing the number from the range that is given in the handbook, considering such factors as operator training, timing and stress of the sequence, and control room indications.

Human factors specialists from Sandia will visit each plant. They will be familiar with the control room and the performance shaping factors affecting the probability of a given error, and they will be available to consult with the analyst should problems

arise in selecting a probability. The Sandia human factors specialist may also provide assistance in assessing the potential for recovery from an accident.

After this final review of the candidate sequences to ensure they have been properly quantified, the final set of dominant accident sequences is identified.

COMPONENT FAILURE RATES FOR NUCLEAR PLANT
SAFETY SYSTEM RELIABILITY ANALYSIS

The purpose of this report is to provide component failure rates and general criteria for selecting component failure rates for use in the reliability analysis of Nuclear Plant Safety Systems. This report is not intended by itself to supply a list of "absolute" and final numerical component failure rates. There are several reasons why producing such an absolute list is impractical - the most pertinent concern, the large physical variation of available components of a given generic type and the possible variations of environment and operation and use.

The basic questions to be asked when determining and using component failure rates are:

- a. What failure rates should one use when modeling specific components in specific safety systems at specific plants?
- b. How should the expected variations of failure rate for specific components within specific systems and plants be described and accounted for?

There do not appear to be absolute answers to these questions and therefore this report is limited to a general discussion of criteria for failure rates while providing only basic lists of "nominal" component failure rates.

The attached Table 1 is a summary of a survey of component failure rates taken in the latter part of 1979. The survey requested "generic" or "average" component failure rates which the respondent would use for a reliability analysis of Nuclear Plant Safety Systems. The survey illustrates the range of generic failure rates currently recommended by the reliability and safety community for nuclear plant safety system analysis. Table 2 shows failure rates obtained from the LER Evaluation Program and comparable WASH-1400 failure rates. Table 3 shows generic failure rates generally recommended for screening purposes for the IREP reliability analysis of nuclear plant safety systems. This list was taken from the WASH-1400 and is unchanged except where revised to account for the results of data analyses which have occurred since the WASH-1400 study. For detailed analyses, it is suggested that the user supplement the Table 3 data with data from Tables 1 and 2. In addition, data from other available valid data sources (e.g., NRC/EG&G LER Summary NUREGs, the NRC or Oak Ridge LER files, etc.) should be referred to whenever more particularly specific, up-to-date, or pertinent failure rates are required. The attached appendix presents a general discussion of the uses and limitations of presently available component failure rates.

APPENDIX

NUCLEAR PLANT SAFETY SYSTEM COMPONENT FAILURE RATES

GENERAL DISCUSSION OF COMPONENT FAILURE RATES AND
FACTORS AFFECTING COMPONENT FAILURE RATES

CONTENTS

	<u>Page</u>
Component Failure Rate Problems - Timeliness, Consistency, Quality	1
Point Values and Range of Component Failure Rates	4
Demand Related Vs. Time Related Component Failure Rates	7
LER Evaluation Program Results	10
Limitations of Calculated Component Failure Rate Accuracy	12
Recommended Component Failure Rates	14
Common Mode Failure Modeling	15
References	19

COMPONENT FAILURE RATE PROBLEMS - TIMELINESS, CONSISTENCY, QUALITY

This report concerns the derivation and use of component failure rates for nuclear plant safety system reliability analysis. In particular, the report is concerned with those failure rates appropriate for particular systems or plants versus more encompassing failure rates which may be appropriate for a generic analysis of all plants.

The problem of deriving and using component failure rates for particular safety systems in particular plants is more difficult than deriving and using "average" component failure rates for "average" plants. There are several reasons for this which are tied to the selection of the proper population of failure data applicable to a specific case. One is that there is usually much less data available to make inferences for a particular plant than there would be when agglomerating the data from several plants. A second and perhaps even more important reason is that any operational or equipment anomalies occurring in a small population over the short term may, when considered for a larger population over a longer term, be "averaged" out. A factor affecting the failure rate data an analyst needs concerns the time or time period his analysis is to cover. Is the analysis for equipment reliability as it was over the last 5 years? As it is now? Or is the desired reliability the average value over some projected time period of say the next 5 years? For assessing the immediate period one would of course want current data, anomalous or not. However, the available data to derive failure rates is of necessity for past periods and experiences - with very good possibilities

that past component failure anomalies have been or will be corrected. Because of equipment modifications, modified operational requirements, equipment deterioration or wearout, etc., the appearance of anomalous component failure rates for particular plants at particular periods should not be unexpected when compared to "averaged" data. The failure rates one selects should recognize these possibilities and be appropriate for the projected period the analysis is to cover.

In deriving component failure rates, similar components (e.g., valves, pumps, etc.) are grouped when they are deemed as physically and functionally belonging to a particular generic population. But, the components in the population could in fact have considerably different individual failure rates and failure rate distributions and thus not be applicable to any specific component or class of components. When components from different populations and useages are combined for failure rate calculations, the quantities within each population are weighted into the calculation. The resulting "composite" component failure median value and distribution strictly applies only to a population having a similar mixture--it no longer applies to any individual subpopulation. The concept of "best estimate" or "point value" has questionable utility when it is derived from failures for composite populations in this manner. For composite populations one can calculate average or mean values and these have meaning when applying them to similar composite populations; but, they may not have meaning for subgroups within the homogenized or aggregate populations. It is expected that for certain components, the best estimate failure rates of the various generic sub-classes may in fact be

very similar. In these cases one number or one distribution may adequately describe all subclasses of components within the generic category. However, this may not be universally true. One of the goals of future data analysis will be to assess generic component composition effects and determine the number of separate failure rates and failure rate distributions required for commonly used safety system components.

For system reliability calculations, one needs to recognize that there will be a variation of quality of failure rates for various components and account for or recognize this in the calculations. The "quality" of the failure rate for any particular component can be dependent on such variables as the quantity of similar components in use from which to gather data, the possible physical variation of particular components, etc. The component failure rate quality required is some function of the importance of the component to system reliability. Generally, in safety system evaluation some few components will, because of their singularity (non-redundancy) or high failure rate "dominate" in probability of causing system failure. Further studies can then be performed to determine the effect on or sensitivity of system unavailability when these critical or dominant components are allowed to cover their expected or bounded range of values. If the resulting system variation is unacceptable, the data quality may have to be improved.

There are several factors which can cause or effect variation or quality of component failure rates including:

A. Intrinsic Factors

- Component Size
- Specific Component Type or Model
- Operating Rating

B. Extrinsic Factors of Component Use

- Condition or Environment of Use
- Derating Factor or Operating Margin
- Medium of Use (Gas, water, steam, etc.)

C. Calculational or Estimation Errors

- Inaccurate reporting of failures
- Inaccurate running or cycle time or demands
- Inaccurate population estimates
- Incorrect agglomeration of Components for Rate Calculation

All of the above factors can affect calculated failure rates to varying degrees and should be recognized and accounted for in detailed failure rate calculations.

POINT VALUES AND RANGE OF COMPONENT FAILURE RATES

Safety system reliability evaluation and quantification problems may be of two kinds. The first evaluation problem involves arithmetically deriving a "best" or "point" estimate value of a systems unreliability. The second or "probabilistic" problem type involves finding a best estimate and the expected variation or range of unreliability. One therefore needs the point estimate (best estimate) and the expected variation or spread of component failure rate data for these two problem types.

The "best" or "point" estimate failure rates used in reliability and risk assessment of Nuclear Power Plants can be further subcategorized and representative of two different component populations. One population consists of a generic mixture of components and the resulting failure rate is an "average" or "generic" type of failure rate intended to cover a broad generic class of components and operating conditions. The other "best" or "point" estimate failure rate is specific to specific components and component operating conditions such as are presented in MIL-SID 217, "Military Standardization Handbook - Reliability Prediction of Electronic Equipment" for electronic components. In the nuclear industry specific failure rates are generally not available. The Nuclear Plant Reliability Data System (NPRDS) has somewhat specific component failure rates; however, the NPRDS lumps together "similar" components having "similar" operating or environmental conditions so that its rates are still generic failure rates. Another example of average or generic failure rates are those derived from Licensee Event Reports (LERs) and shown in the various LER Analysis reports.

For reliability assessments one generally needs best estimate rates and spreads for averaged or generic components rather than best estimate and spreads for specific components. This is because in most cases sufficient engineering or operational detail is not available to the reliability analyst for the system he is analyzing to determine an exact pedigree of the component or the component operating conditions. Therefore, even if one had extremely specific failure rates, the analyst

could probably not provide matching detailed particulars of component type and operational or environmental factors affecting the component. Therefore, for many, if not most reliability analysis problems, extremely specific component failure rates would not be useful. However, where a component's failure rate significantly affects the determination of risk, an attempt should be made to restrict the data used to a suitable subset of the generic population to the extent possible.

A continuing problem encountered in using failure rates concerns the range that should be used to encompass or bound the expected variation of failure rates. The range used can be derived to cover physical variation within a component generic class, environment of use, system, or plant. A related question concerns how specific one must make failure rates as discussed above and the expected penalty one must pay in the form of increased spread (range) penalty when the specifics of component type and component use are unknown or unspecified. Lastly, the type or shape of failure rate distribution to use, be it uniform, log-normal, etc. must be determined.

A failure rate distribution shows the variability and failure likelihood one would expect to find in the failure rate for a particular component. As has previously been indicated, different sub-classes of generic components and component uses may have different failure rate distributions. Hence, when we calculate failure rate distributions from failure rate data, we are evolving a synthesized average failure rate representative of the summed or weighted sub-classes of components. There is no problem

in producing such a synthesized failure rate distribution. However, once "synthesized" the failure rate data cannot easily be "unsynthesized" by the reliability analyst to fit his particular sub-class of components. In some instances, however, we can accommodate this shortcoming somewhat by selecting a failure rate distribution which adequately, albeit conservatively, bounds the generic component, provided undue conservatism is not introduced.

DEMAND RELATED VS. TIME RELATED COMPONENT FAILURE RATES

There are two different measures of component failure commonly used in reliability assessment. These are failures per unit of time and failures per number of demands. The failures per unit of time can be further categorized as follows:

- Standby failure rate - Failures per hour in Standby
- Operating failure rate - Failures per hour of Operation

There is one other component failure rate known as "Shutdown failure rate - Failures per hour of Shutdown" which is sometimes found in reliability literature. This report excludes "Shutdown" failure rates because the component failure rates herein are intended for use in evaluating nuclear plant safety systems while they are either operational or in standby. The three possible types of failure rates used in this report are:

- Failure per demand
- Failure per Standby Hour
- Failures per Operating Hour

The type of failure rate to use in reliability analysis may or may not be obvious. For example, pumps are either operating or not operating (in standby) and would have corresponding failure rates for each of these phases of operation. The applicable rates for other components may not be as obvious. For example, a motorized block valve in a safety system is either open or closed. It is usually inactive except for the short duration of time that the motor is energized to shuttle the valve to the open or closed position. On the other hand, a modulating valve may be considered to be operating continuously for the duration of its parent system operating time. For simplicity, at most two failure rates are given for any particular component. The failure per operating hour is given (if pertinent) along with either the failure per demand or failure per standby hour.

A complication that occurs in failure rate use is that most components can fail either when demanded or while in a standby (non-operating) mode. Because of this, neither the "demand" nor "failure per hour" failure rate is entirely correct except when used to evaluate components that have similar numbers of demands, standby times and times between test. In equation form this means that:

$$Q = Q_0 + \frac{1}{2} \lambda T$$

where: Q = Total component unavailability

Q_0 = Demand unavailability

$\frac{1}{2} \lambda T$ = Time related unavailability

Solving the above equation for λ gives:

$$\lambda = 2 \left(\frac{Q - Q_0}{\tau} \right)$$

This indicates that λ is dependent on both time between tests (τ) and the cyclic or demand fraction (Q_0) of component unavailability. The problem is that we have two unknowns (λ and Q_0) and only one equation. If one can't determine these two basic failure parameters, then one can't correctly use this failure rate except in situations where the test intervals are similar to the intervals from which the failure population is derived. This presents a problem when component unavailability is required for components that are tested at longer than normal test intervals. If one used a failure per demand rate for this case, one would underestimate failure probability and yet if one assumed the failure rate was strictly time related, one would overestimate the failure probability.

In an attempt to help solve the above problem, the LER Analysis Report NUREGs categorize LER failures as Demand related, Time related, or Unknown. This categorizing is subjective insofar as the LER contains a minimal amount of information upon which to make this judgment. And, as might be expected, many of the LER failures could not be classified from the LER description and so are categorized as unknown. The gross fraction or breakdown is included in the LER NUREG failure rate summary tables, however, and can be used to estimate failure rate fractions due to demand and time dependent failures. This can be helpful when evaluating

systems having testing intervals which vary from the norm. It is also helpful to have this information when evaluating optimum safety system testing intervals.

LER EVALUATION PROGRAM RESULTS

The LERs have been analyzed by EG&G/INEL to calculate pertinent nuclear plant safety system component failure rate data. These analyses (refer to references) and the component failure rate statistics produced are for groups of similar reactor plant types (NSSSs) and for individual plants. The LER derived data are "average" failure data for generic component classes. From the LER data one can determine a Chi-square confidence interval for the component failure rate. However, the Chi-square derived interval infers a single population sample rather than a mixture of samples from several populations. It is because of the dissimilar raw data populations that the confidence bounds for the aggregate or generic calculated component failure rates as shown in the LER Data Summary NUREGs are questionable. Other problems associated with determining failure rates from LERs are the problem of variations of failure reporting, determination of components and systems to be reported on, etc.

The LER derived component failure rates indicate that there is a large variation of failure rates "plant-to-plant." Since the plants are each essentially "one-of-a-kind," it is expected that some of this variation is in fact caused by the plant designers using different designs and different quantities of each of the sub-classes of components. Certainly,

the different designs result in slightly different component uses or operating environments and hence different stresses on each component. Therefore, some of the LER calculated plant-to-plant differences are felt to be real. However, some differences of failure rates are undoubtedly caused by variations of reporting rules and the degree or emphasis of reporting by the various plants. The reporting differences can cause an estimated variation of a factor of 2 or 3.

As noted above, the component failure rates as derived in the LER Evaluation program indicate large variations "plant-to-plant." The significance of these variations is not clear, nor is it clear how these failure rates should be interpreted and used. Some contend that the quality of component and system maintenance varies widely between plants. It is further contended that maintenance has a large effect on component failures and hence this factor alone could account for much of the plant-to-plant variation. However, some components, e.g., those inside the primary containment, are not amenable to maintenance; hence, for these components (e.g., control rods, etc.) there should not be the large variation that there in fact appears to be. Conversely, some easily accessible components or subsystems would be expected to vary dependent upon maintenance, e.g., the diesel-generators. Based on the above, it is suggested that some components be described by plant-specific failure rates (e.g., the diesel-generators); however, for other components (e.g., valves) it is proposed that, in spite of apparent plant-to-plant variations, some nominal values be chosen for all plants, at least for screening purposes. For example, some valve failures may be preventable by maintenance,

e.g., keeping valve limit switches and torques switches in proper adjustment. Other failure types seem to have little association with maintenance and the failures would probably occur at the same frequency irregardless of how much or little preventative maintenance is performed. These non-maintenance related types of failure could be, for example, the failure of a valve due to vibration or insufficient design margin, or component internal wearout.

Where plant-specific information is desired, the LER Analysis Report failure rates median values may be used as an indication for each plant. However, where there is a large deviation of some plants from others, the data should first be rechecked to see if these are explainable causes. It may be that some failures occurred in a group of a cause that has since been corrected. If so, the failure rate may appropriately need to be recalculated minus these failures.

LIMITATIONS OF CALCULATED COMPONENT FAILURE RATE ACCURACY

There is considerable uncertainty when statistically "summarizing" phenomena having large and diverse variation such as component failures. To derive failure rates we statistically abstract historical data from a comparatively small quantity of failures. Statistical and prediction techniques can be used when our sample of failures is representative of future failures. There is danger that the sample of component failures which one gathers to make predictions may not be representative of future failures. More importantly however, there are innumerable nuances or subtleties of failures which may not be adequately described

in "summarized" i.e., statistical information. For the above reasons it is recommended that the more basic or detailed data, e.g., the raw data in the LER Data Summary analysis reports themselves be used when anything beyond gross failure rates are needed. The LER derived failure rates are themselves somewhat gross, but they do indicate the limitation on our ability to calculate and characterize component failure rates. We seem to be limited by the fact that each component application or use is somewhat different, therefore, we have a variety of "one-of-a-kind" systems or plants from which we are trying to derive component failure rates and failure rate information.

The whole concept of random failures as applied to nuclear plant safety system components should be critically questioned when determining and using failure rates. In addition to the problem of quantities of subclasses of components, as discussed in a prior section, there are physical and operational factors involved in nuclear plants and nuclear plant safety systems which can affect and change any particular component application away from the concept of some single failure distributions. This might not be a problem if we had sufficient data for each influencing factor. However, some of the factors (e.g., operational and environmental factors) may be only minimally known and therefore cannot be convoluted with the result that our final distribution may not be representative of the actual failure distribution. Because so much is unknown about nuclear plant component failures, particularly the uncharacterized (perhaps uncharacterizable) failure factors the final selection for critical components may need to be made on a more reasoned basis which may involve considerable amounts of engineering judgment.

There are many factors which mitigate against "random" component failures. It has previously been indicated that failures and failure rate calculations are affected by extrinsic, intrinsic and calculation errors or deficiencies and there may be more extrinsic and calculation factors causing systematic component failure rate variations than intrinsic random failures. The extrinsic factors are those affected by environment and operation or use. The intrinsic factors are what we traditionally model. The intrinsic factors are the so called "primary" component failures. Extrinsic factors can cause or result in "Secondary" component failures.

RECOMMENDED COMPONENT FAILURE RATES

The component failure rates as given in tables III 4-1 and III 4-2 of WASH-1400 are recommended to be used for generic rates except as supplemented or modified by new findings from the LER Evaluation Program. The referenced WASH-1400 tables are shown in this report as Tables 3A and 3B. The table entries are marked with an "R" where they have been revised from the WASH-1400 value, and with an "A" where they are additional to the original WASH-1400 tables. The modifications and additions are obtained mainly from the LER Summary Data NUREG results (refer Table 2). The assessed range is provided by the calculated maximum and minimum plant specific component failure rates. The mean is the geometric mean of these two values. The error factor is the multiplier/divisor of the mean to provide approximate bounds. The error factor is rounded off to 3 or 10 to allow using integer exponents for failure rates. A problem with the LER derived failure rates is that only the major components

The result of the quantitative evaluations will be the desired accident sequence probability that is to be associated with the accident results determined for that sequence." [1]

Fault Tree Terminology

A fault tree is a graphical representation of an interrelated set of Boolean equations. Each unique event in the fault tree is represented by a unique Boolean variable. The types of events depicted in the fault tree include the top event, secondary events and primary events. Secondary events correspond to gates of the fault tree and have associated inputs. Primary events correspond to the basic component failures represented in the fault tree and do not have any associated inputs. A cut set of a fault tree is a set of primary events that cause the occurrence of the top event. A cut set is called a minimal cut set if it ceases to be a cut set when any of its primary events are removed. The set of all minimal cut sets for a fault tree denotes all of the fundamental ways in which the top event of the fault tree can occur. Since the minimal cut sets are in terms of primary events and since in general there exists data to quantify the primary events, the top event of the fault tree can be quantified by use of the set of minimal cut sets. For the accident sequence fault tree, the top event is the occurrence of the accident sequence. Quantifying the top event of the accident sequence fault tree is, in effect, quantifying the accident sequence.

Accounting for System Successes

Returning to the example accident sequence fault tree, F , once the set of minimal cut sets for F have been determined,

14

the minimal cut sets are examined to determine if any of the minimal cut sets can cause the failure of system 3. The event "system 3 fails" has an associated fault tree with the top event representing the failure of system 3. If the set of minimal cut sets for this fault tree is in Boolean expression form, the Boolean expression can be complemented. The complemented expression represents the set of minimal cut sets for the nonoccurrence of the top event, which is the success of system 3. (If Boolean expressions are not used, the dual fault tree represents the success of system 3. The dual fault tree is obtained by replacing AND gates by OR gates and OR gates by AND gates in the original fault tree. The dual primary events represent the nonoccurrence of the original primary events. [2] The set of all minimal cut sets for the dual fault tree represents all of the fundamental ways the system can succeed.) If the Boolean expression representing the set of minimal cut sets for F is logically intersected with the complemented Boolean expression representing the success of system 3, then the identity $P^*/P = \emptyset$ will eliminate any minimal cut set of F which can cause system 3 to fail. It is necessary to remove the minimal cut sets that cause system 3 to fail, and hence contradict the "system 3 success" event in the event tree sequence, before proceeding with the quantitative analysis of the accident sequence. Otherwise, an overly conservative probability will be computed.

Preliminary Quantification of Accident Sequences

Let the set of minimal cut sets for F which do not imply the failure of system 3 be represented by the Boolean equation:

$$T = M_1 + M_2 + \dots + M_m$$

15

Assuming statistical independence of the primary events, the probability of occurrence of minimal cut set M_i , $1 \leq i \leq m$, is computed by multiplying the probabilities of occurrence of each primary event in M_i . Minimal cut sets with a probability less than 10^{-10} are discarded. If $P(M_i)$ represents the probability of occurrence of minimal cut set M_i , then the rare event approximation can be used to compute an upper bound on the probability of occurrence of T ; i.e., $P(T) \leq \sum_{i=1}^m P(M_i)$. Since the fault tree models the accident sequence, this approximation is also true for the accident sequence. Note that at this step of the analysis only point values are being used; i.e., the probability of occurrence of a primary event is assumed to be a fixed value. Subsequent steps in the analysis will deal with a probability distribution describing the various data parameters. However, the point value approach is suitable for determining the dominant accident sequences, which are those that have a probabilistic upper bound greater than or equal to 10^{-6} . If the accident sequence has a probability less than 10^{-6} , it is not further analyzed.

If the accident sequence is a dominant accident sequence, the minimal cut sets of the accident sequence fault tree are ranked based on probability of occurrence, from highest to lowest. The primary events represented in the set of minimal cut sets are also ranked. A primary event is considered important if the computed upper bound on the probability of occurrence of the accident sequence is highly sensitive to the probability assigned to that event. This is determined by evaluating the partial

derivative of the upper bound on the probability of the accident sequence with respect to the probability of each primary event. The product of the partial derivative and the probability of the primary event measures the contribution of the event to the upper bound on the probability of the accident sequence. (When normalized, this measure of the importance of each event is called the Fussell-Vesely measure.) After this measure is computed for each primary event, the primary events are ranked in importance, from highest to lowest. Depending on the number of primary events involved, it may be necessary to rank only the most important primary events.

Quantitative Analysis of Dominant Accident Sequences

In order to take into account the variations and uncertainties in the various data parameters, a Monte Carlo simulation is performed on the dominant accident sequences. A median probability and an error factor are associated with each primary event represented in the set of minimal cut sets for the accident sequence fault tree. The error factor is used to define a possible range of values for a particular random variable. If the median probability of occurrence of some primary event X is $X_{0.5}$, then the possible values of the random variable representing the occurrence of X is between $X_{0.5}/f$ and $X_{0.5} \cdot f$, where f is the associated error factor. The median probability and the error factor are used to calculate upper and lower bounds which are assumed to be the 95th and 5th percentile points of a log-normal distribution. From this, the parameters of the probability distribution are calculated for the occurrence of the primary event. The applicability of the log-normal

distribution for describing the various data ranges is discussed in the Reactor Safety Study (1, pp. II-42, II-43).

By taking a random sample from the probability distribution for each primary event, a total probability is computed for the top event of the accident sequence fault tree (by using the rare event approximation and the Boolean equation for the top event, as described in the previous section for point values). By repeating this for a total of n times, a distribution of accident sequence probabilities is found. For the resulting distribution, a mean and standard deviation, as well as the 5th, 50th, and 95th percentile points, are found. These latter are then used to compute the equivalent median and error factor for the probability of the top event of the accident sequence. This output can be used to provide a relative ranking of the dominant accident sequences involving a particular initiating event.

References

1. Reactor Safety Study, WASH-1400, 1975.
2. Barlow, R. E., and Chatterjee, P., Introduction to Fault Tree Analysis, ORC73-30, University of California, Berkeley, CA, 1973.

important to safety systems are included. Therefore, many of the components on fault trees will have to be quantified using old, i.e., WASH-1400 data. It is expected that additional new or revised failure rate data will be periodically forthcoming from current data analysis programs. Therefore, this list of failure rates is subject to change.

The attached lists of failure rates are very general and do not cover specific or peculiar instances of component use. And, as has been noted, we are not able at this time to adequately characterize failure rates to cover all instances of use. Further extensive statistical and qualitative or descriptive data exists (LERs and LER Data Summary NUREGs) and these should be referenced and used where more detail is required. Therefore, it is emphasized that when a component is found critical to a system or sequence that additional or supplemental failure rate information be derived from the LERs or the LER Data Summary NUREGs. The critical component may have peculiar failure modes which other uses of the component may not have.

COMMON MODE FAILURE MODELING

Methods or techniques must be used in system analysis to recognize and account for the possibility of multiple component failures resulting from commonality within or between components. This commonality may be extrinsic or intrinsic to the component. Examples of an extrinsic common mode failure might be the failure of several similar components due to failure of a common interfacing system or function (e.g., a cooling system). An example of an intrinsic common mode failure may be

the miscalibration of several redundant pressure sensor switches by one technician due to faulty equipment, instruction, or calibration procedures. A further (though perhaps questionable) example of intrinsic common mode failure may be common fabrication or manufacturing defects involving an entire production run of components. These defective components may subsequently fail as a group after an abbreviated lifetime or while in a particular operating mode. The validity of including these manufacturing/fabrication type problems as "common mode failures" is questionable and is discussed further below.

Several methods can be used to account for common mode failures in reliability assessments. One of the frequently used methods involves arbitrarily reducing by a factor or percentage a part of all component redundancy within a safety system when assessing its reliability. This method determines an unavailability for the redundant component somewhere between two extremes or bounds. The possible bounds are referred to as the totally coupled case and the totally uncoupled case. The "totally coupled" case refers to that condition where, because of common mode failures, when one redundant component fails, the others fail also. The "totally uncoupled" case results when, because of lack of common mode interactions, the components always fail completely independently of one another. These "coupling factor" methods can produce questionable results for several reasons. For example, if the failures are due to a manufacturing, fabrication, or installation error causing early failures, then we might simply have a case of using the wrong failure rate for the component in question. One cannot correct a wrong failure rate by use

of an artificial correction factor for redundant applications of the component. Furthermore, one should account for "common mode" influences on all possible cut sets which can lead to system or function failure. This would involve adding coupling factors to all cut sets that are possibly coupled even when these consisted of diverse components. That is, an interfacing system (e.g., cooling system) failure could conceivably fail a pump in one redundant train and a motorized valve in the other train of the redundant system. Therefore, one could argue that the coupling factor concept should be expanded and used on all cut sets having possible interrelationship. The coupling would eventually become excessive resulting in overly conservative answers.

A second (and recommended) method of accounting for common mode failure is to address the potential for physically caused common mode failure as a part of and at the time of the system analysis. The analyst should look for the special circumstances or factors which can couple together multiple systems or components. An example of a common mode failure could be the physically disabling of redundant systems caused by a proximate disruptive pipe failure. Another example could involve the common cooling or common diesel oil supplied to multiple DGs with the possibility of multiple failure when losing the common cooling or when contaminating the common fuel oil supply. Again, any failures of this type would depend on configuration and circumstances of component use; therefore, assuming particular fixed coupling factors may be too conservative. An analysis may be just as unbelievable if it appears to have excessive conservatism through applying coupling factors indiscriminately to all

redundant components as it would be unbelievable for assuming no coupling when such potential coupling could or does exist. In other words, where the coupling is physical, this should be found out and noted by the analyst himself during his analysis of the system. This common mode examination is really a normal and expected part of a thorough and competent system reliability analysis.

An arbitrarily assigned coupling factor should be used sparingly and only as a last resort. When the analysis must be truncated before all interactions can be found, then an estimated answer might be obtained with Beta factors or some other technique such as determining the geometric mean of the totally coupled and totally uncoupled values of the redundant system reliability.

The coupling factors to be used for human caused common modes, e.g., miscalibrations of sensors or switches, etc. is highly variable and is to a large extent subjective. Coupling factors for human caused common modes are suggested in the Draft Human Factors Handbook, NUREG/CR-1278.

REFERENCES

1. W. H. Hubble, C. F. Miller, Data Summaries of Licensee Event Reports of Valves in U.S. Commercial Nuclear Power Plants - January 1, 1976 to December 31, 1978, NUREG/CR-1363, EGG-EA-5125, May 1980.
2. W. H. Sullivan, J. P. Poloski, Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants - January 1, 1972 to April 30, 1978, NUREG/CR-1205, EGG-EA-5044, January 1980.
3. W. H. Hubble, C. H. Miller, Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants - January 1, 1972 to April 30, 1978, NUREG/CR-1331, EGG-EA-5079, February 1980.
4. J. P. Poloski, W. H. Sullivan, Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants - January 1, 1976 to December 31, 1978, NUREG/CR-1362, EGG-EA-5092, March 1980.
5. D. W. Sams, M. Trojovski, Data Summaries of Licensee Event Reports of Containment Penetrations at U.S. Commercial Nuclear Power Plants - January 1, 1972 to December 30, 1978, EGG-EA-5157, Draft Report.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
SYMPTOM	GENERAL ALARM	SYMPTOM	MEAS.	METHODS	WASH 1400	WESTHOUSE USE	USE TA	FAILURE RATE AND CONFID.	REMARKS
FAIL TO OPEN			7E 6	3.5E 7				1.6E 6(9.8) 1.4E 6(9.8)	
FAIL TO OPEN			7E 6	2.2E 6					
FAIL TO OPEN			43F 2		3F 5 3E 3(10)	3E 5 3.3F 4		1.5E 6(29.9)B 3E 2(4.3) 3E 3(10)	9.2E 3D 1.3E 5D
FAIL TO OPEN			1.5E 3						
FAIL TO OPEN			7.4E 7 3.2E 6 1.2E 7 2.3E 6		1E 4(3) 11E 3(3)	43E 4		2.3E 6(8.9) 1.4E 4(10) 4.3E 6(10) 4E 4(8.9)	
FAIL TO OPEN			9.1E 7 3.4E 7		41E 4(3)	2.7E 6		3.5E 4(4) 5.7E 6(35)	
FAIL TO OPEN			3E 7		{ 41E 5(3) }			4.5E 6(71.1) 4.5E 6(71.1) 8.4E 6(11.4)	
FAIL TO OPEN			3.5E 5		41E 4(3)			2E 7(3.3) 9.4E 6(36.5)	
FAIL TO OPEN			2.5E 6		43E 4(3)		42E 5	4.2E 6(11.9) 4.2E 6(11.9)	
FAIL TO OPEN			3.5E 5			44E 6	(5-10)E 6	4.4E 6(2.7)	
FAIL TO OPEN			3.4E 5			44E 7	(5-20)E 6	1.7E 7(5.7)	
FAIL TO OPEN			7.7E 5				(5-10)E 6	1.7E 6(5.8)	

3. A "+" preceding a failure rate denotes failure-per-demand.
All other failure rates are failure-per-hour.

NOTE:
1. THESE SHEETS ON FAILURE FAILS TO HOLD THE FOLLOWING:
A. THESE 95% CONFIDENCE BOUND
B. THE STATE FAILURE CHANGE
C. THE FAILURE RATE
D. THE 95% CONFIDENCE BOUND
E. THE FAILURE RATE FOR THE 95% CONFIDENCE BOUND

THE NUMBER OF BOUNDS, IN PARENTHESES, FOLLOWING FAILURE RATES TO HOLD THE 95% CONFIDENCE BOUND, FOR EXAMPLE, 95% MEANS ONE BOUND TO HOLD THE 95% CONFIDENCE BOUND BY XX TO OBTAIN THE 95% CONFIDENCE BOUND AND TO HOLD THE BOUND BY XX TO OBTAIN THE 95% CONFIDENCE BOUND, A SYMBOL TO HOLD TO OBTAIN THE 95% CONFIDENCE BOUND, A SYMBOL TO HOLD TO OBTAIN THE 95% CONFIDENCE BOUND.

TABLE 2

YPS	COMPONENT & FAILURE MODE	FAIL QTY	EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF	FACTORS FOR N555			WASH-1400			
								B	C	W	G			
6-8	REACTOR SCRAM RODS FAIL TO SCRAM TO 96%	1 D	1E-3	1E-3	3E-2	3E-5	1E-3	1	20*	12*	2		1E-4	3
"	"	3 D	4E-4	1E-3	5E-2	5E-5	6E-4	2						
"	"	(WCF)												
"	"	1 D	1E-3	1E-3	3E-2	3E-5	1E-3	1	20*	12*	2			
"	"	8 D	3E-4	3E-3	5E-2	1E-4	8E-4	3						
2-8	FAIL TO SCRAM TO 96%	3 D	3E-4	6E-4	1E-2	4E-5	4E-4	1	6*	5*	1			
"	"	7 D	1E-4	6E-4	3E-2	5E-5	3E-4	2						
"	"	(WCF)												
"	"	3 D	3E-4	6E-4	1E-2	4E-5	4E-4	1	7*	6*	1			
"	"	14 D	1E-4	1E-2	3E-3	1E-4	1E-3	9						
6-8	FAIL TO INSERT NORMAL SHUTDOWN	0 D	-	-	3E-2	1E-4	-		3*	5*	2*			
1 D		9E-4	9E-4	2E-2	3E-5	9E-4	1							
2-8	"	0 D	-	-	3E-2	6E-5	-		3*	6*	2*			
2 D		3E-4	4E-4	8E-3	2E-5	4E-4	1							
6-8	FAIL PWR CHANGE/TESTING	2 D	1E-3	1E-3	6E-2	5E-5	1E-3	1	2	6*	1			
"	"	1 D	4E-4	4E-4	5E-4	4E-6	4E-4	1						
"	"	(WCF)												
"	"	48 D	8E-4	4E-2	6E-2	1E-3	6E-3	7	3	.2	.6			
"	"	1 D	4E-4	4E-4	5E-4	4E-6	4E-4	1						
2-8	FAIL PWR CHANGE/TESTING	2 D	1E-3	1E-3	6E-2	3E-5	1E-3	1	2	7*	.8			
"	"	1 D	1E-4	1E-4	5E-4	2E-6	1E-4	1						
"	"	(WCF)												
"	"	49 D	8E-4	4E-2	6E-2	8E-4	6E-3	7	3	.2	.6			
"	"	1 D	1E-4	1E-4	5E-4	2E-6	1E-4	1						
6-8	DROPPED ROD (PWR)	13 S	9E-7	4E-6	1E-4	5E-7	2E-6	2	1	3	.2			
"	"	(WCF)												
"	"	89 S	9E-7	4E-5	1E-4	3E-6	6E-6	7	3	.8	.2			
2-8	"	15 S	6E-7	4E-6	1E-4	3E-7	2E-6	3	2	3	.1			
"	"	(WCF)												
"	"	105 S	6E-7	4E-5	1E-4	2E-6	5E-6	8	3	.9	.2			
6-8	UNCOUPLED/OVERTRAVEL (BWR)	14 S	4E-7	4E-6	7E-6	3E-7	1E-6	3						
2-8	"	27 S	2E-7	2E-6	3E-6	3E-7	6E-7	4						
6-8	IMPROPER MOVEMENT-PERSONN.	2 S	1E-6	2E-6	1E-4	7E-8	2E-6	1	4	6*	3*			
"	"	5 S	4E-7	1E-6	7E-6	1E-7	6E-7	2						
2-8	"	13 S	6E-7	2E-6	1E-4	3E-7	1E-6	2	3	.4	.5			
"	"	9 S	2E-7	1E-6	2E-6	1E-7	4E-7	2						
2-8	IMPROP. MOVE-PERSONN/HDWARE	13 S	6E-7	2E-6	1E-4	3E-7	1E-6	2	3	.4	.5			
"	"	13 S	2E-7	2E-6	2E-6	1E-7	5E-7	3						
6-8	FAIL FULL INSERT W. SCRAM	1 D	1E-3	1E-3	3E-2	3E-5	1E-3	1	20*	12*	2			
"	"	51 D	4E-4	2E-2	5E-2	8E-4	3E-3	7						
"	"	(WCF)												
"	"	1 D	1E-3	1E-3	3E-2	3E-5	1E-3	1	20*	12*	2			
"	"	56 D	3E-4	2E-2	5E-2	9E-4	2E-3	9						
2-8	"	3 D	3E-4	6E-4	1E-2	4E-5	4E-4	1	7*	6*	1			
"	"	178 D	1E-4	2E-2	3E-2	1E-3	2E-3	1						
"	"	(WCF)												
"	"	3 D	3E-4	6E-4	1E-2	4E-5	4E-4	1	7*	6*	1			
"	"	185 D	1E-4	2E-2	3E-2	1E-3	2E-3	13						

6-8	FAIL TO MOVE NON SCRAM	2	D	5E-4	8E-4	6E-2	3E-5	6E-4	1	2	7*	1	
		2	D	1E-4	4E-4	4E-4	6E-6	2E-4	2				
"	"	(WCF)	48	D	5E-4	1E-2	4E-2	8E-4	3E-3	6	2	.2	.7
			2	D	1E-4	4E-4	4E-4	6E-6	2E-4	2			
2-8	"		2	D	5E-4	8E-4	6E-2	2E-5	6E-4	1	2	8*	.9
			3	D	5E-5	1E-4	4E-4	5E-6	8E-5	2			
"	"	(WCF)	49	D	5E-4	1E-2	6E-2	4E-4	3E-3	6	3	.2	.6
			3	D	5E-5	1E-4	4E-4	5E-6	8E-5	2			
6-8	INADVERTENT MOTION		13	S	9E-7	4E-6	1E-4	5E-7	2E-6	2	1	3	.1
			14	S	4E-7	4E-6	7E-6	3E-7	1E-6	3			
"	"	(WCF)	91	S	9E-7	4E-5	1E-4	3E-6	6E-6	7	3	.8	.2
			19	S	4E-7	4E-6	7E-6	4E-7	1E-6	3			
2-8	"		15	S	6E-7	4E-6	1E-4	3E-7	2E-6	3	2	3	.1
			27	S	2E-7	2E-6	3E-6	3E-7	7E-7	3			
"	"	(WCF)	118	S	6E-7	4E-5	1E-4	3E-6	5E-6	9	3	.8	.3
			40	S	2E-7	3E-6	2E-6	4E-7	7E-7	4			
6-8	AGG STD T.S. PLANTS		12	S	1E-6	6E-6	1E-4	2E-6	3E-6	2	2	1	.2
			2	S	1E-6	1E-6	3E-6	7E-7	1E-6	1			
"	"	(WCF)	89	S	9E-7	1E-4	1E-4	1E-5	1E-5	10	6	.4	.6
			3	S	1E-6	1E-6		1E-6	1E-6	1			
6-8	AGG NONSTD T.S. PLANTS		9	S	9E-7	5E-6	6E-6	5E-7	2E-6	2	1	3	1
			72	S	4E-7	2E-5	2E-6	2E-6	3E-6	7			
"	"	(WCF)	59	S	1E-6	2E-5	5E-6	3E-6	5E-6	4	3	4*	.5
			81	S	4E-7	2E-5	2E-6	2E-6	3E-6	8			
6-8	AGG FAILURES ALL		21	S	9E-7	6E-6	1E-4	8E-7	2E-6	3	1	2	.6
			74	S	5E-7	2E-5	3E-6	2E-6	3E-6	7			
"	"	(WCF)	148	S	9E-7	1E-4	1E-4	5E-6	1E-5	10	3	.6	.4
			84	S	4E-7	2E-5	2E-6	2E-6	2E-6	8			
2-8	AGG FAILURES ALL		29	S	5E-7	6E-7	1E-4	6E-7	2E-6	4	1	1	.7
			258	S	2E-7	2E-5	3E-6	3E-6	2E-6	12			
"	"	(WCF)	184	S	5E-7	1E-4	1E-4	4E-6	7E-6	1	3	.6	.5
			282	S	3E-7	2E-5	1E-6	3E-6	3E-6	10			

** NOTE FOR SCRAM RODS. THE SCRAM ROD TABULATIONS ABOVE DIFFER FROM OTHER COMPONENTS IN THIS TABLE INsofar AS SEPARATE FAILURE RATES ARE CALCULATED FOR PWR'S (THE FIRST LINE OF EACH SCRAM ROD FAILURE MODE ENTRY) AND BWR'S (THE SECOND LINE). THE CALCULATIONS AND RATES ARE KEPT SEPARATE BECAUSE BWR SCRAM RODS AND DRIVE MECHANISM'S DIFFER EXTENSIVELY FROM THE GENERAL TYPE USED BY THE THREE PWR VENDERS.

YRS	COMPONENT & FAILURE MODE	FAIL QTY	EXP MIN	EXP MAX	UD MAX	ALL AVF	GEOM MEAN/EF	FACTORS		FOR NSSS		WASH-1402			
								B	C	W	G				
	<u>DIESEL GENERATORS</u>														
6-8	DOES NOT START (WKLY TEST)	186	D	2E-3	1E-1	4E-1	1E-2	2E-2	8	1	1	.6	1	3E-2	3
"	" (MONTHLY TEST)	186	D	9E-3	5E-1	8E-2	4E-2	7E-2	8	1	1	.6	1		
"	DOES NOT CONTINUE (WKLY TEST)	112	O	2E-3	5E-2	4E-1	6E-3	9E-3	6	1	2	.7	1	3E-3	10
"	" (MONTHLY TEST)	112	O	7E-3	2E-1	2E-1	3E-2	4E-2	6	1	2	.7	1		

YPS	COMPONENT & FAILURE MODE	FAIL QTY	EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF	FACTORS FOR MSSS				WASH-1400	
								B	C	W	G		
RUNNING PUMPS													
2-8	DOES NOT OPERATE	23 D	6E-6	2E-4	2E-3	5E-6	3E-5	6	1	.7	.4	2	3E-5 10
"	" (WCF)	65 D	6E-6	3E-4	2E-3	1E-5	4E-5	8	1	1	.5	1	
6-8	"	8 D	1E-5	8E-5	2E-3	3E-6	3E-5	3	2	3	.6	2	
"	" (WCF)	46 D	1E-5	3E-4	2E-3	2E-5	6E-5	5	1	1	.6	1	
ALTERNATING PUMPS													
2-8	DOES NOT START	15 D	1E-3	2E-2	3E-1	5E-4	4E-3	4	3	.6	1	.6	1E-3 3
"	" (WCF)	56 D	1E-3	2E-2	3E-1	2E-3	4E-3	4	2	1	.9	.9	
6-8	"	10 D	3E-3	2E-2	3E-1	6E-4	7E-3	3	3	.8	1	.9	
"	" (WCF)	32 D	2E-3	2E-2	3E-1	2E-3	6E-3	3	1	1	1	.6	
2-8	LEAKAGE RUPTURE	45 D	3E-6	1E-4	2E-3	5E-6	2E-5	6	3	.8	2	.2	
6-8	"	25 D	8E-6	9E-5	2E-3	6E-6	3E-5	3	.5	.6	2	.4	
2-8	LOSS OF FUNCTION	36 D	3E-6	7E-5	2E-3	4E-6	2E-5	4	.8	3	.9	.7	
"	" (WCF)	39 D	3E-6	7E-5	2E-3	5E-6	2E-5	4	.7	3	.8	.9	
6-8	"	28 D	8E-6	7E-5	2E-3	6E-6	2E-5	3	.8	2	1	.5	
"	" (WCF)	29 D	8E-6	7E-5	2E-3	7E-6	2E-5	3	.8	2	1	.6	
2-8	DOES NOT CONTINUE TO RUN	77 D	5E-6	9E-5	2E-3	9E-6	2E-5	4	.4	.8	1	1	3E-5 10
"	" (WCF)	94 D	5E-6	1E-4	2E-3	1E-5	2E-5	5	.6	.7	1	1	
6-8	"	42 D	1E-5	7E-5	2E-3	1E-5	3E-5	3	.3	.9	1	.6	
"	" (WCF)	55 D	1E-5	8E-5	2E-3	1E-5	3E-5	3	.6	.8	1	.5	
2-8	DOES NOT OPERATE GIVEN START	158 D	5E-6	1E-4	2E-3	2E-5	2E-5	5	.5	1	1	.7	
"	" (WCF)	178 D	5E-6	2E-4	2E-3	2E-5	3E-5	6	.6	1	1	.8	
6-8	"	95 D	1E-5	1E-4	2E-3	2E-5	3E-5	3	.5	1	1	.5	
"	" (WCF)	109 D	1E-5	2E-4	2E-3	3E-5	4E-5	4	.6	1	1	.5	
2-8	DOES NOT OPERATE	173 S	5E-6	1E-4	2E-3	2E-5	3E-5	5	.7	1	1	.7	
"	" (WCF)	234 S	5E-6	2E-4	2E-3	3E-5	3E-5	6	.9	1	1	.8	
6-8	"	105 S	1E-5	1E-4	2E-3	2E-5	4E-5	4	.8	1	1	.5	
"	" (WCF)	141 S	8E-6	2E-4	2E-3	3E-5	4E-5	4	.7	1	1	.6	
STANDBY PUMPS													
2-8	DOES NOT START (MOT)	15 D	7E-4	1E-2	4E-1	5E-4	3E-3	4	2	2	2	.7	1E-3 3
"	" (WCF)	98 D	2E-3	7E-2	3E-1	4E-3	1E-2	6	1	1	1	.9	
"	" (TURB)	18 D	7E-3	1E-1	4E-1	4E-3	3E-2	4	3	1	1	.1	1E-3 3
"	" (WCF)	57 D	7E-3	4E-1	1E-1	1E-2	5E-2	8	2	.8	1	.5	
"	" (DIESEL)	1 D	4E-2	4E-2	6E-2	5E-3	4E-2	1			2	.8	
"	" (WCF)	8 D	1E-2	2E-1	6E-2	4E-2	5E-2	4			1	.4	
6-8	DOES NOT START (MOT)	6 D	4E-3	1E-2	4E-1	4E-4	8E-3	2	5	5	2	.4	
"	" (WCF)	41 D	2E-3	7E-2	4E-1	3E-3	1E-2	6	2	.7	1	.9	
"	" (TURB)	11 D	3E-2	1E-1	3E-1	5E-3	6E-2	2	4	2	1	.7	
"	" (WCF)	34 D	2E-2	4E-1	1E-1	2E-2	9E-2	5	3	.9	1	.2	
"	" (DIESEL)	1 D	4E-2	4E-2	1E-1	9E-3	4E-2	1			1	.12	
"	" (WCF)	6 D	4E-2	2E-1	1E-1	5E-2	8E-2	2			1	.7	
2-8	DOES NOT OPERATE (MOT)	60 S	2E-6	3E-5	1E-3	4E-6	8E-6	4	1	.9	1	.7	3E-5 10
"	" (WCF)	167 S	3E-6	1E-4	1E-3	1E-5	2E-5	7	1	.5	1	.8	
"	" (TURB)	43 S	2E-5	5E-4	9E-3	2E-5	9E-5	6	3	2	.9	.7	3E-5 10
"	" (WCF)	106 S	2E-5	2E-3	9E-3	5E-5	2E-4	8	3	1	.9	.8	
"	" (DIESEL)	2 S	2E-4	2E-4	1E-4	2E-5	2E-4	1			2	.4	
"	" (WCF)	12 S	3E-5	8E-4	1E-4	1E-4	1E-4	6			1	.2	
6-8	DOES NOT OPERATE (MOT)	34 S	3E-6	6E-5	1E-3	5E-6	1E-5	5	1	.3	2	.6	
"	" (WCF)	80 S	6E-6	1E-4	1E-3	1E-5	3E-5	5	1	.2	1	.8	
"	" (TURB)	29 S	3E-5	1E-3	9E-3	3E-5	2E-4	6	3	2	.7	.5	
"	" (WCF)	71 S	3E-5	3E-3	9E-3	6E-5	3E-4	10	3	1	.9	.6	
"	" (DIESEL)	2 S	2E-4	2E-4	2E-4	4E-5	2E-4	1			1	.6	
"	" (WCF)	10 S	8E-5	7E-4	2E-4	2E-4	2E-4	3			1	.4	

YRS	COMPONENT & FAILURE MODE	FAIL QTY	EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF	FACTORS FOR NSSS*				WASH-1400			
								B	C	W	G				
6-8	MOV FAIL TO OPERATE	128	D	1E-3	6E-2	5E-2	4E-3	9E-3	7	1	.6	.6	1	1E-3	3
	" " (WCF)	180	D	1E-3	7E-2	5E-2	6E-3	9E-3	7	.9	.8	.6	1		
	LEAK EXTERNALLY PLUGGED (WCF)	7	S	6E-7	2E-6	8E-5	1E-7	1E-6	2	1	7M	1	.7	1E-8	10
6-8	REMOTE & MOV FAIL TO OPERATE	165	D	1E-3	6E-2	5E-2	5E-3	9E-3	7	1	.6	.6	1		
	" " (WCF)	234	D	1E-3	7E-2	5E-2	7E-3	9E-3	7	.9	1	.6	1		
	LEAK EXTERNALLY PLUGGED (WCF)	12	S	6E-7	2E-6	8E-5	2E-7	1E-6	2	.8	4	1	1		
6-8	AIR OPERATED VALVE FAIL TO OPERATE	3	D	7E-3	6E-2	3E-1	7E-4	2E-2	3	9	4M	.8	4	3E-4	3
	" " (WCF)	10	D	7E-3	8E-2	4E-1	2E-3	2E-2	4	4	.6	.7	3		
	LEAK EXTERNALLY PLUGGED (WCF)	2	S	3E-6	2E-5	8E-4	2E-7	8E-6	2	22M	7M	1	2	1E-8	10
6-8	MANUAL VALVE FAIL TO OPERATE	3	D	1E-3	2E-3	7E-2	8E-5	2E-3	1	2	3	2M	1		
	LEAK EXTERNALLY PLUGGED (WCF)	1	S	6E-7	6E-7	1E-4	1E-8	6E-7	1	21M	8	6M	11M	1E-8	10
	CHECK VALVE LEAK EXTERNALLY PLUGGED (WCF)	3	S	4E-6	5E-6	7E-5	5E-8	4E-6	1	6	7M	2M	1	1E-8	10
6-8	PRM PRIMARY SAFETY PREMATURE OPEN	7	S	1E-5	4E-5	2E-3	3E-6	2E-5	2	3M	2	1		1E-5	3
	FAIL TO OPEN (WCF)	6	D	2E-2	2E-1	8E-1	6E-3	6E-2	3	5M	2	.9		1E-5	3
	FAIL TO RESEAT (WCF)	17	D	3E-3	2E-2	2E-1	5E-3	7E-3	2						
6-8	FAIL TO RESEAT (WCF)	18	D	2E-3	2E-2	2E-1	5E-3	6E-3	3						
	PREMATURE OPEN (WCF)	21	S	9E-6	4E-5	6E-5	6E-6	2E-5	2					1E-5	3
	PREMATURE OPEN (WCF)	22	S	9E-6	5E-5	6E-5	6E-6	2E-5	3						

NOTES FOR TABLE 2

ABBREVIATIONS

1. YRS - DENOTES TIME INTERVAL SAMPLED FOR LER FAILURES
6-8 DENOTES SAMPLE YEARS 1976 THRU 1978
2-8 DENOTES SAMPLE YEARS 1972 THRU 1978
2. COMPONENT & FAILURE MODES - DENOTES COMPONENT TYPE AND MODE OF FAILURE.
THE FAILURE MODES SHOWN ARE INTRINSIC TO THE COMPONENT EXCEPT WHERE (WCF)
APPEARS. WCF MEANS "WITH COMMAND FAULTS" AND INCLUDES FAILURE OF THE COMPONENT
DUE TO BOTH INTRINSIC AND EXTERNAL OR "COMMAND" TYPE FAULTS.
3. QTY - DENOTES QUANTITY OF FAILURES REPORTED FOR THE FAILURE MODE IN THE TIME INTERVAL.
4. EXP' MIN - DENOTES MINIMUM RATE OF ALL CALCULATED PLANT FAILURE RATES
5. EXP' MAX - DENOTES MAXIMUM RATE OF ALL CALCULATED PLANT FAILURE RATES
6. UB MAX - MAXIMUM UPPER 95% CONFIDENCE BOUND FOR ALL PLANTS WITHOUT FAILURES
7. ALL AVE - FAILURE RATE DERIVED FROM ALL DATA FROM ALL PLANTS CONSIDERED AS ONE POPULATION.
8. GEOM MEAN/EF - GEOMETRIC MEAN OF THE CALCULATED EXPERIENCE MINIMUM AND EXPERIENCE MAXIMUM
AND ERROR FACTOR (EF) TO DETERMINE UPPER AND LOWER BOUNDS.
9. FACTORS FOR NSSS* - DENOTES THE APPROXIMATE MULTIPLIER TO BE USED ON THE "ALL DATA"
DATA TO GIVE THE INDIVIDUAL NSSS AVERAGE VALUE.
10. WASH-1400 - FAILURE RATES FROM APP III OF REACTOR SAFETY STUDY.
11. * MANS, UPPER 95% BOUND WHERE NO FAILURES WERE REPORTED

TABLE 3A. MECHANICAL COMPONENTS (FROM WASH-1400, TABLE III 4-1)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE			MEDIAN	EF
PUMPS (INCLUDES DRIVER):						
MOTOR & TURBINE DRIVEN (GENERIC CLASS):						
FAILURE TO START ON DEMAND:	D (A)	3E-4	3E-3	1E-3	3	
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENTS):	O	3E-6	3E-4	3E-5	10	
FAILURE TO RUN, GIVEN START, (EXTREME, POST ACCIDENT ENVIRONMENTS INSIDE CONT.):	O	1E-4	1E-2	1E-3	10	
FAILURE TO RUN, GIVEN START (POST ACCIDENT, AFTER ENVIRONMENTAL RECOVERY)	O	3E-5	3E-3	3E-4	10	
TURBINE DRIVEN PUMPS:						
FAILURE TO START ON DEMAND:	D	1E-3	1E-2	3E-3	3	A
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT)	O	1E-5	1E-4	3E-5	3	A
VALVES:						
MOTOR OPERATED:						
FAILURE TO OPERATE (INCLUDES DRIVER):	D (B)	3E-4	3E-3	1E-3	3	
FAILURE TO REMAIN OPEN (PLUG):	D (C)	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-7	1E-6	3E-7	3	
RUPTURE	S	1E-9	1E-7	1E-8	10	
SOLENOID OPERATED:						
FAILURE TO OPERATE:	D (D)	3E-4	3E-3	1E-3	3	
FAILURE TO REMAIN OPEN (PLUG):	D	3E-5	3E-4	1E-4	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
AIR-FLUID OPERATED:						
FAILURE TO OPERATE:	D (A)	1E-4	1E-3	3E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	D	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-7	1E-6	3E-7	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
CHECK VALVES:						
FAILURE TO OPEN:	D	3E-5	3E-4	1E-4	3	
INTERNAL LEAK (SEVERE):	O	1E-7	1E-6	3E-7	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
VACUUM VALVE:						
FAILURE TO OPERATE:	D	1E-5	1E-4	3E-5	3	
MANUAL VALVE:						
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3	A
FAILURE TO REMAIN OPEN (PLUG):	D	3E-5	3E-4	1E-4	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
PRIMARY SAFETY VALVES (PWR):						
FAIL TO OPEN:	D	1E-3	1E-2	3E-3	3	R
PREMATURE OPEN:	S	1E-6	1E-5	3E-6	3	R
FAIL TO RECLOSE (GIVEN VALVE OPENED)	D **	3E-3	3E-2	1E-2	3	R
PRIMARY SAFETY VALVES (BWR):						
FAIL TO OPEN:	D	3E-3	3E-2	1E-2	3	R
PREMATURE OPEN:	S	1E-6	1E-5	3E-6	3	R
FAIL TO RECLOSE (GIVEN VALVE OPENED):	D	1E-3	1E-2	3E-3	3	R

TEST VALVES, FLOW METERS, ORIFICES: FAILURE TO REMAIN OPEN (PLUG): RUPTURE:	D S	1E-4 1E-9	1E-3 1E-7	3E-4 1E-8	3 10
PIPES PIPE < 3-INCH DIAMETER (PER SECTION): RUPTURE/PLUG:	S + 0	3E-11	3E-8	1E-9	30
PIPE > 3-INCH DIAMETER (PER SECTION): RUPTURE/PLUG	S + 0	3E-12	3E-9	1E-10	30
CLUTCH, MECHANICAL: FAILURE TO OPERATE:	D (D)	1E-4	1E-3	3E-4	3
SCRAM RODS (SINGLE): FAILURE TO INSERT:	D	3E-5	3E-4	1E-4	3

NOTES:

- (A) DEMAND PROBABILITIES ARE BASED ON THE PRESENCE OF PROPER INPUT CONTROL SIGNALS. FOR TURBINE DRIVEN PUMPS THE EFFECT OF FAILURES OF VALVES, SENSORS AND OTHER AUXILIARY HARDWARE MAY RESULT IN SIGNIFICANTLY HIGHER OVERALL FAILURE RATES FOR TURBINE DRIVEN PUMP SYSTEMS.
- (B) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.
- (C) PLUG PROBABILITIES ARE GIVEN IN DEMAND PROBABILITY, AND λ JR RATES, SINCE PHENOMENA ARE GENERALLY TIME DEPENDENT, BUT PLUGGED CONDIT MAY ONLY BE DETECTED UPON A DEMAND OF THE SYSTEM.
- (D) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.
- ** THESE RATES ARE BASED ON LER'S FOR B&W PRESSURIZER PORV FAILURE TO RESEAT GIVEN THE VALVE HAS OPENED.

ABBREVIATIONS:

(1) FOR FAILURE RATE TYPE ABBREVIATIONS:

- D = DEMAND FAILURE RATE - FAILURES PER DEMAND
 O = OPERATING FAILURE RATE - FAILURES PER HOUR OF OPERATION
 S = STANDBY FAILURE RATE - FAILURES PER HOUR OF STANDBY
 S + O = STANDBY OR OPERATING FAILURE RATE - FAILURES PER HOUR

(2) REMARKS (LAST COLUMN) ABBREVIATIONS:

- R = FAILURE RATE SHOWN IS A REVISION OF WASH-1400 VALUE
 A = FAILURE RATE SHOWN IS IN ADDITION TO WASH-1400 FAILURE RATES

TABLE 3B. ELECTRICAL COMPONENTS (FROM WASH-1400, TABLE III 4-2)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN EF	
CLUTCH, ELECTRICAL: FAILURE TO OPERATE: PREMATURE DISENGAGEMENT:	D (A)	1E-4	1E-3	3E-4	3
	O	1E-7	1E-5	1E-6	10
MOTORS, ELECTRIC: FAILURE TO START: FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT): FAILURE TO RUN, GIVEN START (EXTREME ENVIRONMENT):	D (A)	1E-4	1E-3	3E-4	3
	O	3E-6	3E-5	1E-5	3
	O	1E-4	1E-2	1E-3	10
RELAYS: FAILURE TO ENERGIZE FAILURE OF NO CONTACTS TO CLOSE, GIVEN ENERGIZED: FAILURE OF NC CONTACTS BY OPENING, GIVEN NOT ENERGIZED: SHORT ACROSS NO/NC CONTACT: COIL OPEN: COIL SHORT TO POWER:	D (A)	3E-5	3E-4	1E-4	3
	O	1E-7	1E-6	3E-7	3
	O	3E-8	3E-7	1E-7	3
	O	1E-9	1E-7	1E-8	10
	O	1E-8	1E-6	1E-7	10
	O	1E-9	1E-7	1E-8	10
CIRCUIT BREAKERS: FAILURE TO TRANSFER: PREMATURE TRANSFER:	D (A)	3E-4	3E-3	1E-3	3
	O	3E-7	3E-6	1E-6	3
SWITCHES: LIMIT: FAILURE TO OPERATE:	D	1E-4	1E-3	3E-4	3
	D	3E-5	3E-4	1E-4	3
TORQUE: FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3
	D	3E-5	3E-4	1E-4	3
PRESSURE: FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3
	D	3E-6	3E-5	1E-5	3
MANUAL: FAILURE TO TRANSFER: SWITCH CONTACTS: FAILURE OF NO CONTACTS TO CLOSE GIVEN SWITCH OPERATION: FAILURE OF NC BY OPENING, GIVEN NO SWITCH OPERATION: SHORT ACROSS NO/NC CONTACT:	D	3E-6	3E-5	1E-5	3
	O	1E-8	1E-6	1E-7	10
	O	3E-9	3E-7	3E-8	10
	O	1E-9	1E-7	1E-8	10
BATTERY POWER SYSTEM (WET CELL): FAILURE TO PROVIDE PROPER OUTPUT:	S	1E-6	1E-5	3E-6	3
	O	3E-7	3E-6	1E-6	3
TRANSFORMERS: OPEN CIRCUIT PRIMARY OR SECONDARY: SHORT PRIMARY TO SECONDARY:	O	3E-7	3E-6	1E-6	3
	O	3E-7	3E-6	1E-6	3
SOLID STATE DEVICES, HIPOWER APPLICATIONS (DIODES, TRANSISTORS, ETC.): FAILS TO FUNCTION: FAILS SHORTED:	O	3E-7	3E-5	3E-6	10
	O	1E-7	1E-5	1E-6	10

SOLID STATE DEVICES, LOW POWER APPLICATIONS: FAILS TO FUNCTION: FAILS SHORTED:	0 0	1E-7 1E-8	1E-5 1E-6	1E-6 1E-7	10 10
DIESELS (COMPLETE PLANT): FAILURE TO START: FAILURE TO RUN, EMERGENCY CONDITIONS, GIVEN START:	D 0	1E-2 3E-4	1E-1 3E-2	3E-2 3E-3	3 10
DIESELS (ENGINE ONLY): FAILURE TO RUN, EMERGENCY CONDITIONS, GIVEN START	0	3E-5	3E-3	3E-4	10
INSTRUMENTATION - GENERAL (INCLUDES TRANSMITTER, AMPLIFIER AND OUTPUT DEVICE): FAILURE TO OPERATE: SHIFT IN CALIBRATION:	0 0	1E-7 3E-6	1E-5 3E-4	1E-6 3E-5	10 10
FUSES: FAILURE TO OPEN: PREMATURE OPEN:	D 0	3E-6 3E-7	3E-5 3E-6	1E-5 1E-6	3 3
WIRES (TYPICAL CIRCUITS, SEVERAL JOINTS): OPEN CIRCUIT: SHORT TO GROUND: SHORT TO POWER:	0 0 0	1E-6 3E-8 1E-9	1E-5 3E-6 1E-7	3E-6 3E-7 1E-8	3 10 10
TERMINAL BOARDS: OPEN CONNECTION: SHORT TO ADJACENT CIRCUIT:	0 0	1E-8 1E-9	1E-6 1E-7	1E-7 1E-8	10 10

NOTES

(A) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.

ABREVIATIONS:

(1) FOR FAILURE RATE TYPE ABBREVIATIONS:

D = DEMAND FAILURE RATE - FAILURES PER DEMAND

O = OPERATING FAILURE RATE - FAILURES PER HOUR OF OPERATION

S = STANDDBY FAILURE RATE - FAILURES PER HOUR OF STANDBY

S + O = STANDBY OR OPERATING FAILURE RATE - FAILURES PER HOUR

(2) REMARKS (LAST COLUMN) ABBREVIATIONS:

R = FAILURE RATE SHOWN IS A REVISION OF WASH-1400 VALUE

A = FAILURE RATE SHOWN IS IN ADDITION TO WASH-1400 FAILURE RATES

INTERIM RELIABILITY EVALUATION PROGRAM
Phase II
PROCEDURE AND SCHEDULE GUIDE

DRAFT REVISION 2
September 9, 1980

Division of Systems and Reliability Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Page of 8145-214492

1. INTRODUCTION

The Interim Reliability Evaluation Program was conceived in the aftermath of the accident at Three Mile Island Unit 2 to address the concern that differences in the design and operation of nuclear power plants may have a significant influence on the course or likelihood of core-melt accidents.

The program is responsive to the TMI Action Plan (NUREG-0660), Section IIC.

1.1 Objectives

The Interim Reliability Evaluation Program is intended to apply probabilistic safety analysis techniques to a number of nuclear power plants (ultimately all of them) with the following specific objectives: (1) Identify--in a preliminary way-- those accident sequences that dominate the contribution to the public health and safety risks originating in nuclear power plant accidents; (2) Develop a foundation for subsequent, more intensive, applications of probabilistic safety analysis or risk assessment on the subject plants; (3) Expand the cadre of experienced practitioners of risk assessment methods within the NRC and the nuclear power industry; and (4) Evolve procedures codifying the competent use of these techniques for use in the extension of IREP to all domestic light water reactor plants.

1.2 General Assumptions and Scope

Event-tree and fault-tree techniques will be employed to identify hypothetical accident sequences leading to core melt and assess their likelihood. Plant initial conditions will be confined to power generation. Consideration will be given to the possibility of misaligned valves, switches, etc., and components out of service for test and maintenance at the time of the initiating event through the mechanism of unavailability calculations for components within the fault trees. Accident scenarios will be pursued to a stable outcome: the identification of the approximate timing and magnitude of atmospheric releases, if any. Stable hot shutdown will be taken as successful core cooling; such outcomes will not be pursued to cold shutdown.

Excluded from consideration will be external events, earthquakes, fires, floods, and sabotage. Included will be random and common-cause equipment failure, operator and maintenance personnel errors of omission and commission. Operator corrective action during accidents will also be considered.

Component failures will be assumed to be binary: components either function normally or fail outright. Partial failures such as degraded bus voltage will not be considered.

It is the objective of IREP to use fully realistic assumptions on failure likelihood, system failure criteria, accident phenomenology, and the prospects for operator corrective action. However, to avoid much unproductive work, an initial

screening of accident sequences and their expected frequency of occurrence will be made with point estimate probabilities and the least conservative criteria readily available. Once candidates for the dominant sequences are thus identified, the conservatisms in the assumptions and data which influence the course or likelihood of these sequences are to be re-examined and eliminated. The final report will include a discussion of the residual uncertainties surrounding the results, including issues of completeness and modeling approximations as well as uncertainties originating in the failure rate data.

The scope of IREP team analyses do not embrace original analyses of the thermal hydraulics of core uncover, core meltdown phenomenology, of containment challenge by core melt accidents (e.g., MARCH-CORRAL runs) nor does it embrace offsite consequence analysis. The endpoint of the IREP analyses will be the classification of accident sequences according to predicted frequency and a classification according to the approximate timing of core melt and the operability of active containment systems (isolation, sprays, fan coolers, etc.). This classification will allow the accident sequences to be identified--at least tentatively--with release categories by interpolation among the release category assignments made in prior risk assessments of the most nearly comparable plants that did include formal

release category analysis, i.e., the Reactor Safety Study and the Methodology Applications Program Studies. A guidebook for this judgmental assignment of release categories is being prepared for use in IREP phase II and subsequent studies.

2. IREP TASK ELEMENTS AND SCHEDULE

Section 2.1 lists inputs to the IREP project teams. Section 2.2 tabulates task elements, required inputs and deliverable products. Section 2.3 summarizes the schedule.

2.1 Inputs to IREP teams (supplier in parenthesis)

- A. Generic Functional Event Trees and Event Tree Analysis Guide (NRC/Sandia)
- B. Final Safety Analysis Report (Plant Owner)
- C. EPRI NP-801 (Local IREP Contractor)
- D. System Design and Operation Documentation (Plant Owner)
 - System descriptions
 - System diagrams
 - Procedures for operation, test and maintenance, emergency procedures, etc.
- E. Risk Assessment References (NRC/Sandia)
 - IREP Procedure and Schedule Guide
 - WASH-1400

- IREP Fault Tree Guide
- Fault Tree Handbook
- Human Factors Handbook
- Release Category Identification Guide

F. List of LERs Screened for Relevance as Potential Accident Precursors (NRC)

G. Component and Human Failure Rate Data Base and Quantification Guide (NRC/Sandia)

2.2 IREP Task Elements, Inputs, and Outputs

Note that the following task list gives a misleading impression that the tasks are sequential. In practice, it is expected that many tasks will be performed concurrently. Many tasks will also require several iterations; that is, a first approximation to the task will be prepared to enable the work to progress. Then, as more understanding of the accident susceptibility of the plant is developed, it will commonly be necessary to revise earlier task products.

IREP 6-Plant Study Task List

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
1	Prepare a table showing the names of systems installed in the plant corresponding to the functions in the generic event trees. List these systems. Product: 1a) function/system index; 1b) Front Line Systems List (FLSL).	A. Generic event trees B. FSAR
2	Assess generic list of transient initiators for applicability to the plant; draft provisional list of transient or active failure initiators. Product: 2) Initiator List.	B. FSAR C. Generic Initiator List (e.g., EPRI NP-801) F. Precursor LERs
3	Prepare System Description Note Books (SDNB) for each system in FLSL. Product: SDNB-FLSs.	1b. FLSL B. FSAR
4	Prepare a table listing each support system upon which the front line systems (FLS List) depend. Product: 4a) Table of FLS vs. Support Systems; 4b) Support system list (SSL).	3. SDNB B. FSAR, D.

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
5	Prepare System Description Note Books for each system on the Support System List. Product: SDNB-SSs.	3. SDNB-FLS 4., B, D
6	Group transient initiators having common mitigation requirements in order to avoid core melt. Total the expected frequency for each group. Product: Table of grouped transient initiators with estimated frequency of occurrence.	A, B, E, F 1., 2., 3.
7	Identify sites on the reactor coolant pressure boundary where active failures, command faults, support system faults, human error or transients could induce a LOCA. Classify non-passive LOCA possibilities by causal mechanisms, location, effective break size, symptoms, and common-cause failure potential. Product: 7a) Draft table of hypothetical non-passive LOCAs, 7b) List of questions for further research to finalize 7a list.	B, D, E

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
8	<p>Classify all hypothetical LOCAs (passive and non-passive) according to the number and kind of ECCS trains necessary to avoid core melt. Note special cases of passive LOCAs having peculiar symptoms or which have common cause fault effects, e.g., those which bypass containment. Group into classes those LOCAs having common mitigation requirements. Product: 8a) Draft classification of LOCA initiators by mitigation requirements, 8b) List of questions for further research to finalize 8a list.</p>	B, D, E, 7.
9	<p>Prepare an abbreviated fault tree analysis of transient initiators and active-failure LOCAs to identify which--if any--faults in the support systems in the Support Systems List can cause or increase the likelihood of initiating events. Product: 9a) Initiator FTs; 9b) Table of Support system incident initiators.</p>	B, D 4., 6., 9.

<u>Task #</u>	<u>Task Element</u>	<u>Required Inputs</u>
10	<p>Tabulate success criteria for front line systems listed in Task 1 for the several relevant initiating events. Also note where these criteria are suspected of being unnecessarily conservative.</p> <p>Identify questions for further research to finalize the system success criteria.</p> <p>Product: Table of FL System Success Criteria.</p>	<p>1., 2., 3.</p> <p>A, B</p>
11	<p>Commence collecting questions and additional plant data requirements to be requested of licensee. Product: 11a) Letters to plant owner; 11b) Initiate communications file and log book on communications with owner.</p>	<p>Prior tasks</p> <p>1 through 10</p>
12	<p>Transmit products of Tasks 1 through 11 to (1) NRC IREP project management, (2) Sandia IREP project management, and (3) the plant owner for review and comment. Include a brief analysis of manhours spent on each task and problems encountered.</p>	<p>Prior tasks</p> <p>1 through 11</p>

<u>Task #</u>	<u>Task Element</u>	<u>Required Inputs</u>
13	Adapt generic functional event trees into plant specific systemic event trees for each group of initiating events. Product: Systemic Event Trees including explanatory text.	2. 10., A
14	Develop statements of front line system failure criteria and depict as fault tree top logic for each FLS. Product: FT tops with explanatory text for each FLS.	10., 13.
15	Prepare a tabular Failure Mode Effects Analysis for the points of interaction between support systems and the front systems of Task 4. Product: FMEA.	3. SDNB-FLS 4. Dependency Table 5. SDNB-SS
16	Continue the development of the dependency table and the interaction FMEA to include interactions among support systems, e.g., service water depends upon AC power and both may require DC control power. Products: 16a) Table of support system interdependencies; 16b) Additions, if any, to support system list; 16c) FMEA for interactions among support systems.	5. SDNB-SS D. Plant documentation

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
17	Transmit products of Tasks 12 through 15 and any revisions of Task 1 through 11 products to (1) NRC IREP project management, (2) Sandia IREP project management, and (3) the plant owner for review and comment.	Prior tasks 1 through 16
18	Develop the fault trees for the front line systems into parent trees; i.e., extend the failure logic developed in Task 14 to individual trains or branches of the system. Develop train failure to distinguish faults in support systems (according to the FMEA of Task 15) from local faults of the system, but <u>do not</u> resolve local faults in these fault trees or pursue the development of support system faults at this time. Product: Parent Fault Trees for each system in FLSL.	3. SDNB-FLS 14. FT Tops 15. FMEA
19	Tabulate the local faults in the front line system fault trees which contribute to each composite local fault event in the parent trees developed above. Provide a preliminary quantification to	3. SDNB-FLS 18. PFT

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
	limit the development to potentially significant events only. Product: Tabulated daughter trees.	
20	For each support system, collect a list of fault events appearing in the parent trees of the front line systems originating in faults of the support system. Add to the list the support system faults that are (or contribute to) initiating events. Develop fault tree top-logic (failure definition) for the support systems and tree segments to cover faults in support system branches. Products: 20a) Table of support system fault citations in the initiator and front line system fault trees; 20b) Additions to FLS daughter tree tables; 20c) Connector tree segments for support systems fault trees; 20d) Table of failure definitions for support systems; 20e) Top logic fault trees for support systems.	15. FMEA 18. FTs

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
21	If there were new additions to the support system list in 20b, repeat those steps that develop this information, i.e., Tasks 5, 6, 9, 13, 14, ..., and 20c.	20b
22	Report results of Tasks 18 through 21 and revisions of Tasks 1 through 16. Revisions of Tasks 1 through 11 should reflect comments received.	1 through 21
23	Develop parent trees for support systems Product: Support system fault trees.	16. 20. 21.
24	Tabulate the local faults in the composite events of the support system fault trees (23) and provide a preliminary quantification to limit the development to potentially significant events. Product: Daughter tree tables.	23. SS FTs D. Plant documentation G. Data
25	Develop dependency diagrams, one for each support system, each showing all the front line systems, portraying the kinds of fault propagation into the front line systems from support systems using fault tree notation. Product: System failure dependency tables.	15., D 16. 18. 23.

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
26	Develop dependency diagrams for the initiating events showing transient and non-passive LOCA initiator groups and displaying a fault tree logic model of how support system faults may cause or contribute to the occurrence of the initiating events. Product: Initiating event dependency diagrams.	6., 9.
27	Employ the dependency diagrams and event trees to prepare a table of accident sequences caused by support system faults. Product: Table of support system accident scenarios.	25., 26., 13.
28	Re-examine system fault definitions and assumptions employed in the initial quantification of system and initiator fault trees for consistency. Revise as necessary. Product: Statement of consistency of initial quantification with sequences. Revisions, where necessary, to products of tasks 13., 14., 18., 19., 20., 23., 24., 27., etc.	18., 14., 13. 19. 20. 23. 24. 27.

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
29	<p>Formulate parent fault trees for each core melt accident sequence in the systemic event trees by combining under an AND gate the initiating event and the several fault trees for the postulated system failures in the sequence. Obtain minimal cut sets and rank according to provisional quantification of initiating and local events. Truncate at 10^{-10}/yr.</p> <p>Further reduce the list of sequence minimal cut sets by eliminating those cut sets which are sufficient to cause more severe sequences. Each cut set should be attributed to only one sequence. Note cases in which the most severe sequence is ambiguous. Product: Ranked list of minimal cut sets for event sequences.</p>	13., 18., 19., 20., 23., 24.
30-33	<p>Examine and refine the sequence cut set lists and their quantification as follows:</p> <p>30 - Verify the sequence cut sets entailing support system faults by comparison with the dependency diagrams. Correct the dependency diagrams, fault, or event trees as appropriate.</p>	25., 26., 27., 29.

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
	<p>31 - Search for potential common-cause failures, particularly those due to human (maintenance or operator) error. Revise assessed cut set frequency as appropriate. Product: Revisions of prior products or annotations on the event sequence cut set list identifying bases for altered frequency estimates, as appropriate.</p> <p>32 - Re-rank cut set lists for each event sequence by expected frequency of occurrence. Truncate at 10^{-8}/yr.</p>	<p>3., 5., D., 19., 24., 29.</p>
	<p>33 - Think through the chronology, causality and accident processes implied by each sequence cut set in the truncated list to verify that the assumptions underlying the event trees, fault trees and probabilistic quantification are consistent. Look for common cause failure mechanisms that may have been missed previously. Revise prior work as appropriate.</p>	<p>32</p>

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
34	Prepare logic diagrams of fault causation and descriptions of the sequence of events, symptoms, and expected outcome of the dominant accident sequences.	33., 32.
35	Transmit for review and comment the results of Tasks 1 through 34, highlighting revisions of tasks reported earlier.	1 through 34
36	Develop a qualitative list of singular initiating events with the potential to cause core melt without additional passive or random active failures. Insofar as practical with the information at hand, include in-plant fires or floods. The effort should be scoped to include accident susceptibility of the kind revealed by the Browns Ferry fire, the NNI-Y bus fault at Rancho Seco, and the accident at TMI.	7., 9., 13., 25., 26. 33., 34.
37	Re-examine the quantification and assumptions underlying the identification of the dominant sequences identified in	32., 33., 34., etc.

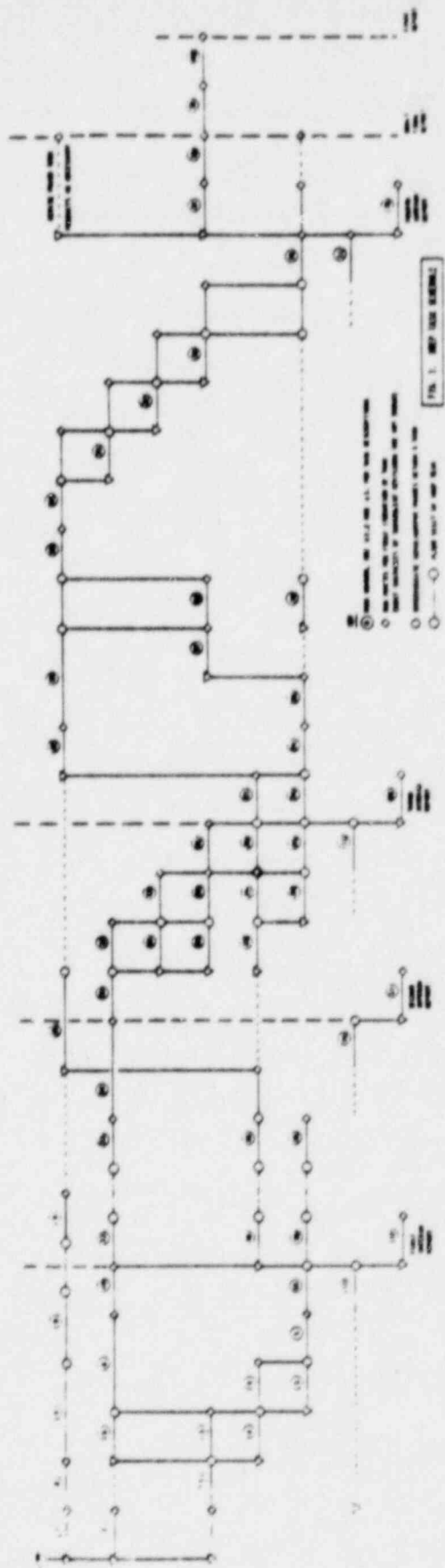
<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
	<p>Task 34. Discuss with plant operations personnel. Employ plant-specific failure rate data, where available, to refine the frequency estimate and discuss the sensitivity of the quantification to the phenomenological assumptions and failure probabilities. Describe the symptoms available to the operator and the opportunities for corrective action during the course of the accident. Note the range of warning times between the diagnosis of the accident and the release from containment.</p>	
38	<p>Prepare a draft of the final IREP study report and submit for review and comment.</p>	
39	<p>Participate in a Research Review Group to assemble critical comments on the draft report. Assist the plant owner in reviewing the draft report.</p>	
40	<p>Prepare and publish as a NUREG report the final edition of the plant-specific IREP study report, incorporating as</p>	

<u>Task #</u>	<u>Task Elements</u>	<u>Required Inputs</u>
	appropriate the feedback from the Research Review Group, NRC and Sandia project management, and the plant owner's comments.	

2.3 Schedule

Each IREP Phase II study is anticipated to take nine months to produce a final report.

One of several ways to schedule the tasks to be performed is suggested in Figure 1. An alternative might entail the concurrent development of the FMEA Tasks 15 and 16 with the fault tree Tasks 18 through 24.



3. IREP TASK DESCRIPTIONS

3.1 Function/System Index and Front Line System List

The effort to develop a simple, complete catalogue of accidents involving a reactor core is facilitated by distinguishing between front line systems and support systems. The front line systems list is a minimal list of systems whose operability completely defines the course of accidents with respect to the timing and magnitude of the release--if any--of radioactivity. Support systems important to safety are those which affect the course of accidents only by way of their effect on the operation of front line systems. Examples of front line systems include main and emergency feedwater systems, emergency core cooling systems, containment sprays and fan coolers, and valves regulating flow across the reactor coolant pressure boundary or the containment boundary. Examples of support systems include auxiliary AC and DC power systems, component cooling water systems, HVAC and instrument air systems. Some ambiguous cases are systems with both front line and support functions (e.g., an essential service water system which is part of the decay heat removal system--i.e., front line--as well as a heat sink for front line systems. Another ambiguous case is an actuation system whose classification as part of a front line system or as an independent support system is a largely semantic distinction.

To keep the number of front line and support systems to a minimum it is commonly helpful to class actuation and control systems as part of the front line system rather than as a separate support system provided that the actuation and control system serves only one front line system. On the other hand, if the actuation system initiates more than one front line system, e.g., the Safety Features Actuation System, it is more convenient to treat it as a support system. By so doing, the potential for multiple faults among the front line systems originating in a single failure of the actuation system can be treated explicitly in the dependency diagrams and the fault trees for the support systems.

Flag those front line systems that normally participate actively in normal power generation, e.g., the main feedwater system, from those which are normally dormant, e.g., the ECCS or auxiliary feedwater system. In most cases it will prove more convenient to treat the normally operating systems in the fault trees for the initiating events rather than in the fault trees for the mitigating systems. However, do not forget to consider the possible restoration of these systems as a potential recovery mode in the later analyses of accident sequences.

3.2 Initiator List

EPRI has classified and estimated generic occurrence rates for transient event initiators at nuclear power plants in EPRI NP-801. This work serves as a satisfactory starting point from

which to estimate the types and frequencies of transients to be expected in the subject plant. Tabulate which of the transients in the EPRI list are applicable to the plant, and indicate their generic occurrence frequency. Keep in mind that the plant in question may be susceptible to different kinds or frequencies of transients than the report suggests. Consider the list of potential precursor LERs in this task. In this and subsequent tasks, look for clues to modifications that may be needed to the transient initiator list and the assessed frequency of occurrence.

3.3 System Description Note Books--Front Line Systems

The System Description Note Books--one for each of the front line systems--are intended to contain (1) a copy of a description of the system (perhaps a photocopy of the system description in the FSAR or from the operator training manual); (2) the principal diagrammatic documentation of the system, e.g., P&ID for mechanical systems; (3) an annotated index of relevant information in the supplied plant documentation, i.e., cross references to elementary diagrams relevant to the system, to operating, maintenance and emergency procedures, etc.; and (4) Copies of letters, telecon memoranda, and interview notes in which the IREP team questions the operators, designers or builders about the details of the system design or operation.

The SDNBs will continue to grow throughout the IREP study. Every piece of information actually employed in the IREP study

results about the plant design or operations should either appear in the appropriate SDNB or should be traceable via the SDNB and retrievable from the central IREP team file.

Four copies of the plant documentation and of the SDNBs are to be maintained throughout the study. They are to be located as follows:

1. Study team
2. NRC IREP project management
3. Sandia IREP project management
4. Utility (plant owner) office designated to track the IREP study.

Document control procedures are to be implemented to assure that all four copies are updated and complete. Each addition or correction to the plant documentation or to an SDNB should be funneled through the IREP team Document Control Engineer (a designated member of the IREP team). The Document Control Engineer should issue revision pages as necessary to update the four copies and a new cover sheet which indicates the latest revision of each page.

The initial preparation of the SDNB described in Task 3 entails the collection of the system description, the principal diagrams, the first edition of the cross index to procedures and the current diagram file, the dissemination of the first set of

four copies, and the initiation of the document control system. It is expected that the entire IREP team participate in the development of the SDNBs. In fact, the initial perusal by the team members of the FSAR and the plant documentation to familiarize themselves with the plant should be combined with the exercise of initiating the SDNBs as well as Tasks 1 and 2.

3.4 Support Systems List, Table of Front Line Systems vs. Support Systems

In the course of reviewing the design and operation of the front line systems, note each active support system, such as auxiliary essential AC power, non-essential AC power, DC power, control and actuation systems, HVAC systems, auxiliary cooling water systems, instrument air, etc., upon which the front line systems depend. Document the survey of support systems in the form of 4a) a master list of all the support systems upon which the front line systems depend, and 4b) a table or matrix with the names of the front line systems in the left hand column and the names of the support systems across the top. Enter check marks to note the dependencies identified.

Conventions involving the definition of system boundaries employed in the analysis should be recorded in the System Description Note Books for future reference. It will suffice to follow FSAR or other plant documentation conventions for the definition of systems.

It is not necessary to distinguish between system trains or divisions nor to distinguish between types of dependencies for the purpose of this expeditious task. However, this information will be needed in the Failure Mode Effects Analysis Task, Task 15, and subsequent tasks. Therefore, clearly note in the System Description Note Books where this information can be retrieved when it is needed.

Treat the main feedwater system as a front-line system in this exercise to support subsequent tasks entailing the analysis of transients and non-passive failure LOCAs.

Where system operation requires operator control, treat the operators as a "support system." In ambiguous cases where the functional dependency is in doubt--e.g., a front line system may or may not require operability of the compartment HVAC--assume the dependency is present and record the system in the list and table with a question mark to note the ambiguity.

3.5 System Description Note Books - Support Systems

Follow the guidelines for Task 3. For operators treated as a "support system," record the references to the procedures or system descriptions describing the operator's role and responsibilities.

3.6 Group Transient Initiators Having Common Mitigation Requirements

Some transients can be ridden through without a requirement for scram or for the initiation of standby cooling systems. These are of no interest unless they deteriorate into scenarios

in which the scram and/or the startup of backup cooling systems are necessary. Therefore, it generally suffices to limit the grouping to two classes: those in which the expeditious termination of criticality is required and/or those in which the delivery of main feedwater is interrupted for long enough to require the initiation of a backup cooling system to dissipate decay heat. A useful convention employed in the RSS is to distinguish transients in which the power conversion system (main steam, condenser, main feedwater, the turbine or the turbine bypass system, and the circulating water system) continues to operate or trips off. That is, the power conversion system is said to be operable if the normal reactor heat dissipation path via the circulating water system remains operable.

Since the focus of the analysis is to give an initially broad catalogue of accident sequences leading to core melt, it is useful to employ a gross classification of transients. When in doubt, employ subgroups of transients within the coarser, broader classifications to denote collections of transients which are similar with respect to the demand for changes of state among the front line systems, but which differ in the timing of the demand, the options for recovery, or the severity of the effects of failures. It is not, however, necessary to develop this fine-structure of the transient initiator classification

at this time. The fine-structure of the classification should be developed in an iterative fashion during the fault tree analysis of initiators.

Total the estimated frequency of occurrence for each transient group by adding the estimated frequencies of the constituent transient types from EPRI NP-801 and Task 2. Update the Task 2 Initiator List if new insights developed in Task 6 suggest alterations.

3.7 Table of Non-Passive LOCA Initiators

Survey the entire surface of the reactor coolant pressure boundary, as documented in P&IDs and other plant documentation, in support of Tasks 7 and 8.

Task 7 is devoted to the identification of hypothetical non-passive-failure LOCAs. Catalogue sites on the reactor coolant pressure boundary at which non-passive LOCAs are possible. Examples of non-passive failures are externally operable valves where active failures, human error, command faults, etc. might result in breaches of the pressure boundary. Note in particular those sites at which transient-induced non-passive failure LOCA might take place, e.g., safety/relief valves, letdown lines, etc. Classify the hypothetical non-passive failure LOCAs in tabular form distinguishing the immediate causal mechanisms, the break location, the range of possible effective break areas, the symptoms discernable by

the operators, and the common-cause failure possibilities. Only the immediate or proximate cause need be identified in this task; subsequent tasks develop--in fault tree form--the root causes of these LOCAs. Symptom identification can be qualitative, it is not expected that reactor coolant or containment atmosphere pressure temperature analyses be performed. Highlight any clues available to the operators of the location or cause of the break. Note if the breach is potentially isolatable. Among the common-cause failure features to be considered are LOCAs that may affect the operability of one or more trains of ECCS, which may breach the containment pressure boundary, or which have unusual symptoms (such as high pressurizer level) that might confuse operators or affect the signature which actuates the engineered safety features actuation system.

It is expected that the available plant documentation may prove insufficient to complete this task. If this is the case, collect a list of questions for the plant owner and/or for the IREP research program management to resolve ambiguities. However, proceed as far as possible with the task at this time, using judgment as necessary to complete the catalogue in order to support successive tasks. Flag judgment calls for future verification or for use in documenting assumptions.

- 3.8 Classify all Hypothetical LOCAs by Mitigation Requirements
Group all hypothetical LOCAs (passive as well as non-passive) into classes sharing common mitigation requirements, i.e.,

whether or not reactor scram is required, whether or not feedwater (normal or emergency) is required, and the kind and number of trains of Emergency Core Cooling Systems required. It is expected that most active and passive LOCAs can be grouped by effective break size. A few hypothetical LOCAs may also depend upon break location or upon common-cause failure potential. Identify any groups or subgroups of LOCAs with particular mitigation problems such as:

- a. LOCAs for which recirculation may be compromised (blowdown outside of containment, blowdown may accumulate in a cavity that does not communicate directly with the emergency sump, etc.).
- b. LOCAs which intrinsically defeat one or more ECCS train.
- c. LOCAs which may intrinsically breach the containment barrier.
- d. LOCAs outside of the ECCS design envelope, e.g., gross reactor vessel rupture.
- e. LOCAs whose symptoms do not trigger the Safety Features
Mitigation System.

For each group or subgroup of passive failure LOCAs develop an estimate of expected frequency of occurrence following RSS practice. See also the quantification guide. Note if there is a subgroup of piping within each group which depends upon

the operability of snubbers or sliding equipment mounts to accommodate thermal expansion and contraction. Collect a list of questions to resolve ambiguities in this task, as outlined under Task 7.

The objective of the IREP study is to use realistic analyses of equipment phenomenology. Thus it is unnecessary to employ licensing conservatism in the classification of LOCAs by mitigation requirements. However, realistic analyses of ECCS requirements may not be available. Generally it is more efficient, in this case, to proceed with the analysis employing the conservative licensing criteria to define ECCS requirements, but to note instances of suspected conservatisms. As the analysis of accident likelihood and causation takes shape, it is then possible to estimate whether a less conservative definition of ECCS requirements would make a significant difference in the assessed risk. In most cases, it will not make much difference in the estimated frequency of core melt accidents whether realistic or conservative ECCS sufficiency assessments are employed. Thus, it may never be necessary to perform the realistic LOCA analyses. In the unlikely case that the conservatisms are predicted to influence the risk significantly, the refinement of the ECCS success/failure criteria can be earmarked for follow-up work.

Note that the lower bound on the break area for the class of smallest LOCAs may be significant. Small leaks and very small

line breaks are rather common in reactor coolant systems. Thus, the assessed frequency of occurrence of the smallest LOCA class is likely to be a sensitive function of the minimum break area. This may prove to be important to the risk. Thus, some care should be taken in identifying the smallest LOCA sizes which would lead (realistically) to core melt if ECCS fails.

Document the results of Task 8 in a table listing LOCA groups classed according to mitigation requirements. It should display the estimated frequency of occurrence for passive-failure LOCAs and carry annotations for special cases. Also document assumptions and collect the questions for further research to resolve ambiguities in the table.

3.9 Fault Tree Analysis of Transient and Non-Passive LOCA

Initiators

The objective of this task is to identify faults in the support systems which can cause or contribute to initiating events as well as degrade the reliability of systems called upon to respond to the initiating event.

Frequency estimates for transients without this common cause aspect will be obtained from actuarial data rather than synthesized with the fault trees from component failure rate data. Therefore, there is no need to detail faults in these trees which do not also appear in support systems for the standby front line

systems. The use of the fault tree approach is merely intended to provide a coherent, disciplined approach to the search for common elements contributing to both the initiator and the mitigation failure.

The key to the efficient performance of this task is to trace fault propagation (in the reverse-causal direction) from the event initiators--transients or non-passive failure LOCA--to support systems belonging in the Support Systems List.

3.10 Success Criteria for Front Line Systems

Tabulate the success criteria for the front line systems in terms of the number of trains of each system operable and the allowable delay in starting these trains for each distinct class of initiating events. Distinguish success criteria for the injection or early accident phase from the recirculation or later phase if different.

Follow the policy suggested under Task 8 with respect to conservatism, i.e., realistic criteria are desirable, but use conservative criteria in cases in which the realistic success criteria are not readily obtainable. Where unquantified conservatism is suspected, note it for future reference.

The allowable start delays may be a sensitive function of the details of the accident sequence, and accurate realistic predictions of the point of no return are rarely available. It is not necessary to pin down these characteristic times

with much accuracy. These times will be employed to assess the window for operator corrective action to restore or initiate the function of those front line systems that do not start automatically or promptly. Since it is beyond the state-of-the-art to predict the probability of such operator success/failure within an order of magnitude, an uncertainty range on the allowable delay as large as a (multiplicative) factor of 3 (or 1/3) will not significantly affect the accuracy of the overall assessment. Therefore, an estimate of the allowable start delay that is no better than a ballpark estimate will generally suffice.

It is worth noting cases in which a delayed start of a standby front line system can potentially change the course of an accident sequence even though the start is ultimately successful. For example, a delayed start of emergency feedwater following a loss of main feedwater in a PWR may be successful with respect to sustaining an adequate heat sink for decay heat dissipation but it may open up the possibility of a transient-induced LOCA in the lifting of a pressurizer relief/safety valve. For this example of a PWR Emergency Feedwater System (EFS) there may even be three (or more) critical time windows:

t_1 - delay time after which EFS start will not preclude opening a pressurizer relief/safety valve

t_2 - delay time after which EFS start--by itself--cannot preclude core melt

t_3 - delay time after which EFS start and HPI start cannot preclude core melt.

It is not intended that the IREP team analyses embrace original analyses of core damage phenomenology or resolve differences between a damaged core and a complete meltdown. Past risk assessments have clearly shown that the offsite risk is dominated by full meltdown accompanied by gross containment failure. Therefore, IREP is to focus on this severe end of the accident spectrum. In any case, our limited ability to predict human reliability or repair/restoration probabilities would generally mask any "fine tuning" of the success vs. failure criteria for delayed starts that distinguished between core damage and full meltdown. The few exceptions to this generality are unlikely to be significant to the public health and safety risk, although they might be significant to the economic risk borne by the plant owner associated with TMI-like outcomes.

Include success criteria for front line containment systems such as sprays, fan coolers, and the isolation system in the table of success criteria. Comments, footnotes or annotations should clearly spell out the assumptions. In addition, prepare a list of open questions necessary to resolve ambiguities in the success criteria. These will be reviewed as part of the review of the first interim report (see Task 12). IREP project management at the NRC, Sandia, and the plant owner's review group will arrive at a consensus on the disposition of these

questions. Some may be answerable directly by one of these groups, others may be left as open issues to be explored by a sensitivity study on the IREP results. Still other questions that are likely to be important may be earmarked for concurrent research by the NRC Office of Nuclear Regulatory Research or by the plant owner. For example, in the Crystal River IREP study Florida Power Corporation requested of B&W some analyses of allowable start delays for the Emergency Feedwater System.

3.11 Plant Data Requirements and Questions

From time to time the IREP teams will identify a need for additional information on the design, function, operation, surveillance or maintenance of systems. Where practical, the utility representative(s) on the IREP team should help to obtain this information directly to avoid unnecessary delays. The plant owner may choose to funnel such questions through one or a few identified points of contact. We anticipate that such data-gathering may be the critical path item in some parts of the IREP schedule. Nevertheless, the team leader should screen and coordinate these requests to assure that no unnecessary burden is placed upon the owner. In addition, the requests for information as well as the supplied information should be logged and maintained under the document control system described in Task 3 to assure that proper records are kept. See also Task 10 description for issues relating to system success vs. failure.

3.12 First Interim Report

Transmit products of Tasks 1 through 11 to (1) NRC IREP project management, (2) Sandia IREP project management, and (3) the plant owner for review and comment. Include a brief analysis of manhours spent on each task and problems encountered.

3.13 Event Trees

Adapt generic functional event trees into plant specific systemic event trees for each group of initiating events. Product: Systemic Event Trees including explanatory text. See also the IREP Event Tree Guide.

The generic functional event trees supplied to the IREP study teams are intended to be a first cut at the functional event trees of the plant. Since the front line functions do not necessarily bear a one-to-one correspondence with the systems installed in the plant, a generic approach is generally feasible. The systemic event trees are intended to correspond with installed systems or groups of systems.

Neither the functional nor the systemic event trees describe accidents in a chronological or root-causal sequence. Rather, they catalogue accidents according to (1) the class of initiating event and (2) the operability or inoperability of systems or functions. They are intended to define an abstract classification of accidents with just enough detail to identify roughly the magnitude and expected timing or radiological releases to the atmosphere. The sequence of branch points in these trees may

conincidentally match the chronology of failure in some cases but the choice is principally governed by a desire to simplify the accident classification scheme as much as possible. This is done by selecting the sequence to take maximum advantage of the fact that for some accident scenarios the operability of many of the front line systems is moot.

The systemic event trees--whose branch points do correspond with distinct systems or groups of systems--serve as the jumping-off point for system reliability analysis. They serve to define the accident scenarios within which system reliability is of interest. They help specify the failure criterion for each of the systems in the context of a particular class of accidents, and they define the window for common cause failures that couple the initiating event with mitigating system failure or couple the failure of more than one mitigating system, including human error or support system faults.

To simplify the analysis, support system faults like loss of AC power are not to be shown on the functional or systemic event trees employed at this stage of the analysis. Only front line systems or functions are to be displayed. However, the systemic event trees may be redrawn at the conclusion of the analysis to display the support system faults so that the revised classification scheme for accident scenarios bears a simpler relationship with the risk-dominant sequences. Both styles of systemic accident classification are useful: those

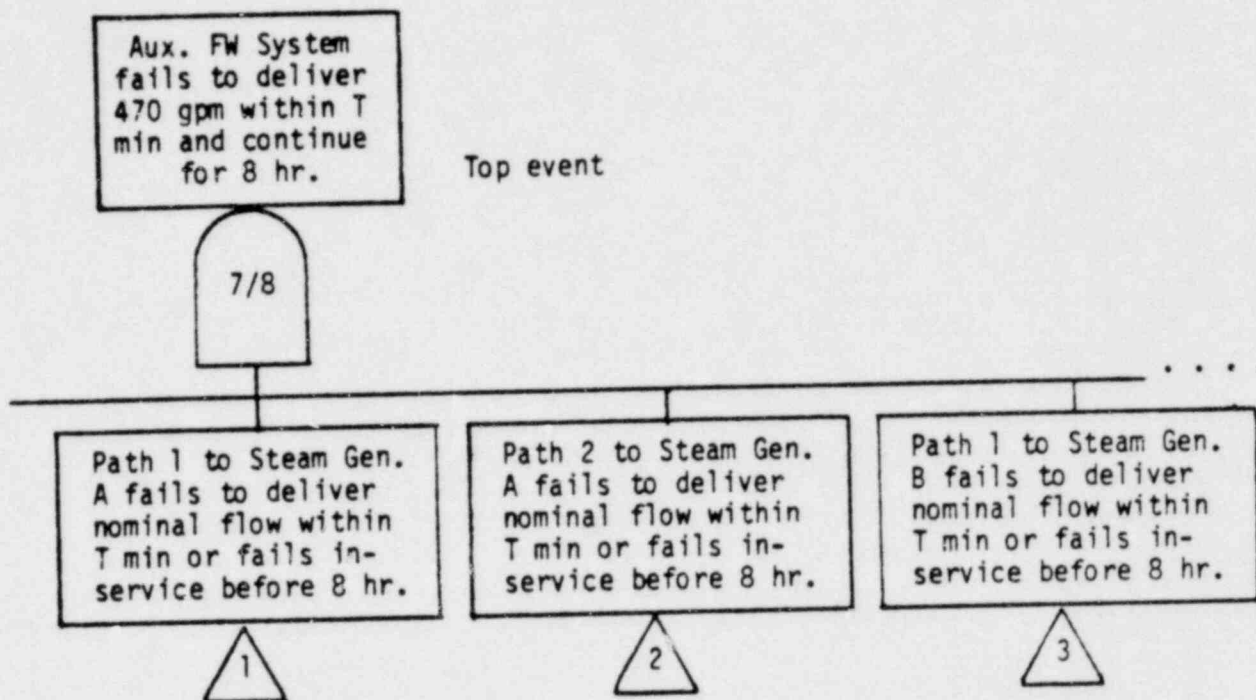
with only front line systems more clearly delineate the factors that directly influence the release of radiation; those with support systems shown more clearly delineate the causal grouping of accident scenarios.

3.14 Fault Tree Top Logic

Employ the system success criteria developed in Task 10 and the event trees developed in Task 13 to formulate system failure definitions for use in the fault tree analysis of the front line systems. Verify that the failure criterion is the same for every instance in which the system appears in the event trees or define different criteria as necessary so that each event tree application is covered. Develop the fault trees for each variant and for each front line system to the extent necessary to portray the number of trains or divisions whose failure is sufficient to fail the system.

An example appears below:

Auxiliary feedwater system for a Westinghouse 4-loop PWR. Success is 470 gpm delivered within T minutes (T depends upon the initiator) to any one or more steam generators. There are eight distinct flow paths (two to each steam generator) from three pumps. Each path normally can provide 250 gpm. Thus, any two of the eight paths, delivering normal flow constitute success. The event tree calls for a failure to start or to sustain auxiliary feedwater for 8 hours.



Note 1. Be prepared, if necessary, to quantify separately failure to start and failure to run for 8 hours or to edit the cutset list to avoid counting spurious combinations of late start on some paths and later failure to run on others that at no time fail the entire system.

Note 2. Critical start times are tabulated below:

Sequence	T	Comments
Feedwater transient without scram	1 to 2 min	PNR*
Feedwater transient with scram	2 to 8 min	time to lift PRZR valve
Feedwater transient with scram	15 to 20 min	PNR* for AFS restoration
Feedwater transient with scram	20 to 30 min	PNR* for AFS and HPI initiation

*PNR = estimated Point of No Return for the avoidance of core damage or melt.

This example is purely hypothetical; the numbers cited are made up for the example.

3.15 Interaction Failure Mode Effects Analysis

The Failure Mode Effects Analysis is a table with one entry row for each point of dependence of the front line systems on support systems, including humans. It is intended to summarize the assumptions or understanding to be used in the analysis of the fault propagation from the support system into the front line system. It is not intended to elaborate on fault propagation within the support systems "up stream" of the point of interaction, as that will be dealt with in the support system fault trees. However, it will be useful to trace faults beyond support system components that uniquely serve the particular front line system component, as their failure can be lumped with FL component failure. Column headings in the FMEA are:

1. Front line system component designation
2. Support system
3. Support system division or train
4. Proximate support system component designation
5. Failure mode
6. Fault effect on front line component function
7. Fault detection interval
8. Fault diagnostics (clues, symptoms, instrumentation, control room vs. local, etc.)
9. Comments

An example follows.

INTERACTION FMEA EXAMPLES

Front Line System			Support System			Failure Mode	Fault Effect	Detection	Diagnostics	Comments
System	Div.	Comp.	System	Div.	Comp.					
1.	AFWS	A	MDP-1A	AC pwr	A	breaker A1131	fail open fail open	at pump test	pump operability only	treat as part of local pump failure
			B	MDP-1B	AC pwr	B				
2.	AFWS	A	MDP-1A	AC pwr	A	bus E11	a) zero voltage b) low voltage	prompt prompt	CR monitor ESG E/F 11 voltage, alarmed	partial failure noted for future reference--not pursued in IREP
			B	MDP-1B	AC pwr	B				
3.	AFWS	A	MDP-1A	HVAC	A	Rm Cooler 3A	no heat removal no heat removal	shift walk around	no warning for local faults	AC and SWS support systems of HVAC monitored but not HX
			B	MDP-1B	HVAC	B				
4.	AFWS	A	MDP-1A	ESWS	A	Oil Cooler S31	loss of service water flow	at pump test	local lube oil temp gauge, none in CR	ESWS header and pumps monitored but not lube oil coolers. Local manual valve alignment checked in maintenance procedure xx but not in periodic walk-around
			B	MDP-1B	ESWS	B				
5.	AFWS	A	MDP-1A	DC pwr	A	bus A131	low or zero voltage low or zero voltage	prompt	CR monitor XXX DC bus voltage--many lamps out in CR	* Effect of DC loss on AC not evaluated here, local motor controller latches on, needs DC to trip or close.
			B	MDP-1B	DC pwr	B				

*CSH - continuous service hours
MDP - motor driven pump

INTERACTION FMEA EXAMPLES (CONT.)

Front Line System			Support System		Failure Mode	Fault Effect	Detection	Diagnostics	Comments
System	Div.	Comp.	System	Div. Comp.					
6.	AFWS	A	MDP-1A	a) remote operators or maintenance personnel	a) leave or switch pump controller to "local" at MCC cabinet in Aux. Bldg. b) override auto start in MCR	a) defeats auto and CR manual start b) turns off pump	shift change check list NA	status lamp XXX in CR flow gauge XXX dischg. pr. XXY status lamp XYY	
			MDP-1B	b) CR operators					
7.	AFWS	A	AF 32	operators and maintenance personnel operators and maintenance personnel	misalignment (closed)	blocked flow div A blocked flow div B	shift walk around	AF flow gauge XX in CR, valve alignment unmonitored	<ul style="list-style-type: none"> - No lock required - On valve alignment check list XX (once per shift) - Closed for pump maintenance
		B	AF 33						

3.16 Dependencies Among Support Systems

Continue the development of the dependency table and the interaction FMEA to include interactions among support systems, e.g., service water depends upon AC power and both may require DC control power. Products: 16a) table of support system interdependencies; 16b) additions, if any, to support system list; 16c) FMEA for interactions among support systems. See foregoing comparable tasks for guidelines of methods and scope.

3.17

3.18 Modular Fault Tree Development for Front Line Systems

Develop the fault trees for the front line systems into parent trees; i.e., extend the failure logic developed in Task 14 to individual trains or branches of the system. Develop train failure to distinguish faults in support systems (according to the FMEA of Task 15) from local faults of the system, but do not resolve local faults in these fault trees or pursue the development of support system faults at this time. Product: parent fault trees for each system in FLSL. See also IREP Fault Tree Guide.

3.19 Tabulation of Local Faults

The subtrees of the system fault trees which detail the fault events that can give rise to a common effect on the function of a division or subdivision (segment) of a system will be

portrayed in a tabular form rather than drawn as part of a detailed fault tree.

A tabular format produces a more compact representation than a drawn subtree and also enables the data normally displayed on a FMEA and a quantification table to be combined with the fault tree documentation.

The composite events that are the endpoint of local fault resolution in the parent fault trees of task 18 have names like, "local faults functionally equivalent to a plug in pipe segment "G" and correction factors for common-cause failures local to two more more branches upstream or downstream of segment "G" that are also functionally equivalent to a plug in "G." This example is shown in the subsequent figures.

In most cases, the components giving rise to these composite fault events are functionally in series. A fault tree developing such composite events would be composed entirely of "OR" gates. The probabilities of the component failures in such a subtree are additive. Thus, the sum of the probabilities of these contributing events gives the correct first order approximation to the probability of the composite event. This makes the tabular documentation of these subtrees particularly convenient. A rule of thumb to assure that there are no errors in the logic of the parent fault tree reads as follows:

6. Quantification columns. These should be adapted on a case-by-case basis to the one (or several) evaluations of the fault tree required in the screening of accident sequence likelihood.

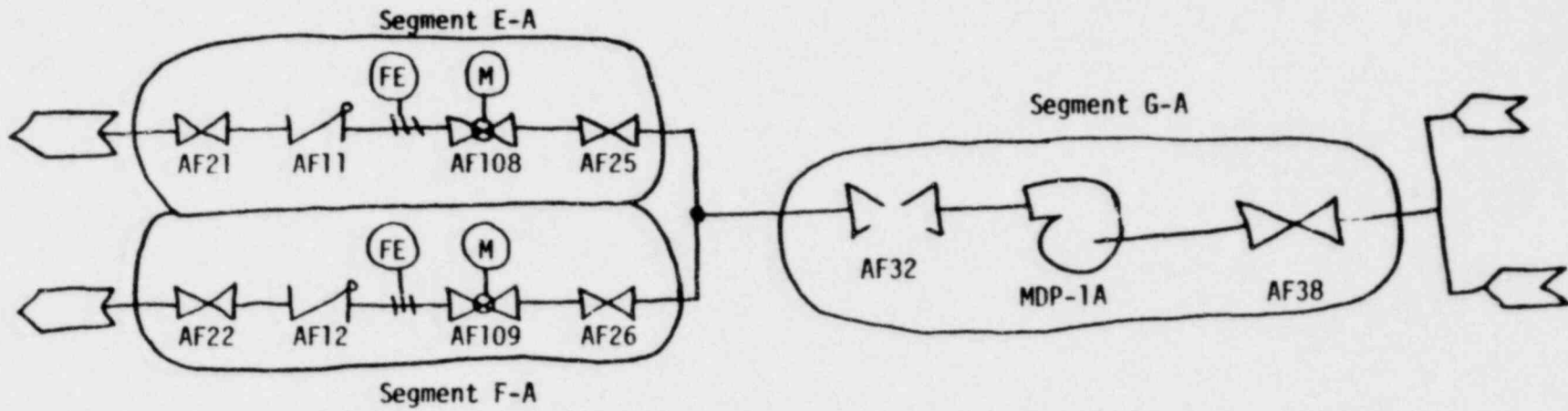
Also suggest in notes attached to the table the refinements of the probabilistic quantification that may be needed if the composite event proves to be important, or in subsequent searches for common cause failures. Where a similar analysis applies to two or more identical trains, show only one with the component designations for the other examples in parenthesis.

An example is shown on the following page.

3.20 System Failure Criteria and Modeling for Support Systems

For each support system, collect a list of fault event citations attributed to the particular support system appearing in the parent fault trees of all of the front line systems. Add to the list the fault event citations appearing in the fault trees of the initiating events. Check the list for completeness against the table of task 4a and the FMEA's of task 15. Fill in a table (one for each support system) listing the fault citations, the affected system, and the time-dependence of the faults, i.e., the critical outage times of interest, whether or not the fault produces a concurrent fault in the front line system, etc. Record all the information needed to select one or more failure criteria and probabilistic quantifications of the fault trees for the support systems.

Example of Table Documenting a Composite Fault Event



Contributors to the Composite Fault Event AF17-A(-B): "Faults Functionally Equivalent to a Plug in AFS Segment G-A (G-B)"

Quantification

Contributor	Type Code	Detection Interval	Diagnostics	Comments	Start Q/d	run λ /hr	Repair Probability			Failure to start within 1 min	Failure to start within 20 min & run for 12 hrs.	Failure to start within 30 min & run for 12 hrs.
							1 min	20 min	30 min			
<u>Singles in Seg G-A (G-B)</u>												
1. Pump Failure MDP-1A(-1B)	A	120 day test	Flow gauge XX in CR	Includes pump, motor, tube, & breaker faults	10^{-3+5}	10^{-4+1}	0	.2 ^a	.3 ^a	10^{-3+5}	$2 \times 10^{-3+1}$	$1.9 \times 10^{-3+1}$
2. Man. Valve AF 32 or 33 left closed	M	once per shift (check list 12)	Flow gauge XX in CR	Maintenance unavailability	10^{-3+5}	neg ^a	0	.1	.1	10^{-3+5}	$9 \times 10^{-4+1}$ ^a	$9 \times 10^{-4+1}$ ^a
<u>CCF in Segs E and F</u>												
Ops close AF108 and 109	O	Continuously displayed	Status lamps XXY, XYY	Closed for test and to throttle flow	10^{-4+1}	$10^{-3}/d$ ^b	.1	.8	.9	$9 \times 10^{-5+1}$	10^{-3+1} ^b	10^{-3+1} ^b
Man. Valve left closed in E & F	M	once per shift (check list 12)	Flow gauge XX in CR	Closed for control valve maintenance	$4 \times 10^{-5+1}$	neg ^a	0	.4	.6	$2.4 \times 10^{-5+1}$	$1.6 \times 10^{-5+1}$ ^a	$1.6 \times 10^{-5+1}$
Composite Event Totals -										2×10^{-3}	3.9×10^{-3}	3.8×10^{-3}

- Notes: ^a Misalignment of manual valves during the accident may not be negligible if repairs are attempted on this, similar, or adjacent equipment during the event.
^b Erroneous closure of control valves or shutdown of MDP of critical duration during the event estimated to have a discrete probability of 10^{-3} for screening purposes. If the event proves to be important, condition this operator error probability upon the level of confusion in the CR, operability of instruments, etc. Note also correlation with operator errors on other trains.

The support systems commonly supply numerous diverse loads. It is usually practical to draw a few subtrees for the branches of peripheral distribution systems that attribute support system failures either to the particular branch of the distribution system or to the core of the system. These "connector" tree segments should also be drawn in parent tree style. That is, use a single fault event for each group of component failures occurring in components effectively in series and which share a common effect on the function of that system segment.

In some cases, the subtree describing faults in a particular branch of a support system may appear in only one form in one front-line system fault tree. If so, it may be more convenient to treat this subtree as part of the fault tree for the front line system. That is, append the subtree to the fault tree of the front line system. In many cases this can be accomplished by adding on to one of the daughter tree tables for the front line system. Doing this is an optional matter of convenience. The advantage in so doing is that it shortens the fault trees and simplifies the analysis of system reliability and of sequence likelihood. The disadvantage in so doing is the loss of the one-to-one correspondence between fault trees and systems. This may prove awkward in post-IREP applications of the fault trees. An example might be the local failure of a motor control center bus that serves only motor-operated

valves in a single front line system. Another example is a branch of the service water system serving one or a few room coolers serving only one system of interest.

As part of this task, tentatively define the one or several support system failure criteria and translate these into a skeletal fault tree structure. Unfortunately, it is not so easy to separate the "top logic" of support systems from the basic tree development as it is with front line systems because of the diverse loads and interdependencies among these systems. However, a systematic development of fault trees that traces fault origins in the reverse-causal direction is almost always feasible.

Iterative analysis is particularly important with tasks 20, 21, 23, and 24. Only as the interdependence of support systems upon one another unfolds in the first pass through these tasks can one verify the completeness or adequacy of the fault trees for the support systems. These interdependencies can be anticipated with the aid of the FMEAs of task 16 for the first attempt, so that subsequent alterations can be minimized, but these tasks will require careful review after the first attempt is carried through.

- 3.21 The initial efforts at drawing fault trees may develop additional information on the interdependencies of support systems on one another. If there are new additions to the support systems list, extend the work of prior tasks to include these systems.

3.22 Reportage

3.23 Support System Parent Trees

Develop parent trees for the support systems in the style suggested under tasks 18 and 20.

Make liberal use of transfer symbols at intermediate points of the parent fault tree of the core of each support system to avoid unnecessary replication of subtrees for different applications. The parent fault tree style lends itself to the task of modeling support systems with many different loads. In most cases, the variety of conditionalities and critical failure criteria can be accommodated by altering only the quantification or the structure of the daughter trees delineating the composite local fault events.

3.24 Tabulate the local faults (daughter trees) in the parent trees of the support systems as described under Tasks 19 and 20.

Provide initial quantifications in the table for use in determining sufficient fault resolution in the trees and for use in the screening assessment of sequence likelihood.

Once the daughter tree tables are complete, reexamine the work of tasks 16, 20, 21, 23 and 24 for consistency. Revise as necessary.

3.25 Dependency Diagrams

Document the dependency of the front line systems on support systems in a simplified form using dependency diagrams similar

to the example shown below. Draw one diagram for each support system. Show all of the front line systems on each diagram. Fault tree or logic circuit notation is suggested for distinguishing the logical structure. Use a consistent notation convention throughout. Employ solid lines to trace concurrent faults (i.e., for cases in which an outage in the support system produces a concurrent outage in the front line system). Employ dotted lines to show conditional, delayed effect, or intermittent, non-concurrent dependencies. For example, if an auxiliary feedwater system depends upon service water as an alternate water supply if the condensate storage tank is depleted or depends upon room coolers for pump motor cooling only during longer-than-normal duty cycles, display the dependency with a dotted line. Employ a dot-dash notation for dependencies that are being eliminated through design changes not yet implemented. Use annotations to describe the circumstances in which the dotted line dependencies are realized. Use double lines to denote dependencies that can disable a train of a front line system even after the support system fault is repaired. For example, if an ECCS pump may seize if run without bearing lube oil cooling via the service water system, use a double dashed line to display this dependency on service water.



Resolve dependencies among the individual trains where feasible, but where cross ties make train identity ambiguous it is not

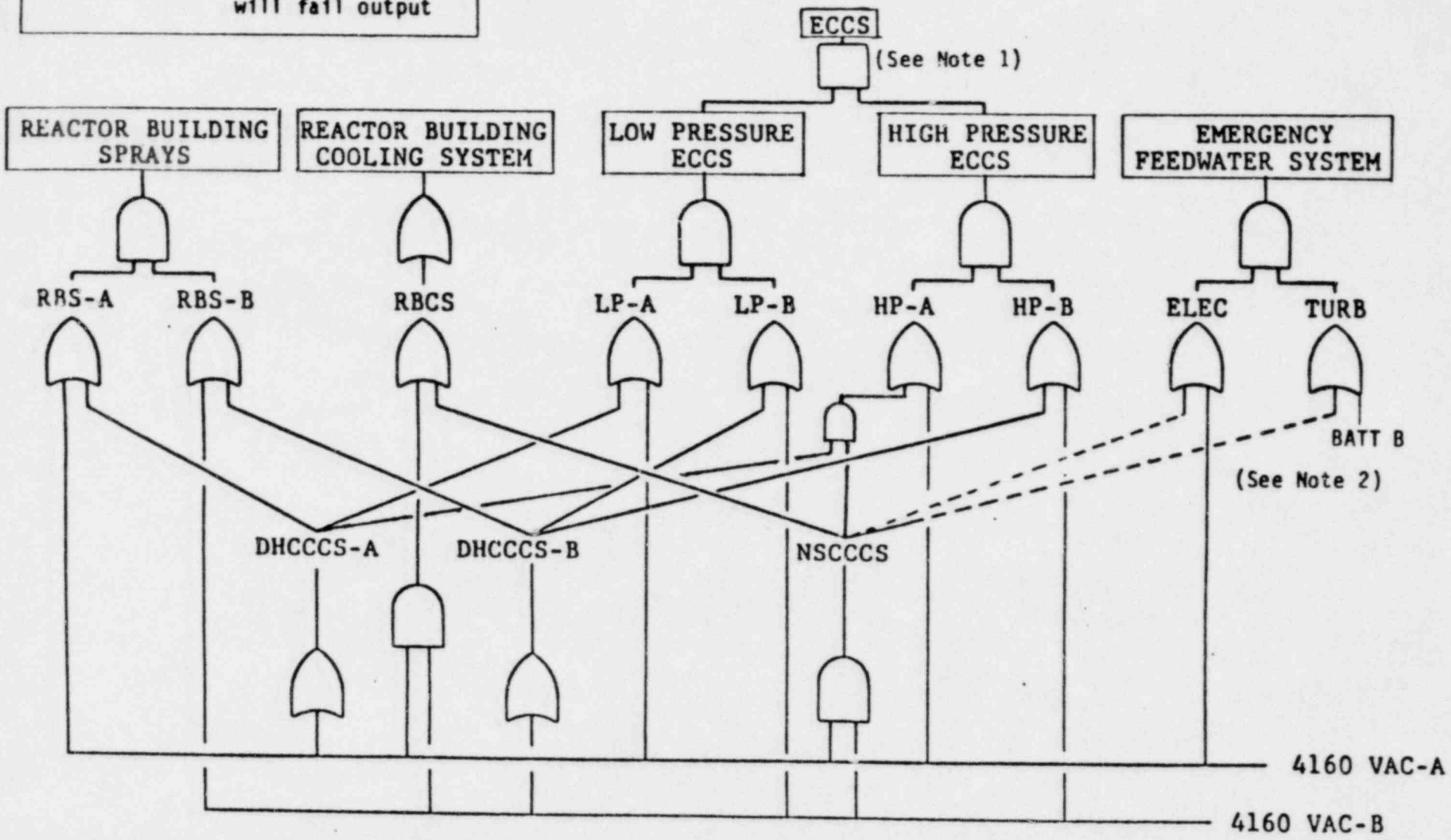
necessary to segregate the trains, see, e.g., the treatment of the Nuclear Service Closed Cycle Cooling System (NSCCCS) in the attached example.

The dependency diagrams are not intended to model the dependencies in the detail present in the event-tree/fault-tree work or in the interaction FMEAs. They are useful, however, to give a simplified picture of the system interdependencies that may become important contributors to accidents. They are an aid to the qualitative identification of important causal mechanisms for serious accidents. They are an excellent communication aid with which to describe methods and results. We expect that they will also prove to be useful in operator training and as an operator aid for rapid diagnosis of multiple faults.

Include in the dependency diagrams not only the direct dependence of front line systems upon support systems but also the implicit dependencies that act on front line systems by way of dependencies between the several support systems. For example, a particular train of a front line system may not directly require DC power to start or run but it may depend upon a support system that does require DC power.

It may not prove feasible to include operators among the support systems for the purposes of direct or implicit dependency diagram documentation. However, the attempt to do so will be a useful aid in organizing task 31.

 - AND Gate: All inputs must fail to fail output
 - OR Gate: Any input failing will fail output



NOTES
 1. Logic depends on LOCA size.
 2. The dashed lines indicate existing dependencies in Crystal River-3 which Florida Power Corporation has committed to remove.

5/5/80

Figure 2.3 Dependencies on Emergency Electric Power and

The first attempt at drawing dependency diagrams may be done before or after the FMEA and fault tree tasks. However, the dependency diagrams ought not to be trusted as a basis for the FMEA or fault trees because they do not fully portray the details of the dependencies, and the dependency diagrams need to be reviewed for completeness after the fault trees are prepared.

3.26 Dependency Diagrams for Initiating Events

Prepare dependency diagrams similar to those drawn in task 25 with initiating events in place of the front line systems. Indicate each class of transient or non-passive failure LOCA (grouped by distinct mitigation requirements).

3.27 Table of Accident Scenarios Based on Dependency Diagrams (27) and 3.28 and Reexamination of Fault Definitions and Assumptions (28)

It is useful to pull together the clues to some of the accident scenarios, based on the event trees and dependency diagrams, before a substantial investment in time is made in computer analysis of the event tree/fault tree models. Doing so helps to avoid the tendency to lose sight of the forest for the trees. One can employ these preliminary, qualitative results to search for phenomenological effects or common-cause failure mechanisms that may not be recorded in the fault trees or event trees, and whose discovery later in the analysis would require massive revisions of prior work.

Thinking through entire core melt accident scenarios can reveal problems that tend to be missed in classical ET/FT analysis. For example, late in the analysis of Surry for WASH-1400 it was discovered that blowdown from a small break LOCA in the reactor cavity might accumulate there for some time before water spilled over into the emergency sump. The Surry design entailed the autostart of the containment spray recirculation system--which in Surry is independent of the spray injection system--at a fixed time delay after a safety features actuation signal. Thus, the spray recirculation pumps might self-destruct by pumping on a dry sump for some small break LOCA scenarios. Another such problem is the effectiveness of containment atmosphere fan coolers after a molten core attacks the basemat. The rapid generation of inert particulates from the core-concrete action may plug filters and deposit an insulating blanket on heat transfer surfaces. Such effects should be considered during the event tree construction phase. However, the search for such problems can be better-focused after the fault trees and dependency diagrams have been constructed and some of the causal mechanisms for core melt accidents have been identified. Also, employ the preliminary list of support-system fault accident scenarios to search for instances in which operator or maintenance errors on different systems may be correlated or share a common cause.

Such searches for not-yet-modeled common cause failure mechanisms must be repeated after the screening analysis of the ET/FT models, but the earlier these effects are discovered the less re-work of prior tasks will be required.

The exercise of identifying core melt accident scenarios from dependency diagrams will also be useful in communicating the results to those unfamiliar with event tree/fault tree techniques.

The effort to tabulate accident scenarios from the event trees and dependency diagrams is intended as a working technique and not a finished product. Its scope need not be standardized. The IREP teams should follow their own judgment on when to do it and how to scope it. However, a suggested scope is to consider:

- a. Single failures in support systems,
- b. Total failure of each individual support system,
- c. Total failure of each individual support system plus a single failure elsewhere.

Employ the results to verify that the assumptions underlying the event trees, the fault tree logical structure and the quantification of the composite basic events (the daughter trees) is consistent with the emerging picture of important accident scenarios (Task 28). It is also very important to verify that a consistent fault event designation system be

used in all of the fault trees. One and the same failure appearing in two or more points in one or more fault trees must have an identical designation to assure that the cut set minimization process treats these as the same event.

3.29 Screening Evaluation of Accident Sequences

Construct fault trees for the core melt accident sequences identified in the event trees. This can be done by combining under an "AND" gate the initiating event (or its fault tree from task 9) together with the parent fault trees for the front line systems whose failure is postulated in the event sequence. The fault trees of the support systems must be added as necessary to complete the fault trees of the front line systems where these fault trees have transfer symbols for faults originating in support systems. There should be one sequence fault tree for each branch of each event tree resulting in core melt.

Obtain minimal cut set lists, cut set probabilities, and rank the cut set list in order of descending indicated probability.

The cut sets for each distinct accident sequence will not be mutually exclusive. There will be many instances in which a group of failures sufficient to cause a severe accident sequence will also be sufficient to cause less severe sequences, i.e., the same cut set may appear in more than one accident sequence. These cut sets should be attributed only to the most severe accident sequence.

There are two or more ways to weed out cut sets that are sufficient to cause more severe sequences. One is to incorporate "NOT" gates in the fault trees of the accident sequence to model explicitly the non-failure of systems that are defined as being operable in a particular sequence. Another way is to find the minimal cut sets (without "NOT-failed" system fault trees) for each sequence and delete cut sets for sequences which recur in cut set lists for more severe or more rapidly evolving accidents. This may be done with a list-matching routine on a computer. Use whichever method appears to be most convenient.

The value of parent fault trees will become apparent in this exercise. It should obviate the need to shorten system fault trees by the use of "reduced" trees. The parent trees should be compact enough to permit the entire parent trees to be employed without truncation. If the trees are too large to handle even in parent tree form, employ fault tree modularization techniques to replace the trees with more compact but formally equivalent, complete trees. This process replaces the composite events with even larger assemblages of events--treated as a unit--under rules that assure that no logical or probabilistic error is introduced by the coalescence of fault events. Computer codes are available to do this automatically, if necessary. A disadvantage in doing this if it is not necessary is that the composite fault events no longer bear a one-to-one

correspondence with failure modes of system segments. Thus, it is more difficult to bring engineering judgments to bear on the results; system insights are harder to come by if fault tree modularization is carried beyond the level suggested for parent fault trees.

Once the event sequence cut sets have been edited to remove failure modes sufficient to cause more severe accidents, have been quantified according to the screening event probability estimates, and ordered by this primitive likelihood assessment, it is important to make some consistency checks to verify the accuracy and completeness of the tables:

- a. Verify that all sequences identified in task 27 are present;
- b. Verify that the symmetry in the plant hardware and functions (e.g., pairs of identical trains) are matched by corresponding symmetry in the event cut sets;
- c. Re-check to verify that fault event designations are consistent throughout the event sequence cut sets, and
- d. Other verifications are suggested in tasks 30, 33, etc.

Criteria must be established to select which sequence cut sets are to be studied in detail in subsequent tasks. The criteria should reduce the number of cut sets to a manageable level for case-by-case examination. At the same time the criterion should be selected to make it very unlikely that an important accident scenario will be dismissed from further consideration. These are sequences that appear to be improbable in the screening assessment but contain not-yet-modeled common cause failure mechanisms that couple the occurrence of several failures, thus making them substantially more likely than the screening assessment suggests. In any case, the full cut set lists should be retrievable for future reference.

The simplest and most primitive criterion is one based upon the frequency for the sequence obtained in the screening quantification. Such a simplistic criterion ought not to be set above 10^{-10} /yr because for higher cutoff frequencies the likelihood of serious omissions becomes significant. We believe that the most serious non-conservative misrepresentations of sequence likelihood in the screening analysis originate in coupled operator errors during the accident. For example, an accident sequence in a PWR might entail a feedwater trip followed by a failure of auxiliary feedwater, high pressure safety injection, containment sprays and containment fan coolers. A contributor to this event is operators erroneously shutting off all four safety systems. The screening analysis will treat this as four

independent, individually unlikely operator errors. In fact, it may be a single operator error. Thus, the screening analysis may throw out this potentially important failure mode. Note that the coupling of operator errors in erroneously shutting down all trains of one safety system should already have been modeled in the system fault trees. However, the initial quantification of the composite basic events cannot be expected to model coupling of failures in different front line systems that does not originate in a common support system failure.

An improvement over the primitive screening criterion, and one that permits the number of sequence cut sets to be further reduced could be based on a screening with all operator errors during the accident artificially set at a probability of one and a screening threshold of 10^{-9} /yr.

If still further truncation is needed to reduce the number of sequence cut sets for case-by-case examination, employ a less stringent cutoff frequency for those accident sequences expected to produce mild outcomes. For example, one might use a screening with operator errors assigned a probability of one and the following table of screening thresholds:

<u>Sequence Release Category*</u>	<u>Cutoff Frequency</u>
1-3	10^{-9}
4, 5	10^{-8}
6, 7	10^{-7}

*PWR release categories from WASH-1400

This proportions the thoroughness of the subsequent studies to the severity of the sequence outcome.

Document the screening technique used to select which sequences are to be given detailed review in subsequent tasks.

It is also important to check the convergence of the quantitative results. In every light-water reactor risk assessment performed so far, a handful of accident scenarios were clearly the dominant contributors to the risk; the grand total risk from the myriad low-probability accident scenarios was found to be very small compared with the risk posed by those few dominant sequences. We believe this to be a general characteristic of LWRs, but it has not been proven to be so. Therefore, it is important to verify that the total of the estimated frequency of all the sequence cut sets discarded in the screening process is very small compared with totaled frequency of accident scenarios that are to be carried forward in the analysis.

3.30 Verification of Sequence Cut Sets

Verify the sequence cut sets by comparison with the dependency diagrams, interaction FMEA, etc. Think through each cut set to verify that it will, in fact, cause all the system failures postulated for that event sequence. Verify the completeness of the cut sets by comparing the accident scenarios predicted in task 27 with the cut sets. Each scenario predicted in task 27 should appear in the cut set lists for one of the event

tree branches. Some may be missing from the cut set lists because they were screened out in task 29. Check to be sure that these genuinely have negligible probability.

3.31 Common Cause Failure Search

Some kinds of common-cause failures or statistically correlated but distinct failures are already modeled in the screening quantification of the event sequence cut sets. Other kinds of common cause failures have not yet been considered. These must be dealt with in this task.

The kinds of common-cause or correlated faults that have been covered already include:

1. Common-cause or correlated failures occurring in different trains of the same system. These should have been modeled explicitly in the screening quantification of the system fault trees.
2. Faults in more than one front line system originating in one or more failures within a common support system. The incorporation of subtrees developing support system failures into the event sequence fault trees should cover such failure modes.
3. Faults in support systems which contribute to the initiating event as well as degrading the reliability of the mitigating systems. The inclusion of fault trees for the initiating

events which trace faults to the support systems should suffice to cover this class of common-cause failure modes.

Although these three classes of common-caused failures should be incorporated in the screening analysis, it is wise to take this opportunity to verify that they are correctly treated during the case-by-case review.

Two classes of common-cause failure that are not already treated correctly are:

1. Statistically Correlated Faults Occurring in different Systems That Do Not Originate In a Hard-Wired Dependency

The most important examples of this are likely to be operator or maintenance errors. For example, the operators might misdiagnose an accident and shut down high pressure safety injection and also shut down containment sprays when both are actually needed, or a procedure for surveillance testing or maintenance could be erroneously applied affecting several systems.

2. Conditional Probabilities

The context underlying the likelihood estimates for the composite fault events in the screening quantification was conditioned upon the top event definitions for the individual front line systems. Some care has been taken in prior steps to assure that these top event definitions

correctly reflect the event tree sequences but even if this has been done without error, it cannot have been highly discriminating. In specific accident scenarios the fault event likelihood may be different.

Each event sequence cut set will have a probability given by a frequency for the initiating event multiplied by the probability of the failures, which, taken together, will give rise to the particular accident of interest.

$$\lambda_{\text{sequence}} = \lambda_{\text{initiator}} P_1 P_2 P_3 P_4 \dots$$

where λ denotes a frequency and the P_i 's denote the concurrent faults.

In the screening quantification, these probabilities have been selected to reflect the broad outlines of the accident sequences, i.e., to the event tree and to the system success vs. failure criteria. However, these checks cannot tailor the probability estimates to the specifics of a particular accident scenario. This must be done now for the accident scenarios that may be dominant.

The revised frequency estimate for the potentially dominant event sequences should reflect the details and conditional probabilities for the concurrent faults that give rise to the accident sequence cut set.

It is also necessary to strip away any unnecessary conservatisms that may have been employed to simplify the screening of the hundred thousand or so accident scenarios emerging from the event tree/fault tree analysis.

An example may help to visualize this task. The event tree may define this sequence as a very small LOCA followed by a failure of high pressure ECC recirculation, and of containment spray recirculation. One of the many event sequence cut sets might attribute the sequence to the following faults: A loss of essential DC power in division B is responsible for a transient induced LOCA and defeats train B of many engineered safety features including HPI and HPR, containment sprays, etc.

Train A of HPI and containment spray injection work properly, but cannot be switched into the recirculation mode due to a fault (plug) in the sump-to-pump suction pipe segment. Therefore, HPR and containment sprays fail in recirculation. The likelihood estimates in the screening analysis will not have reflected the details of this scenario and may require changes. The likelihood that the DC bus fault may be repaired during the injection phase may not have been conditioned on the correct range of times before the point of no return. The distractions in the control room because of the DC bus fault and the consequent instrumentation faults will increase the

likelihood of operator error in making up the correct valve alignment for recirculation at the appropriate time. Lights may be out in the auxiliary building handicapping manual fixes of misaligned valves, and so forth.

General guidelines for the conduct of this task are;

1. Proportion the effort to review the accident sequences to the likelihood and severity of the sequences.
2. Consider all the permutations and combinations of component failures or operator errors or chronological sequences of occurrence that are consistent with the sequence cut set definition. Some of the composite fault events may contain active failures, passive failures, operator or maintenance errors that occur before, during or after the initiating event.
3. Entertain the hypothesis that there may be factors that make the occurrence of any two or more of the distinct failures in the sequence cut set more likely to occur concurrently than the random failure hypothesis would suggest. Search for causal mechanisms for such correlated failures and adjust the frequency estimate accordingly.
4. Eliminate unnecessary conservatism in the frequency estimates and associated assumptions for the dominant risk sequences.

There are computer assisted techniques for identifying fault tree cut sets harboring potential common cause failures. Their use in IREP Phase II and Phase III is optional. They will probably become necessary in successive phases of IREP scoped to address fires, floods, and earthquakes. The computer codes operate by scanning for two or more basic events in any one cut set which share a common characteristic flag. Several characteristic flags are attributed to each fault event by the individual preparing the computer input. They denote features such as the location of the component, the procedures under which it is tested or maintained, component manufacturer, etc. Thus, the computer can identify instances in which two or more apparently distinct fault events that contribute to one accident happen to share the same physical location, the same environmental susceptibility to failure, the same manufacturer, the same maintenance procedure, etc. These computer codes can be a valuable labor-saving device, particularly when very lengthy cut set lists must be scanned for potential common-cause failures. Three computer codes with this capability are COMCAN, BACFIRE, and SETS. These codes cannot replace the case-by-case review of the more important sequence cut sets to replace the screening quantification with more accurate frequency estimates conditioned on the details of the particular causal and chronological possibilities for the accident scenario. It is the intent of the screening

procedure to reduce the number of accident scenarios that require this detailed, case-by-case review to a number small enough that a computerized search for common cause failures is not essential.

3.32 Ranking of Requantified Accident Scenarios

Re-rank the accident sequence cut sets (detailed accident scenarios) in order of descending frequency for each event tree branch. Prepare a description of the dominant accident sequences treating the details of the chronology and causality of the most prominent sequences. We anticipate that a mere dozen or so sequences will be found to be responsible for more than 90% of the total likelihood of severe-release accidents.

3.33 Revision of Event Trees, Fault Trees, and Screening Quantification

It is quite likely that thorough review of the potentially dominant accident sequence cut sets, performed in task 31, will expose omissions or errors in the event trees, fault trees, or the screening quantification. These should be corrected, not merely for future use but also to recheck the screening of the less likely sequences. It is not rare to discover new insights when the alterations are carried forward through the several tasks back to task 31. Thus, two or more cycles of revision may be needed, although the extent of the rework should converge rapidly.

3.34 Failure Mode Logic Diagrams

A useful technique to document the causal mechanisms underlying the dominant accident sequences is the construction of logic diagrams depicting fault propagation through the network of systems. An example from the Crystal River IREP study is attached. These should be prepared for each of the dominant causal mechanisms to illustrate the verbal description called for in task 32.

3.35 Reportage

3.36 Single Point Failures Sufficient to Cause Core Damage

The objective of this task is to focus attention upon those singular, root-cause failures which might realistically give rise to core damage or meltdown without the coincidental occurrence of any other improbable faults. The concept of these singular causes of core damage differs in several respects from the "single failure" criterion employed in licensing. The "single failure" criterion stipulates that no active engineered safety feature may be designed in such a way that the failure of an active component can defeat the safety function. It does not embrace passive failures, human errors, failures in non-safety-grade equipment, nor does it consider the common-causation of the initiating event. The concept employed here is restricted to those singular failures that can precipitate (or be) the initiating event and defeat all

the functions--whether safety grade or not--which would normally be expected to prevent core damage following the initiating event. The root causes are not limited to active failures but rather can embrace any kind of internal or external fault event. Examples of such singular causes of possible core damage include:

1. Gross reactor vessel rupture,
2. Gross plant damage from external events such as missiles, earthquakes, floods, or successful sabotage,
3. A severe in-plant flood or fire, e.g., a more severe version of the Browns Ferry fire,
4. A control system power supply fault that causes a loss of main feedwater, blinds the autostart system for emergency feedwater, and blinds the operators to the need to start backup cooling systems, e.g., a more severe variant of the Rancho Seco "light bulb" incident, and
5. A system interaction involving a vent header fault which could precipitate a feedwater trip and cause one or both scram discharge volumes of a BWR to be filled with water, e.g., a more severe variant of the Browns Ferry scram problem.

There is a sense in which the accident at Three Mile Island Unit 2 is a sixth example. The operators at TMI had been instructed not to permit the pressurizer to go water-solid,

without warning them that a high pressurizer level is symptomatic of a pressurizer vapor space LOCA as well as being symptomatic of an over-full reactor coolant system. With those procedures and operator training in-place, any pressurizer vapor space LOCA could have given rise to a TMI-like outcome without any other failure than the operators following their instructions.

Note that some of these examples fall within the IREP scope for event-tree, fault-tree analysis and should be revealed by the prior analyses, whereas others are not. Examples 4, 5, and 6 should be identified in the principal IREP studies if the plant is susceptible to these scenarios, whereas examples 1, 2, and 3 involve failure mechanisms outside the IREP scope.

The burden of this task is to re-examine the event-tree, fault-tree results to verify that any and all vulnerabilities in the plant to core damage from the kind of single failure suggested in examples 4, 5, and 6 have been identified, to tabulate these single-failure scenarios, and to add to the table any others outside the IREP scope that the team may have identified incidentally in the process of performing the other IREP tasks. It is not expected that the IREP teams expand the scope of the ET-FT analysis to address external events, fires, floods, or sabotage.

A suggested discipline for performing this task is as follows: First, broadly classify the distinct routes to core damage in the plant. The broad classification might look something like this:

1. LOCA plus ECCS failure leading to core damage,
2. ATWS alone or in conjunction with mitigation failure leading to core damage,
3. Feedwater failure together with backup cooling water system failures leading to core damage.

Second, postulate for each of these broadly-defined avenues to core damage that both the initiating event and the failure of the backup systems that are capable--in principle--of preventing core damage, originate from a single root-cause event. Classify and characterize the hypothetical common cause failure mechanisms that could give rise to these core damage scenarios. Third, investigate the design and procedural documentation of the plant to determine whether any of these common cause failure mechanisms could be realized at the plant.

For example, the LOCA plus ECCS failure avenue might be investigated as follows: LOCAs can be classified according to whether or not there is a concurrent triggering event. Those without a concurrent trigger could fail ECCS from a common cause only through the effects of the LOCA, i.e., the LOCA must be intrinsically vulnerable to mitigation failure, perhaps because of its location (vessel rupture, blowdown outside containment so that ECCS recirculation cannot succeed), because of its symptoms (a "signature" that fails to trigger ESFAS and/or confuses operators), or because of its effects (LOCA-induced missiles, jet impingement,

if any, that fail ECCS systems). For those LOCAs that have a concurrent triggering event (earthquake or transient-induced LOCA, etc.) there are potentially common cause failures originating in the trigger event affecting ECCS to be considered as well. This process of working from the abstract and formally complete toward the specific, by alternating analysis and synthesis, can be extended until all the hypothetical singles are classified and found either (i) to exist in the plant, (ii) not to exist in the plant, or (iii) whose existence rests upon ambiguous accident phenomenology.

Although this task is something of a digression from the main thrust of IREP studies, there are several reasons why we feel that the time and effort is warranted:

1. Susceptibilities to core damage from a singular root cause afford less opportunity for discovery through precursor events than do accident scenarios caused by multiple failures. Then, too, most of the more severe incidents that have occurred in commercial power reactors have had this single-cause characteristic. Therefore, these singles deserve particular attention in predictive safety analyses like IREP.
2. The simplicity intrinsic to accident scenarios with a single root cause permits an independent check to be made of the completeness and accuracy of the event tree, fault

tree analyses for singles that can reveal errors or omissions in the main body of IREP work.

3. The expertise developed by the IREP team on the susceptibility of the plant to severe accidents may dissipate after the teams are disbanded. Therefore, particularly significant safety insights discovered by the team should be reported--to the extent practical--in the published report even for those insights outside the principal IREP scope. The most important of these out-of-scope safety insights are likely to involve single point vulnerabilities to core damage.

The reportage of the single root-cause core damage study in the main IREP study can be fulfilled by an annotated list of single fault scenarios. The notes should identify the assumptions and briefly describe the fault propagation by which the single root cause initiates the disturbance and defeats the mitigating functions. In addition, a brief description of the logical development should be reported in an appendix. The methodology suggested above for an independent search for singles is experimental. Experiences with its use should be reported to the IREP project management for use in improving the procedure guide.

3.37 Review and Documentation of Dominant Accident Sequences

This is the final task before the preparation of the draft of the final report. It should include the following elements:

1. Discussion of the dominant accident sequences with the plant operators, operations management, and utility staff engineers.
2. Requantification of the more prominent sequences (dominant and contributory sequences) with plant-specific failure rate data where feasible.
3. Uncertainty analysis for dominant sequences.
4. Sensitivity analysis for dominant sequences.
5. Description of the symptom profile ("signature") of the dominant sequences.
6. Description of the options available to the operators to repair failed systems or otherwise prevent or mitigate the dominant sequences.
7. Discussion of the range of warning times for implementation of the emergency plan.
8. Drafting of systemic event trees including support systems to portray the causality of the more prominent accident sequences.
9. Discussion of the additional research necessary to resolve ambiguities in the identification and quantification of the dominant accident sequences.

It is important to present and discuss the dominant sequences with the plant operators, operations management, and the plant owner's staff engineers. Their review of the IREP results may reveal errors or unnecessary conservatisms in the principal results. It is particularly likely that they can shed light on the conduct of critical procedures or supply plant-specific failure rate data with which to refine the frequency estimates for the dominant sequences.

It may prove to be convenient to conduct these reviews at the plant site and to take this opportunity to develop--with the help of the plant operators--descriptions of the symptom profile that will emerge in the control room during the dominant accident sequences. Describe the hypothetical success paths by which operators might nip the dominant accidents in the bud, e.g., repair. Develop a brief discussion of the pros and cons of the several tactics the operators might employ to deal with the developing accident. Is it plausible or likely that the operators might misconstrue the accident and develop an erroneous hypothesis of what needs to be done? What range of warning times will be available for public protective action between the diagnosis of the severity of the situation and the occurrence of the major release of radiation? Following the collection of critical plant-specific failure rate data and discussions with owner's personnel, some further analysis will be necessary. Wherever feasible, use the plant-specific

failure rate data to refine the probability estimates for the dominant sequences. Perform a sensitivity study to assess the importance of the fault events appearing in the dominant and contributory sequences to the overall risk. Also estimate the importance of several distinct classes of fault events:

1. passive failures,
2. random active failures,
3. common-cause equipment failures,
4. maintenance and operator errors occurring before the initiating event,
5. operator errors and conversely operator corrective action during the incident.

The uncertainty analysis for the dominant sequences should include not merely the assessment of the statistical uncertainty originating in imprecisely known fault event likelihood but also a discussion of the modeling approximations and phenomenological assumptions which also contribute to uncertainty. Include in the report of the uncertainty analysis the team's best judgment of the completeness with which the dominant sequences have been identified. The report should include a brief discussion of any further research that may be needed to resolve significant modeling uncertainties affecting the dominant accident sequences.

Finally, it may prove to be useful to draft event trees at the system level which incorporate support system failures to aid

in the documentation of the results. Such trees are awkward to work with in analysis compared with event trees that depict only front line systems; however, event trees showing support systems provide a classification scheme and graphical depiction that better reflects the principal causal mechanisms underlying important sequences.

3.38 Draft Report

Prepare a draft edition of the final report for use in peer review of the technical and editorial content. A more detailed guide will be prepared for text scope and format. However, we expect that the main report will adhere closely to the task products, with the system fault trees and the details of the quantification reserved for appendices.

3.39 Report Review

An NRC Research Review Group will be constituted to assemble constructive criticism of the draft. The plant owner's review will constitute a second independent peer review. The IREP team will be expected to present and discuss their work at each of the two review group meetings. The review groups will have at least 2 weeks to study the draft before the review group meetings. Each review group will be expected to prepare a written critique within 2 weeks of the review group meeting. Generally, these are prepared in draft form before the review group meeting and edited into final form in the 2 weeks following

the review meeting. Experience has shown that the IREP team itself will be able to identify many shortcomings in this draft report so that we can expect them to be largely occupied by revisions during the review period. The team should also make itself available--at least by telephone--to answer questions by the review group members. NRC and Sandia IREP project management will conduct a limited technical and thorough editorial review.

3.40 Final Report

The IREP team should prepare a final report in the format of a NUREG document. All comments received from the review groups that affect the character, likelihood, or selection of the dominant accident sequences should be addressed. Comments that do not bear upon the dominant sequences should be addressed insofar as time and resources permit.

IREP EVENT TREE METHODOLOGY

Introduction

The proposed IREP event tree methodology is the subject of this chapter. Many of the event tree definitions and terms used in this chapter are similar to that used in WASH-1400, Appendix 1. For that reason it is suggested that the reader review that material as a prerequisite.

The type of reactor accidents of concern in the IREP are core meltdown accidents initiated by a variety of transients and LOCA's. It is also a goal of IREP to rank these core melt accidents in terms of expected frequency and consequence severity. The consequences associated with a core melt accident depend not only on the initiating event but also on which safety systems succeeded or failed during the accident and the approximate time at which they failed; i.e., the accident sequence.

Event trees are the structures from which accident sequences are derived. Two event tree types, used in succession, produce the complete accident sequences. The system event tree interrelates the initiating event and the safety system failure events and results in system accident sequences. The containment event trees relate the possible responses of the containment to the accident phenomenology associated with each system accident sequence. The resulting containment failure modes are added to the system accident sequences to form the complete accident sequences.

This chapter is divided into the following event tree topics:

- 1.0 Event Tree Construction
- 2.0 Event Tree Initiating Events
- 3.0 Development of Event Tree Heading Failure Definitions
- 4.0 Display of Dominant Accident Sequences
- 5.0 Accident Process Analysis of Event Tree Sequences

These topics represent the major IREP event tree analysis steps. The first four topics are concerned with the construction and utilization of system event trees to determine system accident sequences for the IREP plant. The last topic is concerned with classifying these accident sequences in terms of consequence severity and use is made of the containment event tree. A discussion of each of these major analysis steps with appropriate illustrative examples is presented first followed by a summary list of procedures.

1.0 Event Tree Construction

The first step in modeling core melt accidents over the full range of consequence severity is to construct a functional event tree. Construction of a functional event tree requires the determination of the functions the plant systems perform to either successfully mitigate a LOCA or transient, or lessen the consequences of a core melt if mitigation of the LOCA or transient is unsuccessful. These functions will now be discussed.

1.1.1 LOCA Functional Event Tree Construction

In response to a LOCA, reactor systems perform the following basic functions:

- A) reactor subcriticality
- B) emergency core cooling

- C) radioactivity removal from the containment atmosphere
- D) containment overpressure protection due to steam evolution

Except for reactor subcriticality, which must be performed immediately after the LOCA, the other functions must be continuously performed for an extended period of time (weeks). In order to estimate the consequences (defined in terms of radioactivity release) of a particular LOCA accident sequence, it is important to know which functions failed and the time at which they failed. The timing consideration can be handled to a certain extent by splitting functions B through D into injection and recirculation phases and splitting the recirculation phase of functions B and D into an early recirculation phase and late recirculation phase. The functions now become:

- A) reactor subcriticality
- B) emergency core cooling during injection phase
- C) radioactivity removal during injection phase
- D) containment overpressure protection during injection phase
- E) emergency core cooling during recirculation phase
- F) radioactivity removal during recirculation phase
- G) containment overpressure protection during recirculation phase
- H) { containment overpressure protection during late recirculation phase } Containment
 { emergency core cooling during late recirculation phase } heat
 { } removal

The last two functions can be replaced by a single containment heat removal function; since, if containment heat removal fails to be initiated during the late recirculation phase, both of these functions fail. This is because the containment will eventually fail due to overpressurization followed by an assumed failure of the emergency core cooling function due to pump cavitation.¹

There are, therefore, three time frames modeled by the above set of functions. These time frames represent relative rather than absolute time frames (e.g., depending on the LOCA size, the injection phase may range from approximately 30 minutes to several hours). It is assumed that if a function succeeds at the start of a time frame, it will continue to be successful throughout the time frame. This is equivalent to saying that the failure probabilities of the systems which comprise the functions are dominated by their unavailability (e.g., failure to start or change state) rather than the unreliability (e.g., failure to continue successful operation).

A functional LOCA event tree can be constructed by making these eight functions the event tree headings and incorporating the functional interdependencies into the event tree structure. The functional interdependencies are incorporated into the event tree structure by removing success/failure decision points at appropriate places in the tree. The following criteria should be utilized for removing decision points:

¹ It should be noted that whether or not the pumps will actually fail due to cavitation depends upon the temperature of the containment sump water or vapor suppression pool water at the time of containment failure.

- 1) Function X succeeds/fails by definition due to success/failure of function(s) Y, Z, etc.
- 2) Function X fails due to the expected system physical processes (e.g. system thermohydraulic dynamics) associated with the accident sequence.
- 3) Success/failure of function X does not matter due to the type of initiating event or the success/failure of function(s) Y, Z, etc.

As an example, let us construct the large LOCA functional event tree for the Oconee reactor studied in the RSSMAP.

Table 1 lists the eight functions and the corresponding plant systems required to perform the functions. Figure 1, the functional LOCA tree, depicts the inter-dependencies between these functions along with a table which lists the functions which failed in each sequence. The interdependencies reflected in the tree structure result from application of criteria one and three given above. Application of criterion three was used in eliminating the success/failure choice for reactor subcriticality. For a large LOCA the voids created in the reactor core during the blowdown will automatically render the reactor subcritical and success/failure of the system which provides the reactor subcriticality function does not matter. The remaining interdependencies reflected in the tree structure result from application of Criterion 1. For example, no success/failure choice is given for containment heat removal on sequence seven since for this sequence containment heat removal would be defined as succeeded due to the defined success of the RBCS. This is because it is known that containment overpressure

TABLE 1

Alternate Equipment Success Combinations For Functions
Incorporated Into the Dones LOCA Event Tree

LOCA Size	Reactor Subcriticality	Injection Phase			Recirculation Phase			Late Recirculation Phase
		Emergency Core Cooling	Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Emergency Core Cooling	Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Containment Heat Removal
(>1.0 ft ²) A LOCA	No System Needed	1/3 High Pressure Injection (HPI) and 1/2 LPI and 2/2 CPT	1/2 Containment Spray Injection (CSIS) OR 1/3 Reactor Bldg. Fan Coolers (RBCS)	1/2 CSIS	1/2 LPRS Low Pressure Recirc. (LPRS)	1/2 Containment Spray Recirc. (CSRS) OR 1/3 RBCS (during recirc. phase)	1/2 CSRS	1/2 CSRS With LPRS Heat Exchanger OR 1/3 RBCS (during late recirc. phase)

succeeded. This is because it is known that containment overpressure during recirculation succeeded due to the success of the RBCS only, since the CSRS failed to provide radioactivity removal in this sequence.

It can be noted from Figure 1 that ECI failure implies ECR failure. This is consistent with the approach taken in WASH-1400. By glancing at Table 1, it is seen that ECI could fail due to failure of the accumulators only. If this failure mode occurs, ECR would not be precluded. If it is determined that ECR success given ECI failure has a significant effect on accident consequences, then a success/failure choice for ECR given ECI failure should be incorporated into the event tree structure.

1.1.2 Transient Functional Event Tree Construction

In response to a transient, the reactor systems perform the following functions during the early phase of reactor shutdown:

- A) reactor subcriticality
- B) initial core cooling
- C) reactor coolant system overpressure protection

Reactor subcriticality must be achieved immediately following the transient. RCS overpressure protection is necessary if, for a given transient, the plant design requires it or if a delay is experienced in achieving initial core cooling. It should be noted that one additional function, RCS inventory control, could be included in the above list as being required if an RCS safety or relief valve failed to reclose after performing its RCS overpressure protection function. However, an accident sequence with a stuck open

safety or relief valve constitutes a small LOCA and can therefore be transferred to the LOCA tree and treated as such. By making this transfer the functions and corresponding systems required to mitigate these transient induced LOCA's are made more explicit.

The functions stated above are required to bring the plant to a hot shutdown condition. Since a PWR can be maintained in a hot shutdown condition without threatening a core melt for an extended period of time (provided enough stored cooling water is available), the above functions are an adequate representation for the important PWR functions.¹ In the case of a BWR, however, a hot shutdown condition cannot be maintained for as long as a PWR unless a long term core cooling system is activated. The reason for this is that the heat sink for the systems performing the initial core cooling function at a PWR can be the atmosphere whereas the heat sink for the similar BWR system is a closed system such as the suppression pool or condenser. If long term cooling of these closed systems is not achieved, then the core would eventually overheat and melt and/or the containment would overpressure and fail. It is, therefore, necessary to consider the following function for a BWR:

D) long term core cooling (BWR only).

If successful mitigation of the transient cannot be achieved and a core melt ensues, the following plant functions can aid in lessening the consequences of the accident:

¹It should be noted that at some PWR power plants, the function of initial core cooling can be provided by injecting cooling water directly into the RCS and allowing it to boiloff through the RCS safety or relief valves and discharging into the containment. If this cooling method is utilized for an extended period, then the function of containment overpressure protection due to steam evolution must also be provided.

- E) radioactivity removal from the containment atmosphere
- F) containment overpressure protection due to steam evolution

A functional transient event tree can be constructed by making these 5 PWR and 6 BWR functions the event tree headings and incorporating the functional interdependencies into the event tree structure. Each core melt sequence on the event tree would be characterized by a different combination of succeeded and failed functions.

As an example, let us construct the transient functional event tree for the Oconee reactor. Table 2 lists the 5 PWR functions and the corresponding plant systems required to perform these functions. Figure 2, the functional transient tree, depicts the interdependencies between these functions along with a table which lists the functions which failed in each sequence.

Before discussing the dependencies depicted on the tree, an explanation of the events which appear before and after the Reactor Coolant System Overpressure Protection (RCSOP) heading is in order. As mentioned earlier, the requirement for the RCSOP function depends on the type of initiating event and/or if initial core cooling has been delayed. These cases are explicitly covered by the inclusion of this event. The event after RCSOP is included to identify the transient induced LOCA sequences discussed earlier.

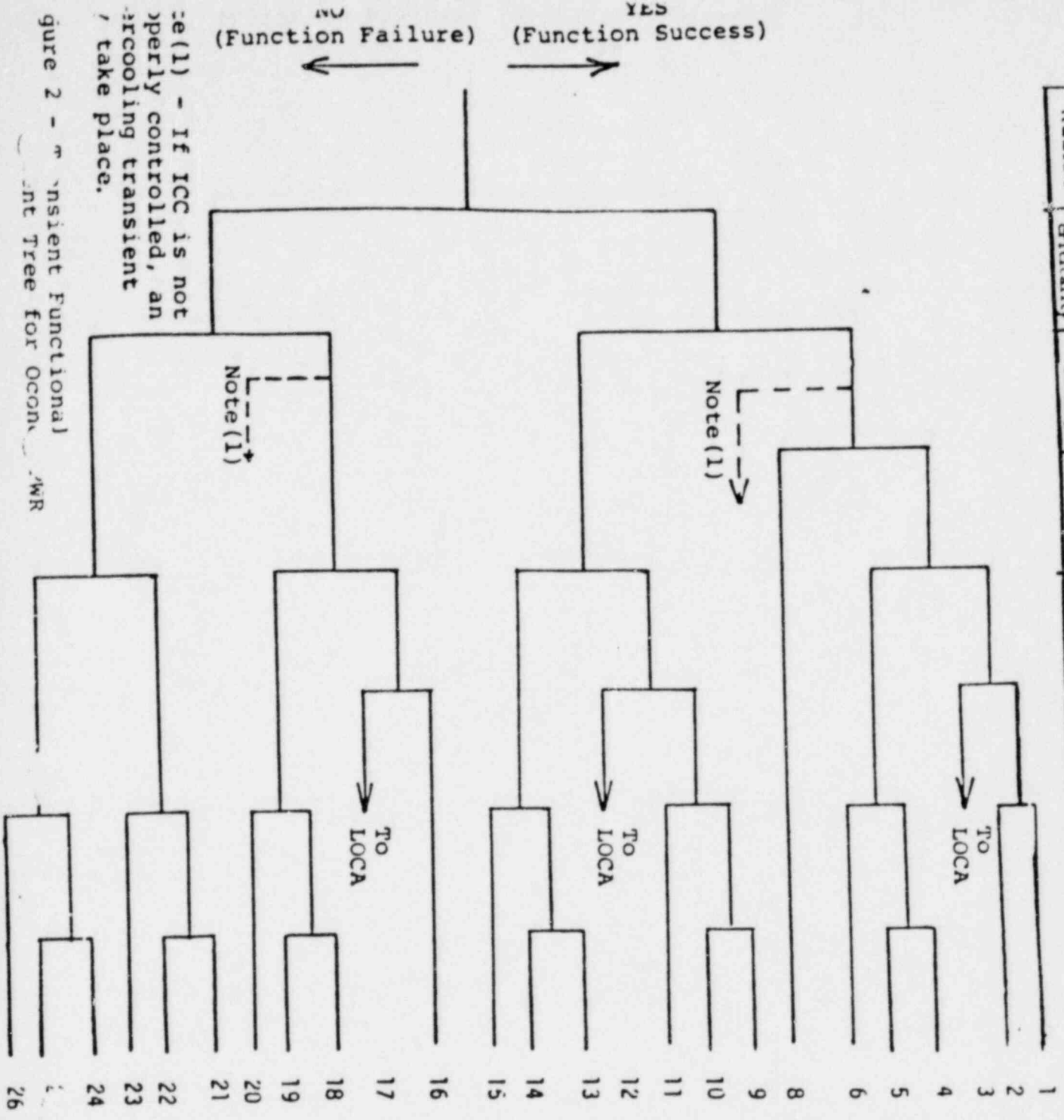
The dependencies incorporated into the event tree structure result from application of all three criteria presented in the

Table 4

Alternate Equipment Success Combinations for
Functions Incorporated Into Oconee Transient Event Tree

Subcriticality	Core Cooling	Reactor Coolant System (RCS) Overpressure Protection	RCS Integrity	Containment Overpressure Protection Due to Steam Evolution	Post-Accident Radioactivity Removal
<p>> 6 Control Rod Groups Inserted Into Core by the Reactor Protection System (RPS)</p>	<p><u>RPS Success</u></p> <p>Power Conversion System or Emergency Feedwater System or High Head Auxiliary Service Water System or 1/3 High Pressure Injection System</p> <p><u>RPS Failure</u></p> <p>Power Conversion System or Emergency Feedwater System and 1/3 High Pressure Injection System</p>	<p>1/3 Safety/Relief Valves Open When Demanded</p>	<p>All Safety/Relief Valves Reset</p>	<p>1/3 Reactor Building Cooling System Fan Trains</p> <p>or</p> <p>1/2 Containment Spray System w/Recirculation</p>	<p>1/2 Containment Spray System w/Recirculation</p>

Transient	RP9 Reactor Sub- criticality	RPV Initial Core Cooling	RCS Overpressure Requirement	SRV RCS Overpressure Protection	ICV RCS Overpressure Valves Close	RCS or CSIS Overpressure Requirement	CSIS Nucleonically Removal
-----------	---------------------------------------	-----------------------------------	------------------------------------	--	---	--	----------------------------------



1	2	3	4	5	6	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	26
S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D
E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

X (SUCCESS ASSUMED)

Figure 2 - Transient Functional Decision Tree for Occurrence of WRR

previous section. Examples of how these three criteria were incorporated into the tree structure are the following:

Criterion 1) Radioactivity removal is by definition failed if containment overpressure fails due to the defined failure of the CSIS. This is because it is known that the CSIS failed if containment overpressure failed. Criterion 2) The RCS overpressure valves will not reclose given failure of reactor subcriticality and initial core cooling. This is because the RCS pressure will equilibrate at a level at or above the pressurizer relief valve reclosure setpoint and will remain there throughout core meltdown. Criterion 3) As mentioned previously, radioactivity removal is an important mitigating function in core melt accident sequences only. For non-core melt sequences, therefore, the success/failure of this function does not matter.

Additional explanation is in order concerning the "note 1," depicted in Figure 2. Given success of initial core cooling if the flow rates of the main or auxiliary feedwater systems are not properly controlled and too much cooling is provided to the secondary side of the steam generators, a rapid RCS cooldown transient would ensue. Following RCS depressurization, due to the shrink of the RCS coolant, the high pressure injection system would be demanded at the Oconee plant. If actuation occurs, the pressurizer relief valves could be demanded and thus create a potential for a LOCA if they do not reclose. This particular sequence could be modeled as part of the existing sequence 3. When transferring to the small LOCA tree, the high pressure injection system and auxiliary feedwater system would

be defined as operating (success). However, if actuation does not occur, a potential exists for emptying the pressurizer due to the continued shrink of the RCS coolant. If this occurs, pressure control of the RCS is lost, which could ultimately result in a saturated RCS. If forced RCS circulation is lost (as would be the case for a loss of offsite power transient) and the RCS is saturated, natural circulation would also be lost at the Oconee plant. The core would then lose steam generator cooling and RCS inventory would boil off eventually leading to a core meltdown. This latter case is not modeled by any event tree sequence presented thus far. Since it is a special case, it does not warrant a separate event tree and is discussed here for completeness.

1.1.3 LOCA and Transient Systemic Event Tree Construction

It can be noted from the functional event tree examples given in the previous sections, that in general there is not a one to one correspondence between the functions modeled on the event tree and the plant systems required to perform these functions. Because of this the same system may appear in the definitions of more than one functional event tree heading. It is often desirable to decouple the functional event tree headings such that each heading represents a major plant system or group of plant systems (i.e., "front line systems"). (A front line system is defined as the system described in the plant FSAR which performs the LOCA and transient functions described in the previous sections. A front line system does not include support systems common to many front line systems such as electric power systems, component cooling water systems,

(instrument air systems, etc.) This type of event tree is known as a systemic event tree and the tree structure would reflect interdependencies between major plant systems rather than plant functions.

The LOCA and transient systemic event trees for the Oconee plant are presented in Figures 3 and 4. The event tree headings represent the major systems described in the Oconee FSAR. The system event tree headings are listed in the approximate order they will be called upon during a LOCA or transient accident sequence. The event tree structure reflects the application of the criteria presented in Section 1.1.1 (replace the word "function" with "system"). Also depicted on these figures are tables which list the functions which failed in each sequence.

If one compares the LOCA and transient functional and systemic event trees it can be noted that the system trees contain a greater number of accident sequences. These additional sequences result from the fact that several system accident sequences may be represented by a single functional accident sequence. Each functional accident sequence represents a unique set of succeeded and failed functions whereas each system accident sequence may not. For example, sequences 8 and 17 on the LOCA systemic event tree are modeled by the single sequence 4 on the LOCA functional event tree.

1.2 Procedure

Procedure for Functional Event Tree Construction

1. LOCA functional event tree construction.

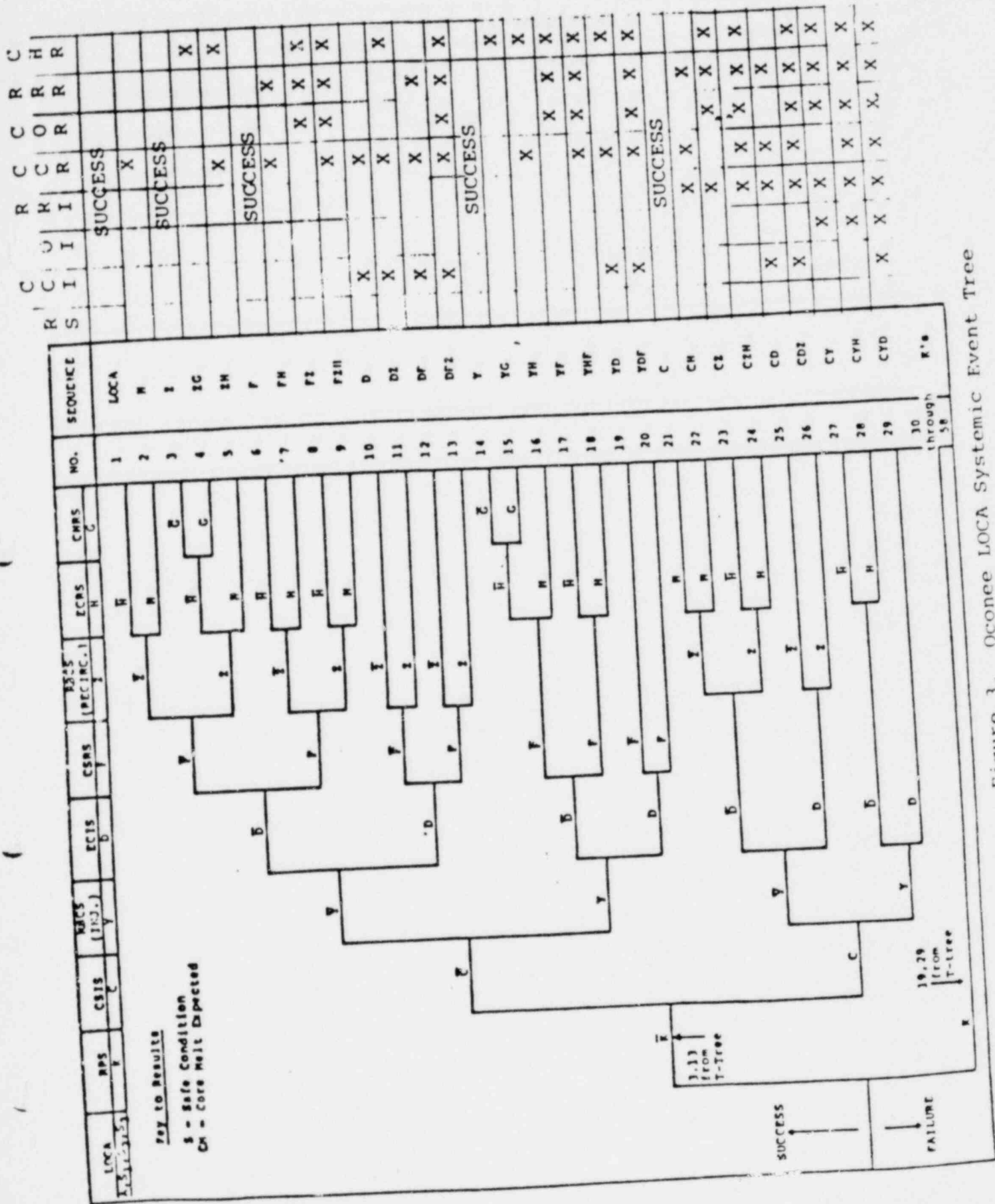
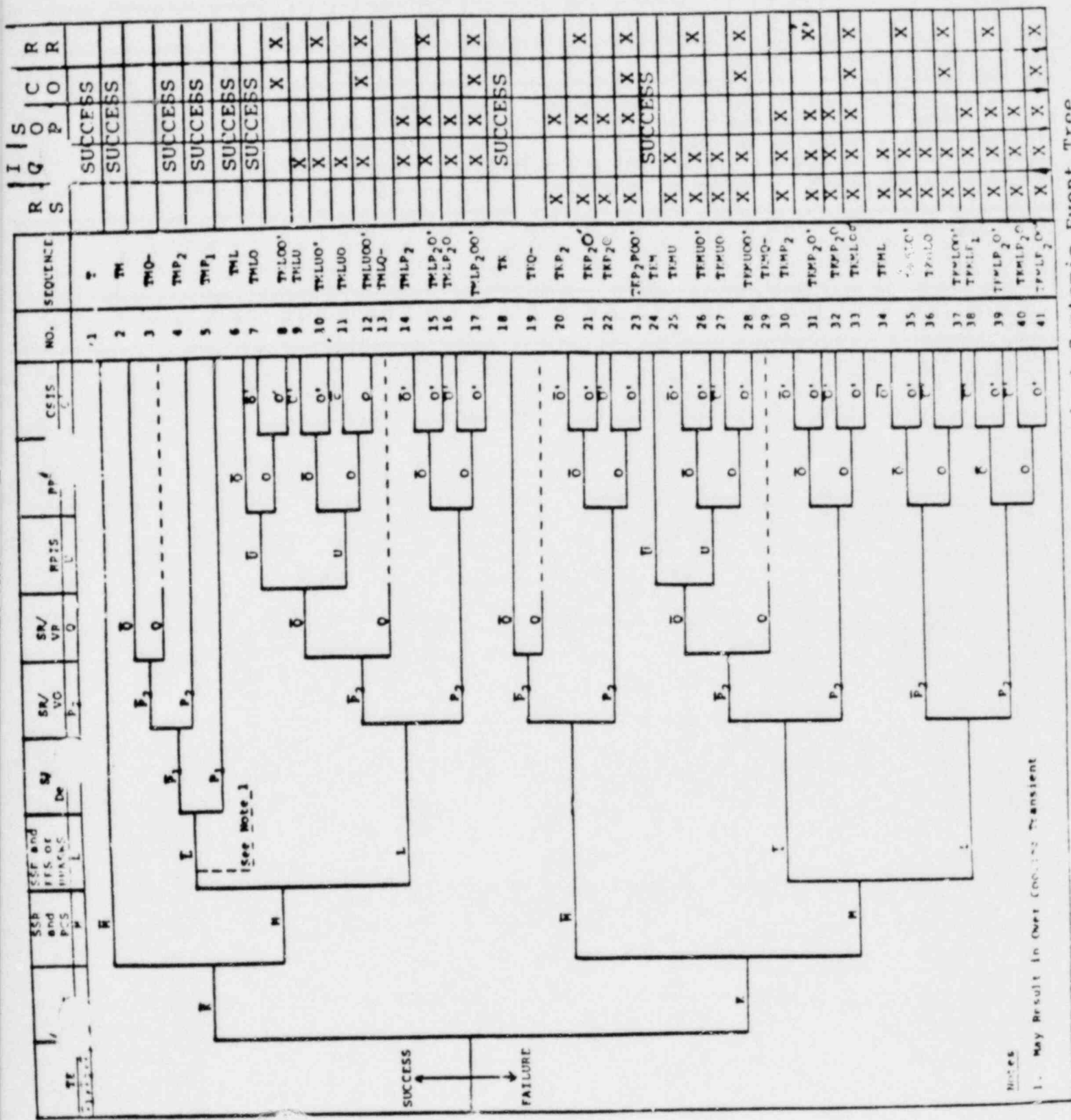


Figure 3. Oconee LOCA Systemic Event Tree



(Assumed)

Figure 4. Oronoo Transient Customic Front Tree

Notes
 1. May Result in Over Cooling Transient

- a. Identify from the FSAR the plant ESF systems/sub-systems which perform the following functions:
- 1) reactor subcriticality
 - 2) emergency core cooling
 - 3) radioactivity removal from containment atmosphere
 - 4) containment overpressure protection due to steam evolution
 - 5) post LOCA containment heat removal.
- b. Determine the minimum number of ESF systems/sub-systems which are required to successfully perform these functions. The FSAR usually states success criteria for a variety of LOCA sizes. Discuss the FSAR success criteria with the reactor vendor or other sources and determine if it is overly conservative. FSAR criteria need not be used if sufficient documentation is available supporting an alternate criteria.
- c. For functions 2 through 4, determine if different success criteria are required for the injection and recirculation phases.
- d. The five functions listed above become eight functions due to the split of 2 through 4, into injection and recirculation phases. These eight functions will comprise the event tree headings. (Refer to Oconee LOCA tree example given in this section.)

- e. Incorporate functional interdependencies into the event tree structure by applying the criteria presented in Section 1.1.1.
 - f. Characterize each accident sequence by determining which functions have succeeded and failed in each accident sequence. (This will be used later during the analysis of these sequences for core meltdown physical processes.)
2. Transient functional event tree construction.
- a. Identify from the FSAR the plant ESF systems/subsystems which perform the following functions:
 - 1) reactor subcriticality
 - 2) initial core cooling
 - 3) RCS overpressure protection
 - 4) long term core cooling (BWR only)
 - 5) radioactivity removal from the containment atmosphere
 - 6) containment overpressure protection due to steam evolution.
 - b. Same as Part 1-b.
 - c. These functions will comprise the event tree headings. Add the "RCS overpressure requirement" and "RCS overpressure valves reclose" headings before and after the RCS overpressure protection heading. (Refer to Oconee transient event tree example given in this section.)
 - d. Same as Part 1-e.

- e. Same as Part 1-f.
3. LOCA systemic event tree construction.
- a. Determine the "major" FSAR LOCA systems. "Major" systems are those which perform the eight LOCA functions given in 1-d and do not include support systems (e.g., electric power, component cooling, etc.). These systems will comprise the event tree headings.
 - b. Place these systems in the approximate order they will be called upon during a LOCA.
 - c. Incorporate systemic interdependencies into the event tree structure by applying the criteria presented in Section 1.1.1. (Replace the word "function" with "system.")
 - d. Determine which functions have succeeded and failed in each accident sequence. (This will be used to identify the LOCA system accident sequences with their equivalent LOCA functional accident sequences.)
4. Transient systemic event tree construction.
- a. Determine the "major" FSAR transient systems. "Major" systems are those which perform the transient functions given in 2-a and do not include support systems. These systems will comprise the event tree headings. Add the "SR/Demand" and "SR/VR" headings before and after the "SR/VO" heading.

b.-d. Same as 3-b through 3-d. Replace the word
"LOCA" with "transient."

2.0 Event tree Initiating Events

2.1 Discussion

In the preceding section, the generic PWR and BWR LOCA and transient functions were identified and examples were given which identified the plant systems to the appropriate functions. The question which is now asked is how will various size LOCA's and different types of transient initiators affect the performance of these systems. After answering this question, it becomes clear which LOCA and transient initiators must be considered.

For the plants studies in the RSS, it was determined that three ranges of RCS LOCA sizes must be considered as initiating events. Three sizes were chosen since the LOCA mitigation requirements (ECCS, reactor protection system, and auxiliary feedwater system) were a function of the size of the LOCA. However, they could be grouped into three categories for which the mitigation requirements were the same for each category. In a similar manner, each IREP plant will have to be evaluated to determine which LOCA range sizes must be considered. Also important is the location of the break (e.g., a cold leg break may require a different set of ECCS subsystems than a hot leg break). Direct use of the RSS LOCA sizes for the IREP plant without a prior evaluation would be incorrect.

Transient initiators considered in the RSS were of three major types. These were reactor shutdowns caused by a loss of offsite power, loss of the power conversion system (e.g., heat rejection to

the condenser via the main steam, bypass to condenser and main feedwater loop) caused by other than a loss of offsite power, and other shutdowns in which the power conversion system is initially available. These transient initiators were assessed to adequately represent a spectrum of LWR transients (RSS, Table I 4-9, I 4-12 for PWR's and BWR's respectively) in terms of their effects on the mitigating systems. (For example, a loss of offsite power requires the operation of an emergency AC power system to operate various components of the mitigating systems whereas shutdowns with offsite power available do not require emergency power.) Subsequent to the publishing of the RSS new transient initiator data sources, which supercede Tables I 4-9, I 4-12, have been made available. One of the most notable sources is "EPRI-NP801 ATWS: A Reappraisal, Part III, Frequency of Anticipated Transients." This data source should be examined for each subject plant to determine what types of additional transient initiators should be considered. (A listing and description of the PWR and BWR transients which appear in this document are presented in Appendix 1.)

EPRI NP-801 serves as a satisfactory starting point from which to estimate the types and frequencies of transients to be expected in the subject plant. It does not, however, indicate the specific cause of the transient. For example, PWR transient 36 indicates a transient can be caused by a loss of power to a necessary plant system. It does not indicate the specific type of power failure (e.g., Train A Vital AC, Train B 125 V DC, etc.) or what effect these power failures have on the safety systems

which must respond to the transient (e.g., the auxiliary feedwater system may lose the use of an electric driven pump). One method of identifying all such plant specific transients is to develop an initiating event fault tree.

The top event of an initiating event fault tree would be labeled "Requirement for a Reactor Shutdown." The second level of the tree would be a listing of the reactor scram signals. Subsequent levels of the fault tree would be developed such that all subsystem and/or component failures which cause a reactor scram signal are identified. The plant LER's should be reviewed so that any peculiar initiating events can also be modeled on the tree. Special attention should be taken in developing those areas of the fault tree where it is noted that the initiating event could also significantly degrade the reliability of any of the safety systems which must respond to the reactor shutdown.

One additional initiating event which should be considered is the extra-containment or interfacing system LOCA (event V in the RSS). This initiator is actually a complete accident sequence, since no reactor systems are available to mitigate this initiating event. An assessment of all low pressure piping that interface with the high pressure RCS, and which lead outside containment, should be made to determine if the frequency of failure of the isolation valve(s) is quantitatively significant ($\sim 1 \times 10^{-7}/\text{yr.}$). The methods used in quantifying this initiating event have been discussed for a variety of isolation valve configuration and isolation valve test procedures in the RSS, RSS MAP and

EPR1 NP-262 - "PWR Sensitivity to Alterations in the Interfacing System LOCA."

2.2 Procedure

Procedure for Selecting Event Tree Initiating Events

1. LOCA initiating events selection
- a. Select RCS LOCA break size ranges. A separate break size range should be considered if a unique combination of ECCS subsystems or other ESF systems are required to mitigate a LOCA within a certain break size range.
- b. Select RCS LOCA break locations. A separate break location should be considered if a unique combination of ECCS subsystems or other ESF systems are required to mitigate a LOCA at a certain break location.
2. Interfacing system LOCA initiating events selection
- a. Identify low pressure piping which interfaces with the high pressure RCS and lead outside containment. Assess if isolation valve(s) failure is quantitatively significant ($\sim 1 \times 10^{-7}/\text{yr.}$).
3. Transient initiating events selection
- a. Reactor trips caused by a loss of offsite power will be studied.
- b. Loss of power conversion system reactor trips caused by other than a loss of offsite power will be studied.
- c. Reactor trips with the power conversion system initially available will be studied.

- d. Review EPRI-NP801 and determine what types of additional transient initiating events should be considered.
- e. Develop an initiating event fault tree to a level such that all the specific subsystem and/or component failures which cause a transient are identified. Check the initiators identified in the fault tree with the general initiators described in EPRI-NP801 and plant specific LER's to assure completeness.

3.0 Development of Event Tree Heading Failure Definitions

3.1 Discussion

After completing the construction of the functional and system event trees and determining which initiating events will be studied, the next task of the event tree analysis team is to develop event tree heading failure definitions, which will instruct the fault tree team modeling these events how to structure their fault trees. These definitions, in general, depend upon the type of initiating event and on the success or failure of other functions which appear in an accident sequence.

In the previous sections, the functional event tree heading failure (or success) definitions were discussed to a limited extent. Definitions in those sections were limited to determining what combinations of systems were required. This is the proper first step, but in order to complete the definition, one must understand:

- 1) the procedures which dictate how the systems will be implemented
- 2) the expected physical process dynamics for each sequence.

Examples of why this understanding is important follow.

Consider an accident sequence in which the containment overpressure function is performed by a spray system. Following a large LOCA, the containment pressure would rapidly rise and the spray system would be called upon to start automatically when the actuation set point is reached. The role of the control room operator would be to verify that the sprays had started and were performing as designed. However, following a small LOCA, the containment pressure would rise more slowly such that the operator would have time to implement a small LOCA emergency procedure. Let us assume that one step in the procedure was for the operator to bypass the automatic LOCA circuitry and take manual control of the systems. If at a later time, the pressure in containment finally reached the point where sprays were required, they would have to be manually initiated. The event tree should incorporate this subtlety into the containment overpressure event/containment spray system definition so that credit for an automatic start is not given for the small LOCA situation.

A classic example of how the accident sequence physical processes can affect the event tree heading/system failure definition is the accident sequence that occurred at Three Mile Island. That accident sequence was initiated by a loss of main feedwater, followed by a failure of a pressurizer relief valve to reclose and initial success of core cooling through the operation of the high pressure injection system (HPIS). The operator at a later time essentially terminated the HPIS because a high pressurizer level was indicated and he did not want to drive the pressurizer solid (prior to TMI operators were trained to avoid a solid pressurizer).

It is evident that the knowledge of whether or not the pressurizer is solid is crucial to the formulation of the correct HPIS failure definition for this sequence. This is an example of how an operator error which occurs during the course of an accident affects the event tree heading/system failure definition. In order to assess other similar types of operator errors, the analyst must be aware of the control room indications which the operator is relying upon to make decisions and how these decisions will affect the availability of the safety systems responding to the accident.

As a third example, consider a PWR accident sequence which is initiated by a loss of main feedwater and followed by a failure of the reactor subcriticality function (ATWS). The initial physical process associated with this accident would be that the pressurizer would become water solid and a large quantity of water would be passed through the relief valves. The RCS system pressure would eventually be reduced until the closure set point of the relief valves was reached. If they fail to reclose, a small LOCA would exist. Since the pressurizer relief valves are designed to pass steam rather than water, the valve reclosure failure probability would be expected to be substantially higher in ATWS sequences over what it would be for sequences in which only steam was relieved. It would be the responsibility of the event tree team to incorporate this subtlety into the RCSOP valves closed event definition so that a proper assessment of the valve closure failure probability could be made.

As a final example, assume that the above described ATWS occurs and the initial core cooling function is called upon. Since an ATWS is a rapid transient, if initial core cooling is going to have any affect on mitigating the accident, it must be initiated immediately. It will be recalled from the example discussed in Section 1 that a success mode of initial core cooling was to restore the main feedwater system. Given an ATWS, this would take too much time and could not be considered. The event failure definition for initial core cooling given an ATWS, must therefore include this subtlety.

The examples above attest to the fact that the event tree team must have a good overall understanding of the plant behavior if the correct event tree heading failure definitions are to be developed. To gain this understanding, the team must be completely familiar with the plant procedures and the expected physical processes for each accident sequence on the event tree. Much of this can be learned by reading the plant operating, abnormal, or emergency procedures, which discuss either the total event tree sequence or portions of that sequence. What cannot be learned from the procedures should be asked of the control room operators at the initial plant visit. A good portion of the expected physical processes associated with each sequence can also be learned from discussion with control room operators. However, it would not be expected that the operators could give a complete description, especially if the multiple system failures have occurred and the plant is operating in a mode not covered by any procedure. If a complete description is required, then a computer

model which simulates the physical process dynamics of the IREP plant accident sequence would have to be utilized. Such a computer model will most likely be supplied by the reactor vendor.

3.2 Procedure

Procedure for Developing Event Tree Heading Failure Definition

1. Refer to Functional Event Construction Procedure for determining the combinations of ESF systems required to perform the LOCA and transient functions.
2. Develop a top level fault tree depicting these requirements (see Figure 5 for an example).
3. Review operating, abnormal operating, or emergency procedures associated with each event tree sequence or portion of each sequence, if available. If not available, discuss expected operator actions with the control room operators.
4. Understand the expected physical processes associated with each accident sequence.
 - a. Discuss with control room operators to gain a general description.
 - b. If description is not complete, then utilize a computer model which simulates the physical processes of the IREP plant. An adequate model should be available at the reactor vendor.
5. From the knowledge gained in steps 3 and 4, modify the top level fault tree failure definition, if necessary. These modifications should appear as "notes" on the top level tree (see Figure 5 for example).

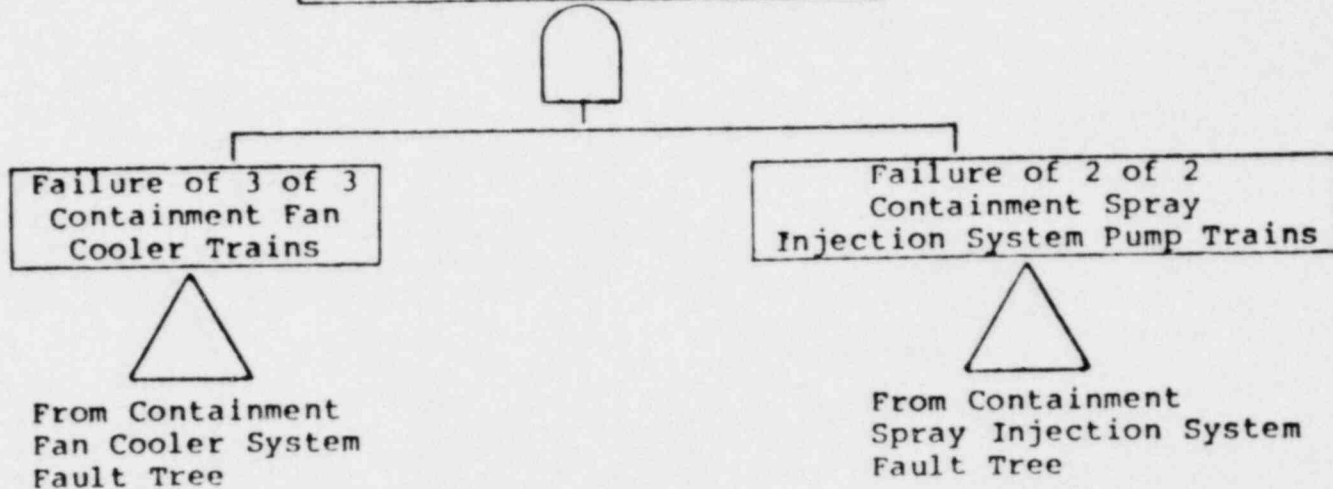
4.0 Display of Dominant Accident Sequences

4.1 Discussion

The functional and systemic event tree methodology discussed thus far provides a consistent approach for modeling the accident sequences for all the IREP plants. These trees will be used as an integral part of the procedure used in assessing the dominant accident sequences.

Based on the event heading failure definitions discussed in the previous sections, fault trees will be developed to determine the various failure modes which can cause the function and system event heading failure. As a general case, the function and system events are not independent (e.g., due to subsystems and components which are common to more than one event tree function or front line system). Because of this, a complement of the event heading fault tree must be created to determine the success modes which can cause event heading success. Each sequence will be quantified by combining and Boolean reduction of the initiating event fault tree and the functional or systemic fault trees and "success trees" associated with each sequence. The result of this procedure will be separate cut set equations representing the minimum combination of system and/or component failures which will cause the occurrence of each functional or systemic accident sequence. (This procedure is discussed in detail in the paper entitled "Accident Sequence Quantification.") The sequence cut sets will then be quantified by assigning the appropriate failure probabilities to the cut set literals (e.g., a cut set such as AB has two literals) and the dominant cut sets in each accident sequence will be identified.

Containment Overpressure
During Injection Phase
Fails Following a Small LOCA



- Notes: 1) Fan cooler system will start automatically, but is manually shutdown after containment pressure is reduced below 4 psig. Any restart would have to be done manually (Emergency Procedure XYZ).
- 2) Containment spray system must be manually started since manual shutdown of the fan cooler system deactivates automatic start circuitry.

Figure 5 Top level fault tree for the containment overpressure protection function in response to a small LOCA. The plant depicted in this example performs this function with either 1 of 2 containment spray trains or 1 of 3 containment fan cooler trains.

Besides its usefulness as a tool as part of the sequence quantification procedure, event trees are also useful ~~for~~ displaying tools in showing important interdependencies between the systems and system components required to respond to an initiating event. The functional event trees discussed in Sections 1.1.1 and 1.1.2 hide many of these interdependencies, since several systems and system components are generally a part of the definition of a single functional event tree heading. The systemic event trees discussed in Section 1.1.3 display interdependencies between the front line plant systems but hide the effects of support systems which are common to more than one front line system. It would be desirable, to construct an event tree which explicitly displays these type of interdependencies.

Such an event tree could be constructed based on information contained within the list of dominant functional accident sequence cut sets. After careful examination of the dominant cut sets, it will become apparent which systems, support systems, or system components are the most important. These would be designated as the event tree headings and the dependencies between them incorporated into the event tree structure. The resulting event tree would provide an excellent means of summarizing and displaying the most important accident sequences in terms of the critical systems, subsystems, and system components.

(An alternate method of displaying the most important accident sequences is to use a system dependency diagram. Examples of these types of diagrams can be found in the main body of the Crystal River risk analysis.)

4.2 Procedure

Procedure for Display of Dominant Accident Sequences

1. Identify dominant cut sets for each functional or systemic accident sequence.
2. Examine the literals of the dominant cut sets to determine what are the systems and/or components which have failed.
3. If the literal is a component, identify the system(s) it is a part of.
4. Create a system/system component event tree by making the important systems/components the tree headings, and incorporating into the event tree structure, dependencies between them.

5.0 Accident Process Analysis of Event Tree Core Meltdown Sequences

5.1 Discussion

After the quantification of the event tree core melt accident sequences is completed, those with the highest probability will be analyzed in terms of core meltdown accident processes. The output of this analysis will be an assessment of the appropriate containment failure modes, containment failure mode probability and radioactive material release category placement for each of these sequences. This will be done primarily by comparing these accident sequences with similar sequences which were generated as part of the RSS and RSSMAP programs.

For each plant studied in IREP, an assessment of which of the six plants studied in the RSS and RSSMAP most closely resembles the study plant, in terms of system and containment design features, will be made. After this assessment, the accident sequences for the two plants will be compared and sequences with the identical combination of succeeded and failed functions will be identified. Once this identification has been made, the appropriate containment failure modes, containment failure mode probabilities, and release category placement for the IREP plant accident sequence will also be identified.

The results of the core meltdown accident process analysis for the Oconee LOCA and transient accident sequences is given in Tables 3 and 4. The containment failure modes which apply to the Oconee reactor are defined by the containment event tree depicted in Figure 6. Similar tables of results and containment event trees will be provided for the remaining RSS and RSSMAP plants (Surry, Peach Bottom, Sequoyah, Calvert Cliffs, Grand Gulf) at a later date.

Several notes are in order concerning the use of Tables 3 and 4. Firstly, the β containment failure mode probability must be supplied by the IREP team since its value is a function of the containment isolation system design for the particular IREP plant. Secondly, transient accident sequences involving a stuck open pressurizer relief valve (e.g. sequences 3 and 13 in Figure 4) should be treated as a LOCA with a size corresponding to the valve discharge area. Whether or not the main or auxiliary

TABLE 3

Summary of the LOCA Initiated Core Melt-down Accident Process Analysis for the Oconee Plant

LOCA EVENT TREE FAILED FUNCTIONS		LOCA SIZE			CORE MELT RELEASE CATEGORY								
MRI	COI	ECI	RRP	COR	ECR	CHR	1	2	3	4	5	6	7
X				X			D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2		β β		ε.5 ε.8
	X			X			D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
		X			X		D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
X	X	X		X			D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
		X	X		X		D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
			X		X		D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
X				X			D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
X	X	X		X			D ≤ 2" D > 2"	a.0001 a.01	γ.5 γ.2	β β		ε.5 ε.8	
X	X	X	X	X	X		D ≤ 2" D > 2"	a.0001 a.0001	γ.5 γ.5	β β		ε.5 ε.5	
X	X	X	X	X	X		D ≤ 2" D > 2"	a.0001 a.0001	γ.5 γ.5	β β		ε.5 ε.5	
X	X	X	X	X	X		D ≤ 2" D > 2"	a.0001 a.0001	γ.5 γ.5	β β		ε.5 ε.5	

Inter-facing System LOCA V

TABLE 4

Summary of the Transient Initiated Core Meltdown
Accident Process Analysis for the Oconee Plant

TRANSIENT EVENT TREE FAILED FUNCTIONS					CORE MELT RELEASE CATEGORY						
RS	CC	RCSOP	CO	RR	1	2	3	4	5	6	7
	X				$\alpha.0001$		$\gamma.5$		β		$\epsilon.5$
	X			X	$\alpha.0001$	$\gamma.5$			β		$\epsilon.5$
	X		X	X	$\alpha.0001$	$\delta.5$		β		$\epsilon.5$	
	X	X			$\alpha.0001$		$\gamma.5$		β		$\epsilon.5$
X	X				$\alpha.0001$		$\gamma.5$		β		$\epsilon.5$

CONTAINMENT RUPTURE DUE TO VESSEL STEAM EXPLOSION α	CONTAINMENT LEAKAGE β	CONTAINMENT RUPTURE DUE TO HYDROGEN BURNING γ	CONTAINMENT RUPTURE BY OVERPRESSUR- IZATION δ	CONTAINMENT FAILURE BY BASE MAT MELTTHROUGH ϵ
--	-----------------------------------	--	--	--

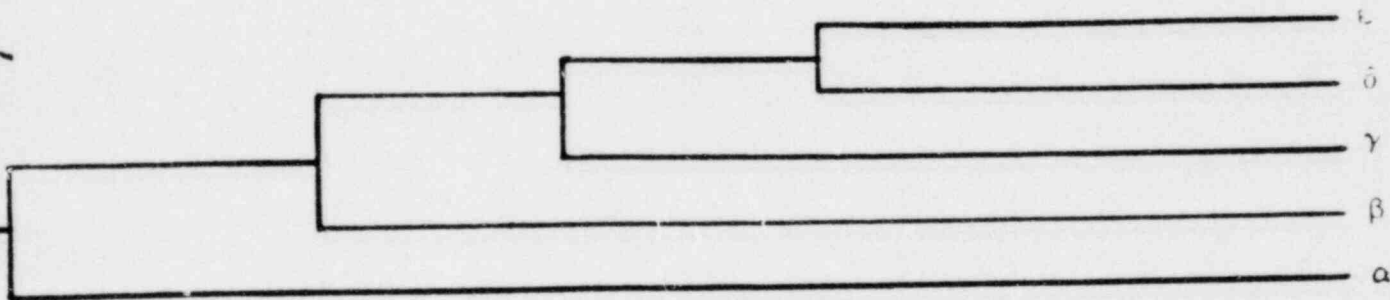


FIGURE 6. OCONEE CONTAINMENT EVENT TREE

feedwater systems are operating in these sequences can be ignored, since they do not significantly affect the core meltdown accident processes. And finally, analysis of the IREP plant may yield important accident sequences which do not correspond to any of the exact combinations of failed functions presented in Tables 3 and 4. If this occurs Sandia National Laboratory personnel should be notified to determine if additional accident processes analysis of these sequences is required.

5.2 Procedure for Accident Process Analysis of Event Tree Core Meltdown Sequences

1. Compare the IREP plant design with the plant designs studied in the RSS and RSSMAP. This should include comparisons of:
 - a. containment designs (e.g., volume, design pressure, structural design, degree of compartmentalization, potential for water entrapment underneath reactor vessel, etc.).
 - b. ESF system designs (e.g., types of systems which perform the event tree functions, flow rates, heat removal rates, actuation setpoints, etc.)
2. Based on this comparison, identify which RSS or RSSMAP plant most closely resembles the IREP plant.
3. Compare accident sequences and identify those with the identical combination of failed functions.
4. Sequences with an identical combination of failed functions should have similar containment failure modes, containment failure mode probabilities and radioactive release category placements.

Appendix 1
PWR Transients

PWR Transient Category Definitions

1. Loss of RCS Flow (1 Loop)

This transient occurs when an inadvertent hardware or human error interrupts the flow in one loop of the reactor coolant system.

2. Uncontrolled Rod Withdrawal

This transient occurs when one or more control rods are withdrawn inadvertently.

3. CRDM Problems and/or Rod Drop

This transient occurs when failures in the control rod drive mechanism (CRDM) occur which lead to out-of-tolerance conditions in the primary system. The transient may include dropping of one or more control rods into the core as part of the CRDM failure.

4. Leakage From Control Rods

This transient occurs when primary system leakage around the control rod drive mechanism is excessive and reactor shutdown required.

5. Leakage in Primary System

This transient occurs when primary system leakage through various piping components is excessive and reactor shutdown required. This transient does not include:

- #4 - Leakage from control rods
- #7 - Pressurizer leakage
- #26 - Steam generator leakage

6. High or Low Pressurizer Pressure

This transient occurs when the pressurizer pressure is outside of the required operating limits.

7. Pressurizer Leakage

This transient occurs when pressurizer components allow excessive primary system leakage and reactor shutdown is required.

8. Pressurizer Relief or Safety Valve Opening

This transient occurs when hardware or operator error results in inadvertent opening of pressurizer relief or safety valves.

9. Inadvertent Safety Injection Signal

This transient occurs when hardware or operator error initiates a safety injection.

10. Containment Pressure Problems

This transient occurs when hardware or operator error results in containment pressure exceeding limits.

11. CVCS Malfunction-Boron Dilution

This transient occurs when hardware or operator error results in a CVCS malfunction such that reactor power is affected.

12. Pressure, Temperature, Power Imbalance

This transient occurs when various primary systems signals indicate pressure, temperature or power imbalances.

13. Startup of Inactive Coolant Pump

This transient occurs when an idle coolant pump is started at an improper power and flow condition.

14. Total Loss of RCS Flow

This transient occurs when a hardware or operator error causes a loss of reactor coolant system flow.

15. Loss or Reduction in Feedwater Flow (1 Loop)

This transient occurs when one feedwater pump trips or when another occurrence results in an overall decrease in feedwater flow.

16. Total Loss of Feedwater Flow (All Loops)

This transient occurs when a simultaneous loss of all main feedwater occurs, excluding that due to loss of station power (definition #35).

17. Full or Partial Closure of MSIV (1 Loop)

This transient occurs when one main steam isolation valve (MSIV) closes, the rest remaining open, or the partial closure of one or more MSIV occurs.

18. Closure of All MSIV

This transient occurs when any one of various steam line or nuclear system malfunctions requires termination of steam flow from the vessel, or by operator action. The closure of one MSIV may cause an immediate closure of all other MSIVs; this occurrence is also included in this transient definition. However, any closure which is the by-product of another initiator is not included.

19. Increase in Feedwater Flow (1 Loop)

This transient occurs when an increase in feedwater flow occurs in one loop.

20. Increase in Feedwater Flow (All Loops)

This transient occurs when an increase in feedwater flow occurs in more than one loop.

21. Feedwater Flow Instability-Operator Error

This transient occurs when feedwater is being controlled manually, usually during startup or shutdown, and excessive or insufficient feedwater flow occurs.

22. Feedwater Flow Instability-Miscellaneous Mechanical Causes

This transient occurs when excessive or insufficient feedwater flow results from hardware failures in the feedwater system.

23. Loss of Condensate Pumps (1 Loop)

This transient occurs when one condensate pump fails, reducing feedwater flow.

24. Loss of Condensate Pumps (All Loops)

This transient occurs when all condensate pumps fail, causing a loss of feedwater flow.

25. Loss of Condenser Vacuum

This transient occurs when either a complete loss or decrease in condenser vacuum results from a hardware or human error.

26. Steam Generator Leakage

This transient occurs when excessive primary system to secondary leakage occurs in the steam generator.

27. Condensor Leakage

This transient occurs when excessive secondary system leakage occurs in the condenser.

28. Miscellaneous Leakage in Secondary System

This transient occurs when excessive leakage occurs in the secondary system, other than the condenser (see definition #27).

29. Sudden Opening of Steam Relief Valves

This transient occurs when a secondary system steam relief valve opens inadvertently, causing an unacceptably low pressure in the secondary system.

30. Loss of Circulating Water

This transient occurs when circulating water is not available to the plant.

31. Loss of Component Cooling

This transient occurs when excessive temperature of critical components is a result of a loss or decrease in component cooling water flow.

32. Loss of Service Water System

This transient occurs when the service water system fails to perform its function.

33. Turbine Trip, Throttle Valve Closure, EHC Problems

This transient occurs when a turbine trip occurs, or if turbine problems occur which in effect decrease steam flow to the turbine, causing a rapid change in the amount of energy removed from the primary system.

34. Generator Trip or Generator Caused Faults

This transient occurs when the generator is tripped due to electrical grid disturbances or generator faults.

35. Loss of Station Power

This transient occurs when all power to the plant from external sources (the grid or a dedicated transmission line to another plant) is lost.

36. Loss of Power to Necessary Plant Systems

This transient occurs when power is lost to a component or group of components such that plant shutdown is necessary. It does not include loss of power to those components whose failure causes another defined transient to occur.

37. Spurious Auto Trip-No Transient Condition

This transient occurs when an auto scram is initiated by a hardware failure in instrumentation or logic circuits and no out-of-tolerance condition exists.

38. Auto/Manual Trip Due to Operator Error

This transient occurs when an auto scram or manual scram is initiated by human error and no out-of-tolerance condition exists.

39. Manual Trip Due to False Signals

This transient occurs when an operator initiates a scram based on information from erroneous instrumentation.

40. Spurious Trips-Cause Unknown

This transient occurs when a scram occurs and no out-of-tolerance condition can be detected, nor cause of scram determined.

41. Fire Within Plant

This transient occurs when a plant shutdown is necessitated by a fire in some part of the plant.

BWR Transients

BWR Transient Category Definitions

1. Electric Load Rejection

The electric load rejection transient occurs when electrical grid disturbances result in significant loss of load on the generator. Also included are intentional generator trips.

2. Electric Load Rejection with Turbine Bypass Valve Failure

The transient is identical to #1 except that the turbine bypass valves do not open simultaneously with shutdown of the turbine.

3. Turbine Trip

A turbine trip transient occurs when any one of a number of turbine or nuclear system malfunctions requires the turbine be shut down.

Turbine trips which occur as a byproduct of other transients such as loss of condenser vacuum or reactor high level trip are not included. Intentional turbine trips are also included.

4. Turbine Trip with Turbine Bypass Valve Failure

This transient is identical to #3 except that the turbine bypass fail to open.

5. Main Steam Isolation Valve (MSIV) Closure

The MSIV closure transient occurs when any one of various steam line and nuclear system malfunctions requires termination of steam flow from the vessel, or by operator action.

6. Inadvertent Closure of One MSIV

This transient occurs when only one MSIV closes, the rest remaining open, due to operator or equipment error.

7. Partial MSIV Closure

This transient occurs when partial closure of one or more main steam isolation valves results from a hardware or human error.

8. Loss of Normal Condenser Vacuum

This transient occurs when either a complete loss or decrease in condenser vacuum results from a hardware or human error.

9. Pressure Regulator Fails Open

This transient occurs when either the controlling pressure regulator or backup regulator fails in an open direction. The failure causes a decreasing coolant inventory as the mass flow of water entering the vessel decreases.

10. Pressure Regulator Fails Closed

This transient occurs when either the controlling pressure regulator or backup regulator fails in a closed direction. This failure causes increasing pressure and thus decreasing steam flow from the vessel.

11. Inadvertent Opening of a Safety/Relief Valve (Stuck)

This transient occurs when a safety/relief valve sticks open. Due to an operator or equipment error a single safety/relief valve can be opened, increasing steam flow from the vessel. If the valve cannot be closed, a scram is initiated. This transient only includes those openings which cannot be subsequently closed before a scram occurs.

12. Turbine Bypass Fails Open

The transient occurs when equipment or operator error results in inadvertent or excessive opening of turbine bypass valves so as to decrease vessel level.

13. Turbine Bypass or Control Valves Cause Increase Pressure (Closed)

This transient occurs when either operator error or equipment failure causes the turbine bypass or control valves to close, resulting in increased system pressure.

14. Recirculation Control Failure-Increasing Flow

This transient occurs when a failure of a flow controller, either in one loop or the master flow controller, causes an increasing flow in the core.

15. Recirculation Control Failure-Decreasing Flow

This transient occurs when any flow controller failure causes a decreased flow to the core.

16. Trip of One Recirculation Pump

This transient occurs when one recirculator pump trips due to a hardware or human error.

17. Trip of All Recirculation Pumps

This transient occurs when the simultaneous loss of all recirculation pumps occur.

18. Abnormal Startup of Idle Recirculation Pump

This transient occurs when an idle recirculation pump is started at an improper power and flow condition. The increased flow could cause a flux spike, or, if the loop has been idle so as to allow coolant in the pump loop to cool, core inlet subcooling.

19. Recirculation Pump Seizure

This transient occurs when the failure of a recirculation pump is such that no coast down occurs, and a sudden flow decrease is experienced.

20. Feedwater-Increasing Flow at Power

This transient occurs when any event causes increasing feedwater flow at power. Excluded (see item 26) are increasing flow events during startup or shutdown, when manual feedwater control is being utilized.

21. Loss of Feedwater Heater

This transient occurs when the loss of feedwater heating is such that the reactor vessel receives feedwater cool enough to exceed core scram parameters.

22. Loss of All Feedwater Flow

This transient occurs when the simultaneous loss of all main feedwater flow, excluding that due to loss of station power (see item 31), occurs.

23. Trip of One Feedwater Pump (or condensate pump)

This transient occurs when the loss of one feedwater pump or condensate pump is such that a partial loss of feedwater is experienced.

24. Feedwater-Low Flow

This transient occurs when any plant occurrence causes decreasing feedwater flow at power. Excluded are events at low power (see item 25).

25. Low Feedwater Flow During Startup or Shutdown

This transient occurs when any event results in low feedwater flow at essentially zero power; this definition includes only startup or shutdown operations.

26. High Feedwater Flow During Startup or Shutdown

This transient occurs when excessive feedwater flow occurs during startup or shutdown. The reactor is essentially at zero power.

27. Rod Withdrawal at Power

This transient occurs when one or more rods are withdrawn inadvertently in the power range of plant operation.

28. High Flux Due to Rod Withdrawal At Startup

This transient occurs when inadvertent withdrawal of a rod causes a local power increase.

29. Inadvertent Insertion of Rod or Rods

This transient occurs when any malfunction causes an inadvertent insertion of rod or rods during power operation.

30. Detected Fault in Reactor Protection System

This transient occurs when a scram is initiated due to an indicated fault in the reactor protection system. An example is the indication of a high level in the scram discharge volume.

31. Loss of Offsite Power

This transient occurs when all power to the plant from external sources (the grid or dedicated transmission lines to another plant) is lost. This event requires the plant emergency power sources to be available.

32. Loss of Auxiliary Power (Loss of Auxiliary Transformer)

This transient occurs when the loss of incoming power to a plant results from onsite failures such as the loss of an auxiliary transformer.

33. Inadvertent Startup of HPCI/HPCS Water Flow

This transient occurs when any of the systems supplying high pressure cold water to the vessel inadvertently start up.

34. Scram Due to Plant Occurrences

This transient occurs when a scram, either automatic or manual, is initiated by an occurrence which does not cause an out of tolerance condition in the primary system, but requires shut-down. Examples are turbine vibration, off-gas explosion, fire, excess conductivity of reactor coolant, etc.

35. Spurious Trip Via Instrumentation, RPS Fault

This transient occurs when a scram results from hardware failure or human error in instrumentation or logic circuits occurs.

36. Manual Scram-No Out-of-Tolerance Condition

This transient occurs when a manual initiation of a scram, either purposely or by error, occurs and there are no out-of-tolerance conditions.

37. Cause Unknown

This transient occurs when a scram occurs, but the cause was not determinable.



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

#21

Docket No. 50-313

August 15, 1980

Mr. William Cavanaugh, III
Vice President, Generation and
Construction
Arkansas Power and Light Company
P.O. Box 551
Little Rock, Arkansas 72203

Dear Mr. Cavanaugh:

Subject: IREP Schedule

At our meeting on August 4 we promised to send you an outline of the IREP schedule for the first 5 months annotated to highlight the skills and knowledge that could best be provided by your representative(s) on the IREP team. The anticipated start date is September 15, 1980. The following discussion refers to the IREP Procedure and Schedule Guide, Enclosure 1 to my letter of July 25, 1980.

First 2 weeks - First cut at tasks 1-5, late September. The team will be familiarizing itself with the plant documentation and performing the first few tasks in the IREP Procedure and Schedule Guide. We anticipate a number of document requests to be made from the procedure index or diagram index. Someone thoroughly familiar with the plant design and operations documentation would help the team to be selective and to request the appropriate documents.

Third through eighth week - First cut at tasks 6-17, October and early November. The team will be classifying initiating events, developing the catalogs of accident scenarios in broad outline (event tree analysis), defining system success vs. failure criteria, and tracing the possible causes of the initiating events to faults in the support systems which also serve the required mitigating systems. During this phase, the assistance of an individual who has a broad understanding of accident processes, systems design, and operation would be particularly valuable. We have not requested the voluminous plant design documentation on power generation equipment that may prove to be necessary to perform the fault tree analyses of transient initiators and non-passive failure LOCAs. Therefore, we will probably assign to the more knowledgeable owner's representative the lead responsibility for the development of the fault trees for the initiating events. He will also be expected to participate in each of the other tasks: event tree analysis, definition of the system success vs. failure criteria, etc.

Dupe of 8409020322

Ninth through sixteenth week - First cut at tasks 18-27, late November through January. This phase of the study will focus on fleshing out the reliability-predictive models of the systems (fault tree analysis). The visit to the plant by the team will occur late in the prior phase or early in this phase. We anticipate that the early work in this phase will concentrate on the relatively straight-forward front line engineered safety features. In the later phase the work will move to the modeling of the network of support systems. We expect a progressively growing need for owner's representative assistance to the team within this interval in the contexts of (1) surveillance and maintenance practices, (2) operating and emergency procedures, and (3) control and instrumentation.

Sixteenth through twentieth week - First cut at tasks 28-35, February. The initial screening of accident scenarios according to likelihood and the search for not-yet-identified common cause failure modes will take place in this interval. Particularly useful knowledge and skills in your representatives will be in the areas of possible operator corrective action in the face of multiple failures, control and instrumentation, and procedures.

In this and successive phases the team will be refining their models of the potentially dominant accident scenarios. The questions the team will need to ask of your personnel will be more sharply focused. The physical presence on the team of the more knowledgeable and valuable personnel will be less important than in the formative second phase (weeks 2-8). You will, however, want to keep your more senior people in engineering and operations apprised of the emerging picture of the dominant accident sequences. You may want to intersperse the occasional management briefings with more frequent technical briefings during the last few months of the program.

From our point of view, we would prefer as much continuity, knowledge, and skill as we can get in your participants. We do understand, though, that your better people are in great demand. If I were in your shoes and could manage it, I would assign a junior systems and licensing engineer or systems reliability engineer to stay with the IREP team throughout. He or she would be in it for the experience, for liaison, and to take a prominent role in the digestion and use of the results at the conclusion of the IREP study. He or she might be earmarked to exercise and keep the IREP models updated after the NRC study is complete, as Florida Power Corporation is planning to do. I would select that person for imagination, sound abstract thinking or broad overview, and at least a passing familiarity with mechanical, electrical and control systems engineering. That person should also have the facility with mathematics to rapidly learn probabilistic system reliability analysis while on the team. In addition to this continuous presence on the IREP team, I would assign a couple of others for temporary assignment to IREP. I would pick the most knowledgeable individual I could pry loose in plant operations and engineering for the 6 week second phase period

in October and November (event trees, system success criteria, and the analysis of initiating events). I would try to earmark 1 day per week of this same person's time from February through the conclusion of the study - while he or she remains at their normal post - to review the convergence on results. A third person, chosen for familiarity with control and instrumentation, maintenance procedures and emergency procedures would be detailed to IREP in January and February (late in the system reliability modeling phase and the subsequent probabilistic evaluations) to assure that the modeling of the network of support systems is done correctly, to participate in the evaluation of equipment unavailability due to test and maintenance, and to assist in modeling the possibilities for operator corrective action during accidents. That person, too, I would assign to part time review of IREP results after their return to normal assignment in March. To make sure that person can get up to speed promptly when he or she joins the team in January, that person should have attended - as a minimum - an engineering short course in probabilistic system reliability analysis or fault tree analysis.

This representation, one person full time and two more highly-qualified people for 6 week assignments should meet our mutual need to assure that the models produced in IREP fairly portray your plant and offer your people considerable experience in probabilistic safety analysis without unduly burdening your already hard pressed staff, or so we believe. I hope that this helps you in your planning for IREP participation.

Sincerely,

Original signed by
Darrell G. Eisenhut

Darrell C. Eisenhut, Director
Division of Licensing
Office of Nuclear Reactor Regulation

cc: See Attached List

bcc: Docket File
NRC Public Document Room
G. Vissing
R. Mattson
M. Ernst
S. Israel
F. Rowsome ←
J. Murphy
R. Bernero

Arkansas Power & Light Company

cc:

Mr. David C. Trimble
Manager, Licensing
Arkansas Power & Light Company
P. O. Box 551
Little Rock, Arkansas 72203

Mr. James P. O'Hanlon
General Manager
Arkansas Nuclear One
P. O. Box 608
Russellville, Arkansas 72801

Mr. William Johnson
U. S. Nuclear Regulatory Commission
P. O. Box 2090
Russellville, Arkansas 72801

Mr. Robert B. Borsum
Babcock & Wilcox
Nuclear Power Generation Division
Suite 420, 7735 Old Georgetown Road
Bethesda, Maryland 20014

Mr. Nick Reynolds
DeBevoise & Liberman
1200 17th Street, NW
Washington, D.C. 20036

Arkansas Polytechnic College
Russellville, Arkansas 72801

Director, Bureau of Environmental
Health Services
4815 West Markham Street
Little Rock, Arkansas 72201

Mr. Paul F. Levy, Director
Arkansas Department of Energy
3000 Kavanaugh
Little Rock, Arkansas 72205

Mr. William T. Craddock, Mgr.
Availability Engineering
First National Bank Building
P. O. Box 551, Seventh Floor
Little Rock, Arkansas 72203

Mr. Robert Szalay, Licensing and
Safety Project Manager
Atomic Industrial Forum
7101 Wisconsin Avenue
Washington, DC 20014

Mr. E. P. O'Donnell
Ebasco Services, Inc.
89th Floor
2 World Trade Center
New York, NY 10048

Dr. Edwin Zebroski
Nuclear Safety Analysis Center
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94303

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

JUL 25 1980

Docket No. 50-313

Mr. William Cavanaugh, III
Vice President, Generation and
Construction
Arkansas Power and Light Company
P.O. Box 551
Little Rock, Arkansas 72203

Dear Mr. Cavanaugh:

Subject: Interim Reliability Evaluation Program (IREP) - Phase II

The concerns about the IREP program expressed at our meeting of June 12, 1980 and letters we have received since, have prompted us to share with you more of the details of the IREP program plan and the technical guidance for conduct of IREP studies. We may have left you with the impression that the methods and procedures will be made up as the studies progress. This is not the case. As the enclosures demonstrate, the broad outlines of methods and procedures are well established. What remains to be done is to fine-tune some of the instructions to the teams to assure a standardized quality product with reasonable opportunities for management oversight and redirection.

Enclosed are (1) the current draft of the IREP Procedures and Schedule Guide*, (2) the draft IREP Event Tree Guide, and (3) a draft guide for selecting component failure rates. We expect that these items will be refined and edited in the coming weeks. It is our intention to base their revision on the comments of the Probabilistic Analysis Staff and its IREP contractor, Sandia National Laboratories. We do not expect substantial alterations to the technical approach. However, we and Sandia are taking special care to select the intermediate milestones for documentation and review. We both hope to ensure high and consistent quality, but at the same time avoid the dissipation of resources on premature status reports and their evaluation. The enclosed Procedure and Schedule Guide represents what we consider the strictest approach to both procedure and schedule. We are presently considering substantial relaxation of both aspects.

*Some have taken to calling this procedural guide a cookbook. We dislike the term "cookbook" since it implies a well established recipe for something. We do not have a well established recipe for performing an interim reliability evaluation of a plant but are trying to develop one.

Many of the licensee's concerns with IREP Phase II have been enumerated in a letter from Arthur Lundvall of Baltimore Gas and Electric Company (BG&E) to NRC dated June 25, 1980. This letter, too, is enclosed for ease of reference (Enclosure 4). We think Mr. Lundvall's concerns warrant a detailed reply, not just to BG&E but the other owners of IREP II plants as well. The concerns are generic. TVA has sent us a letter expressing similar concerns. Arkansas Power and Light has conditionally agreed to proceed with the IREP program but has also expressed these concerns.

1. Schedule

We are more concerned with promptly initiating the IREP Phase II studies than we are with rushing to judgment on the results. Just as we are proceeding with deliberation on the completion of the Phase I study of Crystal River, we are fully prepared to modify the schedule on the completion of a Phase II study if that is necessary to perform an adequate job.

Our sense of urgency on the inception of the Phase II studies is based upon a perception in both RES and NRR at NRC that it is desirable to survey all operating reactors in IREP-like studies as soon as practically possible. This work is covered in the Task Action Plan (NUREG-0660) as Tasks II.C.1 and II.C.2. The Phase II IREP studies will serve, among other objectives, as a proving ground for a study scope and task description that can be followed on all plants with the resources the NRC and the industry might realistically be able to provide within the next few years. The objective is to distill the essence of risk assessment to a level that would permit a plant to be studied in less than a year by a team composed of two experienced system reliability analysts, one engineer thoroughly versed in the design and operation of the plant; and three reactor systems engineers of the background commonly found in utilities, vendors, or architect-engineer staffs. These teams are to generate a standardized and meaningful product, albeit one that is not so complete as one entailing, say, thirty man years effort per plant.

NRC plans to prepare the procedural guide (perhaps in collaboration with the industry) drawing upon the Phase II experience and NRC will request, sometime in 1981, that these studies be started on operating plants. Roger Mattson has suggested a forum for industry input on the procedural guide, to which I will turn later.

It is with this background that we feel a sense of urgency to get on with the inception of the Phase II studies. It is also responsible for the impression we gave that the "cookbook" is still developing; we intend to be working on the Phase III procedural guide throughout Phase II, drawing upon the Phase II experience.

2. Methodology

We feel that the state-of-the-art in probabilistic risk assessment is quite well-developed through many applications, refinements, and peer review. There are many shortcomings in the completeness and precision of available techniques but the time is ripe to divert some of our research resources from the advancement of the frontiers of risk assessment to the broad scale application of the well-developed portions of the discipline. Our principal problem in this context is to distill the essence of the techniques that are well known to the community of experienced practitioners into a form that can be usefully implemented by many small teams of less specialized analysts throughout the industry in a comparatively short period of time. We are targeting a plant-specific catalog of core melt accidents that is abstract enough to be fairly complete yet specific enough to be useful in risk assessment, operator training, emergency planning, and the like. The state-of-the-art in event tree analysis can support this. In addition, we are aiming for the performance of system reliability analysis and common-cause failure analysis - including operator error - of sufficient depth to give fairly good odds that the risk-dominant accident sequences will be identified. In particular, we want to screen the subject plants for susceptibility to those accidents in which common factors couple the initiating event with the degradation of the reliability of the systems expected to mitigate the event, e.g., scenarios like TMI or the NNI-bus faults at Rancho Seco and Crystal River.

The task of preparing the instructions for such studies requires input from experts in risk assessment and the experience of the Phase II studies. We welcome industry input to the Phase III instructions developed in parallel with the Phase II effort. However, it would unnecessarily delay the program to schedule the industry input to Phase II and thereby substantially delay the conduct of this phase.

3. Timing vs. Plant Alterations

It is not a problem to incorporate in IREP studies design or procedural alterations that are well-planned but not yet implemented. For example, the Crystal River Unit 3 study credited alterations to the Emergency Feedwater System that were just evolving from conceptual to detailed design as the study was in progress. For those cases in which a conceptualized change is not yet well enough elaborated for modeling in a system reliability analysis, it is feasible to perform sensitivity studies which could give useful input to detailed design or procedural implementation. Therefore, we see as many or more advantages as disadvantages in performing IREP studies while the TMI modifications are in the pipeline.

4. Licensee Participation

As you can see, the IREP Procedure and Schedule Guide provides for a number of points at which preliminary results and working papers are submitted to the plant owner as well as the NRC Research and Sandia IREP program management for review and comment. There will be ample opportunity for the owners' engineering and operations personnel to keep posted on the developing study. We welcome your suggestions for improvements in the structure of this oversight. We intend to provide periodic briefings of NRC and licensee management on the progress of the IREP reviews. At these times, if you have any basic problems with the conduct of the studies, you will have ample opportunity to voice your concerns.

We would welcome the membership on the IREP study teams of one to three engineers drawn from and supported by yourselves (the owner) or your consultants. We think it would be more valuable to you as well as to the team effort if your participants on the IREP team are drawn from your engineering or operations staffs. An individual thoroughly familiar with the design and operation of the plant would be the most useful to the study team. One who knows to whom to route technical design or operations questions would enhance the speed and accuracy of the IREP effort. Such an individual would be particularly well suited to maximize the benefit of the experience for yourselves as well. That person would be equipped to translate the engineering insights that will be implicit in the study into useful guidance for your conduct of operations, maintenance, personnel training and the evaluation of retrofit options. The experience would enhance the participant's usefulness in economic risk management, availability engineering, and in dealing with subsequent regulatory issues as well. That person need not have prior experience with risk assessment or system reliability analysis - an alert individual can learn much of that through the IREP experience. Such team members detailed to IREP from your staff will be free to keep you posted of the team's activities as you see fit even outside the framework of scheduled IREP reporting. You may also want to employ the services of a competent risk assessment engineer to help in your review of the preliminary reports and the subsequent draft report. While we would be happy to accept such a consultant as a detailee to the IREP team, we would prefer members of your own staff.

NRC is paying for these IREP studies. We and our contractors will provide working space for participants sent by the owner. Salary, travel and subsistence costs for the owner's representatives are the responsibility of the plant owner. From time to time in the IREP study there may arise technical questions about plant response which may not be answerable from existing records. These questions will be directed to the owner for response. Any costs of special

analysis by the owner or support by contractors to the owner are the responsibility of the plant owner. We do not expect to encounter a large number of such questions or any which require extensive special analysis. Our experience in the Crystal River IREP supports this expectation.

5. Regulatory Ratcheting

The controversy surrounding the Reactor Safety Study, the many reviews and criticisms of it, and the culmination of that controversy in the Lewis Committee Report is fresh in our minds. We are very conscious that careless use of probabilistic risk analysis can lead to incorrect understanding and action. At the same time we and many others are convinced that probabilistic risk analysis is a tool which can make substantial contributions to nuclear safety. Certainly, if we had all heeded the message of the Reactor Safety Study, we would have focused our attentions on transients, small breaks, and operator error years ago. Perhaps the TMI accident would have been prevented if we had.

As you know, many groups have undertaken probabilistic risk analyses now and we must address what to do with the results. It is not enough to say that the results of such an analysis should be carefully reviewed and considered. Such analyses, if carefully done, can reveal the Achilles heel of the plant and give a fair measure of how vulnerable the plant is to serious accidents. We need a consistent way to decide whether to backfit the plant to reduce either the likelihood or the consequences of the accidents which dominate the risk. Owners and the NRC need to look at the results of these analyses, considering their quality and their uncertainties, and decide what changes, if any, are warranted. In virtually every case I would expect the owner of the plant to factor the results of these analyses into the plant's procedure reviews and operator training. In many cases I would expect the analyses to identify areas where minor changes in testing, maintenance, or hardware would substantially reduce risk; and in other cases, analyses will point to design features of the plant which are not easy to change. The owner's voice should be the first heard on what changes are warranted, but I realize that many owners are concerned that NRC will press ahead with ratcheting decisions before the owner is heard. The best way to avoid this is for the owner to follow the analysis closely, evaluate the significance of findings as they develop, and take the lead in identifying what actions are appropriate.

A larger forum has been proposed for joint industry and NRC consideration of probabilistic risk analysis methods and their use in regulation. The NRC and the Institute of Electrical and Electronic Engineers (IEEE) held a joint technology transfer conference here in Washington in January of this year. The first proposal for followup action

made by the steering committee of that conference was to encourage industry and NRC consideration of probabilistic risk analysis methods and uses in a structured technical forum. This idea led to a meeting at the IEEE on May 15, 1980 where Roger Mattson of the NRC proposed NRC/industry collaboration on the procedures and policies to govern the extension of IREP to all the operating nuclear plants. A copy of the minutes of that meeting is enclosed as Enclosure 5. He suggested that this initiative be hosted by the IEEE as a neutral technical (and public) forum with unique connections to related areas of expertise. He suggested that two committees be formed. One of these would be a steering committee composed of managers to deal with issues such as objectives, schedules and resource constraints, and consideration of the form and quality of IREP results for ultimate use in regulation. The second would be a working group of experts in risk assessment to work up the scope, procedures, and assumptions for the accomplishment of IREP Phase III or the "National Reliability Evaluation Program," NREP, as Roger calls it. In addition to the host role, the IEEE would obtain periodic input to the two committees from its resources in non-nuclear industries that have extensive experience in system reliability analysis and reliability assurance.

There was another meeting on June 11, 1980. Nuclear industry representatives at the meeting were Walt Fee of Northeast Utilities, Bob Szalay of the Atomic Industrial Forum, and Ed O'Donnell of Ebasco Services who is chairman of the AIF Ad Hoc Committee on Probabilistic Safety Analysis. The AIF Ad Hoc Committee has since met and we expect to meet with them again here in Washington on August 5.

I believe that I have addressed the three recommendations with which Mr. Lundvall's letter closes but, to summarize:

- a. Licensee Input on Methodology and Assumptions. There will be ample opportunity for licensee input on the way the plant is modeled: system success criteria, points of no return, accident phenomenology, and the modeling of system behavior. The teams will be under instructions to use the most realistic (but justified) data on system behavior and plant response that is readily available. They are also to weed out any identifiable conservatisms in the final analyses of those accident sequences that rise to prominence in the preliminary screening. There will also be ample opportunity for licensee review of interim reports, the draft report, and the final report.
- b. Schedule. As noted above, we wish to proceed to the draft report stage to garner the experience with the use of the procedure guide which is needed to prepare for Phase III. We will not rush an

incomplete job into print in a final report. The end date may slip as necessary to achieve a quality product. At the same time I am aware, as I am sure you are, of the danger of having a poor quality draft report in existence with a correcting final report too distant.

I would like to begin work by gathering the teams in late August. Based on your comments we now propose to handle Millstone 1 and Calvert Cliffs in Washington, Arkansas 1 in Albuquerque, New Mexico, and Browns Ferry in Idaho Falls, Idaho. I hope this gives you the basis for enthusiastic participation in the IREP-II work. I propose that we meet with the four participating licensees on the afternoon of August 4 here in Bethesda if you feel that such a meeting would be of mutual benefit. Please call Robert M. Bernero, Director of the Probabilistic Analysis Staff, Office of Nuclear Regulatory Research, on (301) 492-6528 with your views.

Sincerely,

Original signed by
Darrell G. Eisenhut

Darrell G. Eisenhut, Director
Division of Licensing
Office of Nuclear Reactor Regulation

Enclosures: As Stated

cc w/encl: See Attached List

bcc w/encl: Docket File
NRC Public Document Room
G. Vissing, NRR

bcc w/o encl: R. Mattson
M. Ernst
S. Israel
F. Rowsome
J. Murphy
R. Bernero



Arkansas Power & Light Company

cc:

Mr. David C. Trimble
Manager, Licensing
Arkansas Power & Light Company
P. O. Box 551
Little Rock, Arkansas 72203

Mr. James P. O'Hanlon
General Manager
Arkansas Nuclear One
P. O. Box 608
Russellville, Arkansas 72801

Mr. William Johnson
U. S. Nuclear Regulatory Commission
P. O. Box 2090
Russellville, Arkansas 72801

Mr. Robert B. Borsum
Babcock & Wilcox
Nuclear Power Generation Division
Suite 420, 7735 Old Georgetown Road
Bethesda, Maryland 20014

Mr. Nick Reynolds
DeBevoise & Liberman
1200 17th Street, NW
Washington, D.C. 20036

Arkansas Polytechnic College
Russellville, Arkansas 72801

Director, Bureau of Environmental
Health Services
4815 West Markham Street
Little Rock, Arkansas 72201

Mr. Paul F. Levy, Director
Arkansas Department of Energy
3000 Kavanaugh
Little Rock, Arkansas 72205

Mr. William T. Craddock, Mgr.
Availability Engineering
First National Bank Building
P. O. Box 551, Seventh Floor
Little Rock, Arkansas 72203

Mr. Robert Szalay, Licensing and
Safety Project Manager
Atomic Industrial Forum
7101 Wisconsin Avenue
Washington, DC 20014

Mr. E. P. O'Donnell
Ebasco Services, Inc.
89th Floor
2 World Trade Center
New York, NY 10048

Dr. Edwin Zebroski
Nuclear Safety Analysis Center
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94303

#21

2. J.A. Murphy
3. R.M. Bernero
4. File, IREP

BALTIMORE GAS AND ELECTRIC COMPANY

P. O. BOX 1475
BALTIMORE, MARYLAND 21203

June 25, 1980

ARTHUR E. LUNDVALL, JR.
VICE PRESIDENT
SUPPLY

Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attn: Dr. Robert Bernero, Director
Probabilistic Analysis Staff

Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attn: Dr. Harold R. Denton, Director

Subject: Calvert Cliffs Nuclear Power Plant
Unit No. 1, Docket No. 50-317
Interim Reliability Evaluation Program

Calvert Cliffs
I REP

Reference: NRC letter dated 5/23/80 from D. G. Eisenhut
to IREP Participants, same subject.

Gentlemen:

The referenced letter informed us of the NRC's intention to conduct an Interim Reliability Evaluation Program on a cross-section of operating plants as the second phase of a three-phase effort to develop and implement probabilistic techniques for overall assessment of risk to the public health and safety from core damage accidents. The letter confirmed earlier indications from NRC that Calvert Cliffs Unit No. 1 would be asked to participate in the program.

A meeting was held on June 12, 1980 by your Staffs with the prospective licensee participants to discuss the concept and objectives of the Program. We agree wholeheartedly with the concept of using probabilistic techniques for risk assessment and of applying those results to the regulatory process, both during the design review phase of plant licensing and during the operational phase with due regard to appropriate value-impact assessments. We firmly believe that all parties concerned - the public, the licensees, and the regulators - can benefit from such an approach that is well-planned and has the cooperative participation of both the licensees and the NRC. However, we have several basic concerns with the Interim Reliability Evaluation Program as it was outlined in our June 12, 1980 meeting with members of your Staffs. These concerns are enumerated below.

Dupe of 84474329

1. Schedule. The proposed schedule for the program seems to be unrealistically compressed. It may be possible to conduct an evaluation of a specific plant in six months assuming the methodology is clearly understood by all parties and has been developed and tested. To attempt to develop a methodology concurrent with obtaining meaningful results and to do so with the full participation of licensee representatives, who are basically unfamiliar with the detailed program objectives and the possible types of methodology, is overly ambitious. Assuming completion of the program in this case, we are concerned that it would be at the expense of licensee understanding and participation, and that the results may be inconclusive and ambiguous because of time restrictions imposed on program development.
2. Methodology. The actual methods which will be used to initiate the program might apparently be drawn from experience at Crystal River or they might come from other sources. While we are not yet experts in risk assessment techniques, we do recognize that there are many ways to approach the task. It was indicated at our meeting that a "cookbook", which includes the basic methodology and assumptions upon which the entire program depends, would be developed as the program progressed, keeping about a month ahead of the actual program. The schedule, we were told, does not allow time for licensee input into the development of the "cookbook". We do not believe the results of the program will be meaningful without significant licensee participation in development of assumptions and methodology.
3. Timing. There is, as you know, a great deal of activity now taking place at all operating plants in response to the lessons learned at TMI-2. This activity includes such things as major modifications to auxiliary feedwater systems, changes to emergency power systems, control room changes (human factors engineering), operator training upgrades, the procurement of plant-specific simulators to improve operator response, and the like. These factors and others can and will have a major impact on system- and operator response, and their impact on the results of the IREP must be just as great, assuming all of these changes are being made to enhance overall safety. In some cases, NRC has not had the manpower necessary to review design changes being made, and it would seem appropriate to delay the start of the IREP until all of the TMI-related modifications are at least reviewed so that final designs can be factored into the IREP data base.
4. Licensee Participation. We are concerned that the party coming out of the IREP at the end with the least total contribution and the least understanding will be the licensee. The verve with which the NRC's Probabilistic Analysis Staff has described the conduct of the program has us concerned that they may charge off and leave us dragging along behind in the dust. To this end, licensees may want to have an outside consultant provide guidance and/or review services.

5. Regulatory Ratcheting. The close involvement of the NRC's Licensing Staff in the IREP makes it clear to us that the possibility exists of short notice changes to licensing requirements. Even though the IREP has been described as a "research program", we all know that, as time goes on, the results of this research will become more and more concrete as a foundation for licensing changes. The spirit of cooperative research and learning with which the program is conducted will likely be replaced by regulation based on the resulting numbers, which in fact may have little real basis because the assumptions and methodology were arbitrarily chosen by the Staff. Further down the road, assumptions and agreements made in the early stages of this "research" may well be forgotten as NRC personnel changes occur, as they frequently do.

For all of these reasons, we do not believe either the Staff or the licensees involved will benefit significantly from the IREP as it is now planned; the program may in fact result in negative effects. We strongly recommend the following changes:

1. Provide for licensee input into the methodology and assumptions to be used. This includes time for substantive peer review and comment of the Crystal River study, and licensee review and comment of the "cookbook", with formal resolution of all concerns and comments prior to beginning the program. To this end, it may be beneficial to have a meeting once the final version of the groundrules is drafted to ensure that all of the participants have a basic knowledge of and agreement on the methods to be utilized.
2. One of the NRC's admitted main objectives of the program is to meet the (arbitrary) schedule. This constraint should be greatly deemphasized, and the program tied instead to reasonable development and implementation of a meaningful program. We feel strongly that a Spring 1981 completion date is unattainable with any meaningful results, and that the program should allow for a Fall 1981 completion date or later if the need for such an expansion of the schedule is indicated.
3. Schedule periodic check points in the program which provide specific and ample time for review of the project to that point, and allow for consideration of possible changes in direction, scope or method as a result of review of the experience of other IREP plants and of other studies proceeding concurrently, such as the NSAC study of Oconee.

June 25, 1980

We are certain that you share our desire to make the Interim Reliability Evaluation Program as meaningful and beneficial as possible to all concerned. To this end, we request the opportunity to discuss the resolution of these concerns prior to finalizing our plans for participation in the Program.

Very truly yours,



cc: J. A. Biddison, Esquire
G. F. Trowbridge, Esquire
Messrs. E. L. Conner, Jr. - NRC
Dr. M. L. Roush, U of MD
~~D. K. Davis - TERA~~
G. D. Baston - Northeast Utilities
W. T. Craddock - AP&L
J. A. Raulston - TVA