Revision 1
12-10-80
1990f

INTERIM RELIABILITY EVALUATION PROGRAM
BROWNS FERRY TEAM FAULT TREE GUIDE

Milan E. Stewart

96
8105210096

TABLES

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 handbook[1].

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

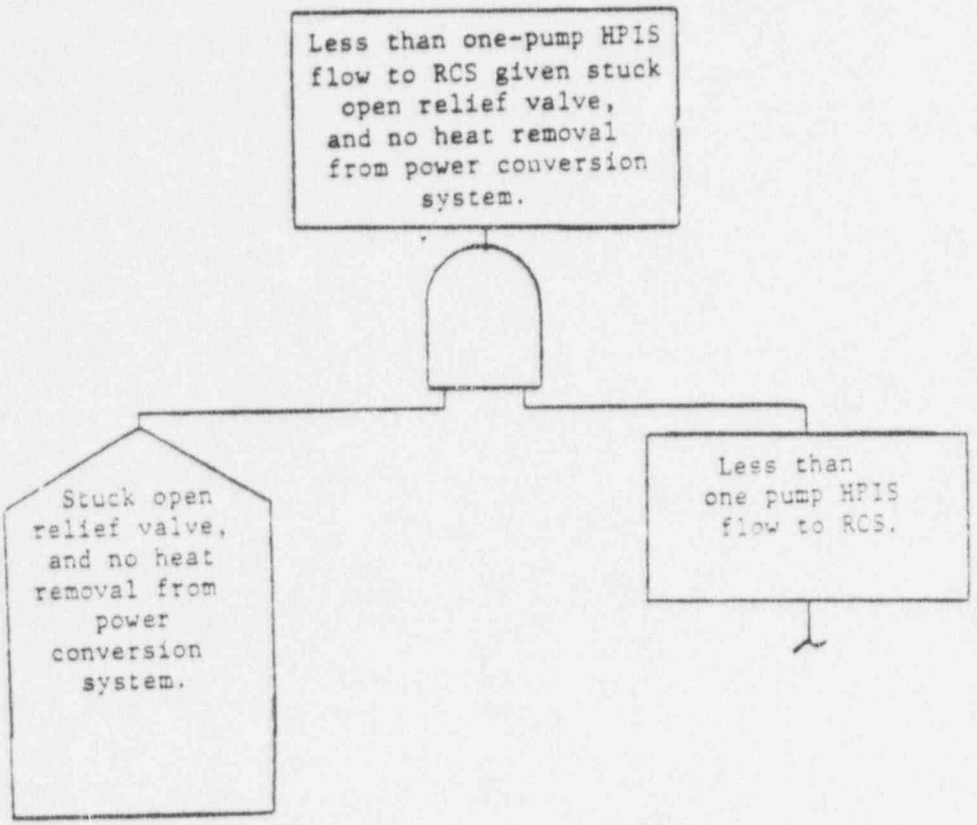


Figure 2
Top Two Fault Tree Tiers

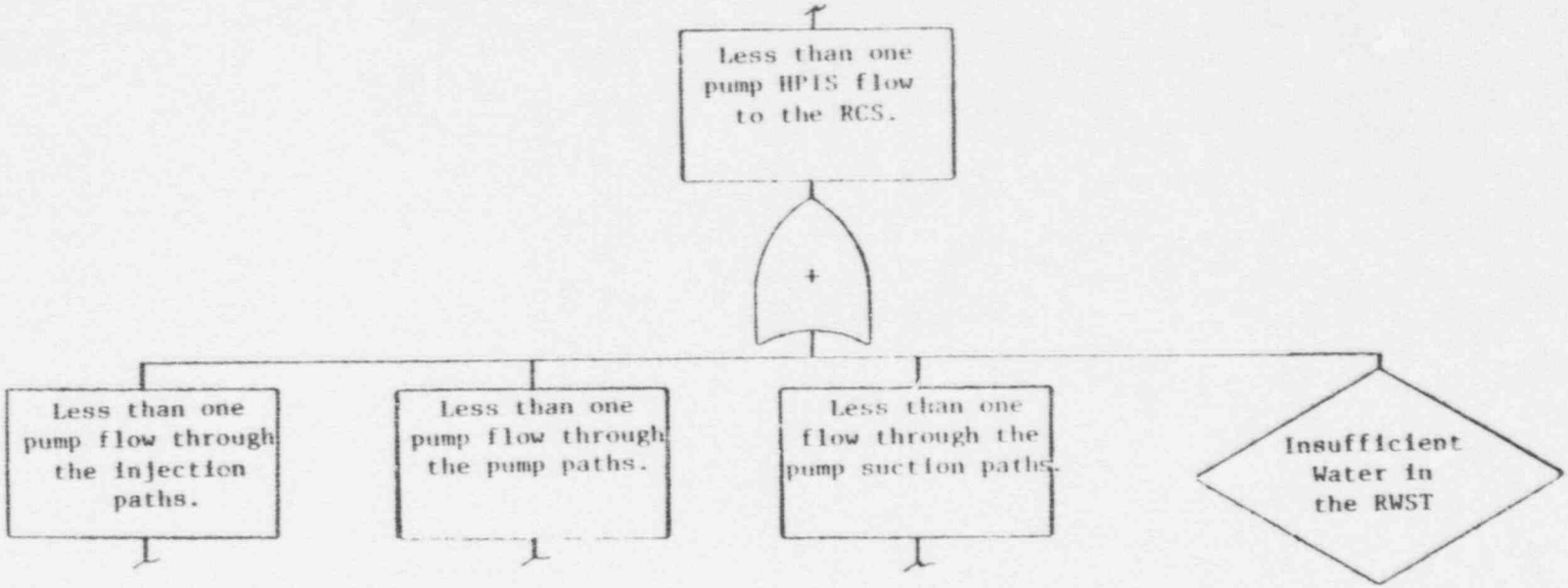


Figure 3

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.

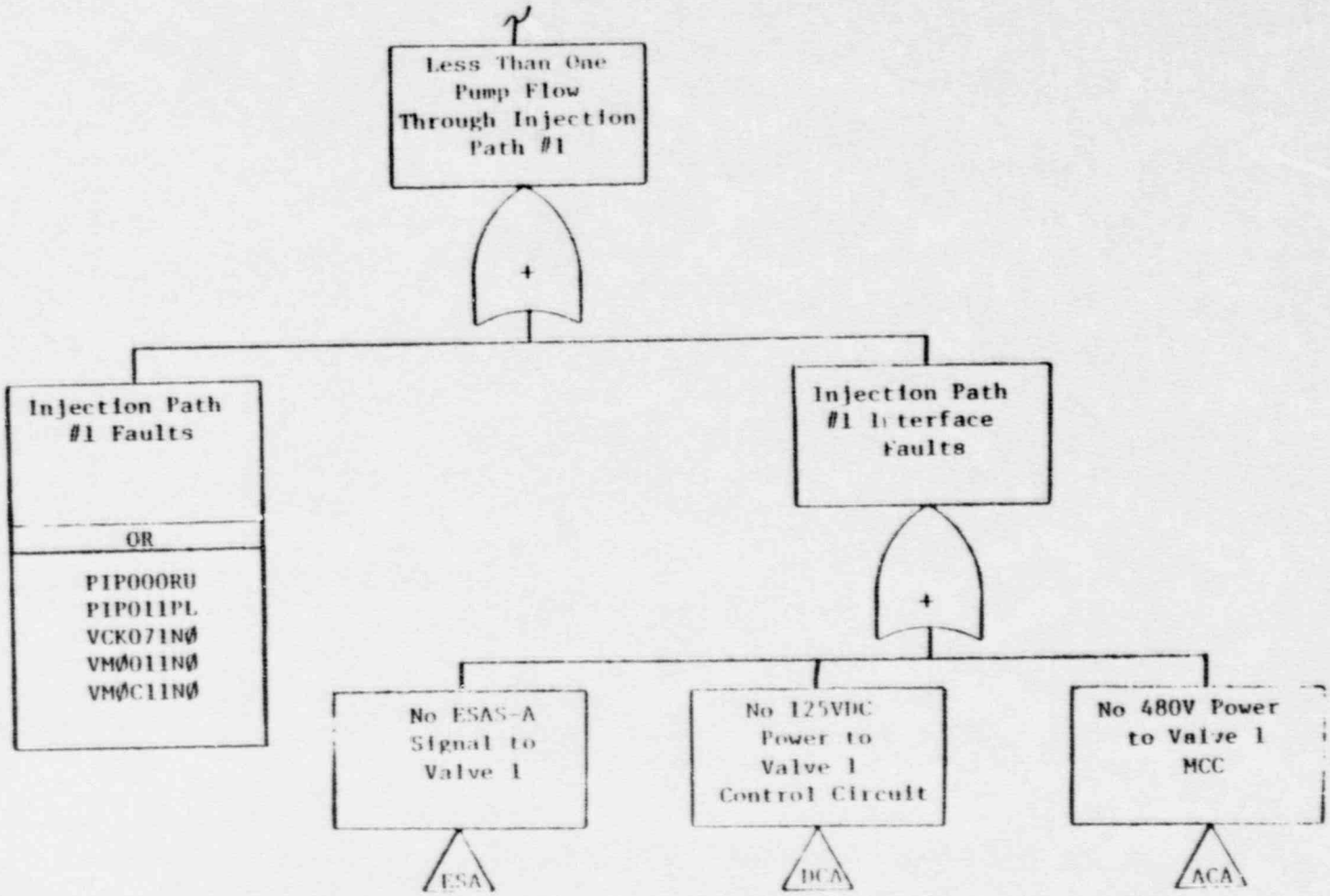


Figure 6

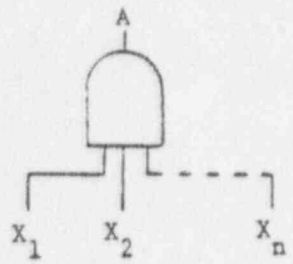
Basic Fault Events

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.

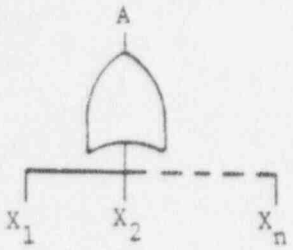
Most of the data available on nuclear components embody both primary and secondary causes for failure; therefore, the distinction between the two types of failure is not made on the fault tree except for the case in which a secondary cause results in multiple component failures, and the distinction is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

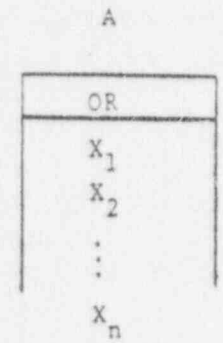
$A = X_1 X_2 \ldots X_n$ (all input events independent)



OR GATE

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

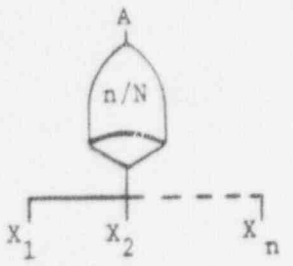
$A = X_1 + X_2 + \ldots X_n$ (all input events independent)



TABULATION OR GATE

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

$A = X_1 + X_2 + \ldots X_n$ (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 $N = 3$:

$A = X_1X_2 + X_2X_3 + X_3X_1$

Figure 7

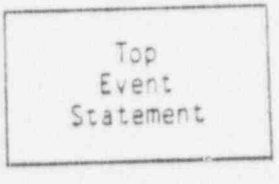
Abbreviated Fault Tree Logic Gates

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:



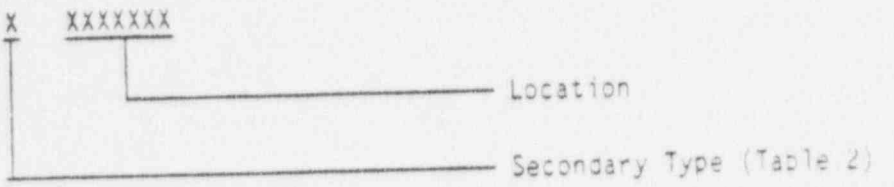
CBB-H2

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 desireable 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 existance 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 in.^{2}, >2 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.

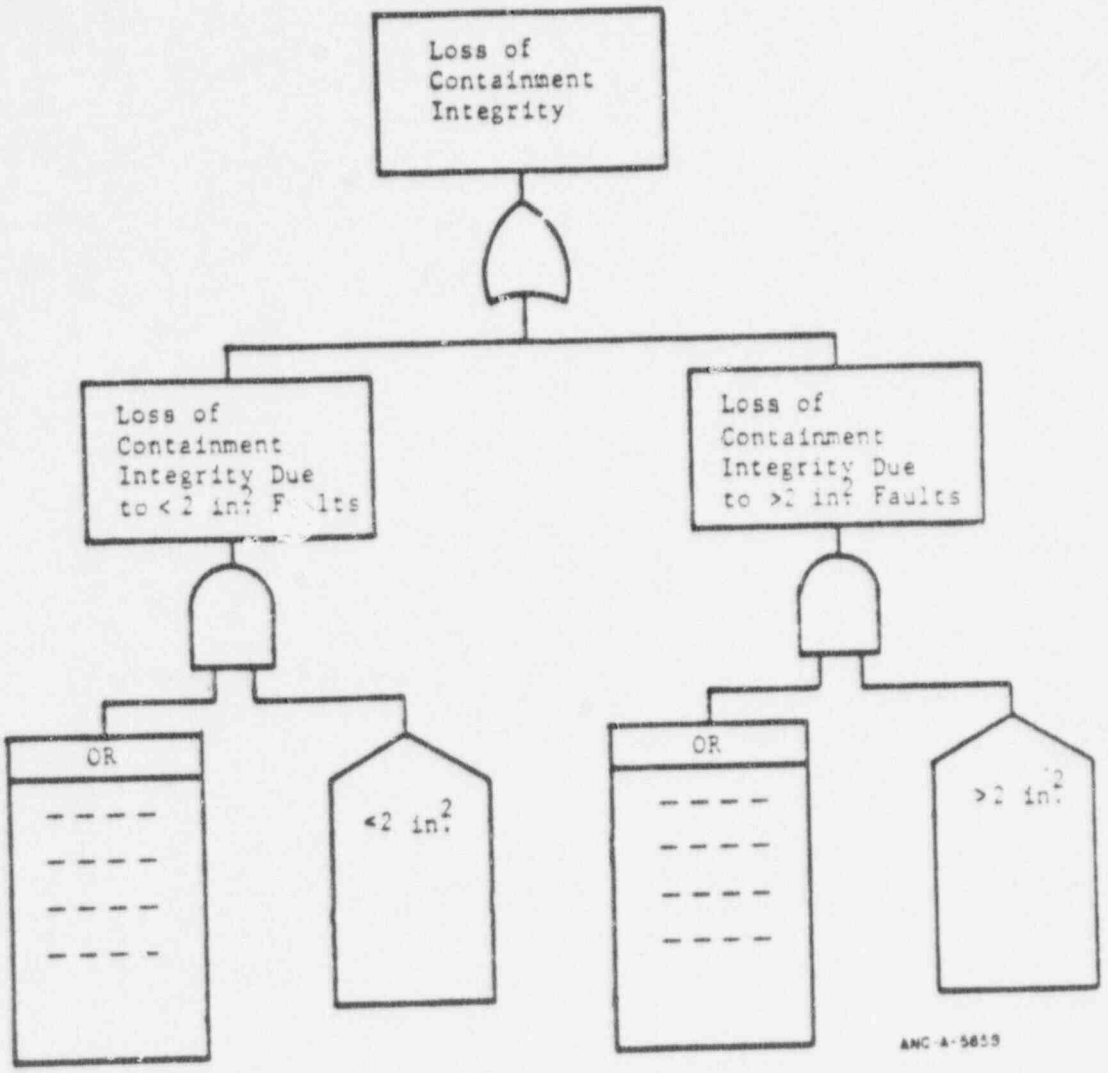


Figure 10
Classifying Faults Using the House

$$
\begin{aligned}
A &= A_2 \cdot A_3 \\
&= (A_1 + X_1) \cdot (X_1 + X_3) \\
&= (X_1X_2 + X_1) \cdot (X_1 + X_3) \\
&= X_1X_1X_2 + X_1X_1 + X_1X_2X_3 + X_1X_2
\end{aligned} \tag{1}
$$

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 agebraic 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.

TABLE 3

COMMON MODE EVENTS ON FAULT SUMMARY

EVENT NAME	EVENT COMPONENT	FAILURE MODE	PRIMARY FAILURE			SECONDARY EVENT (10 *) &																		LOCATION	REMARKS
			FAILURE RATE	FAULT DURATION	ERROR FACTOR	FIRE	FLOOD	EXPLOSIVE	STEAM	HI TEMP	PRESSURE	HUMIDITY	FREEZING	MISSILE	FIRE WHIP	WIND	DUST	RADIATION	CORROSION	NON-ELEC VOLT	VIBRATION	SOLVENT		
BPP001AR	Pipe 1	Rupture	10^{-9}	270	10			3			8		6	8	7									Pipe Tunnel	
BRE026A	Relay 26A	Doesn't Close	10^{-7}	270	10	05											(1)		5					Rm 211	
						3											(1)		3					Rm 211	
D00002111	Dust			(New Event)																					

*PROBABILITY OF SECONDARY EVENT OCCURRING (UPPER NUMBER)

PROBABILITY OF COMPONENT FAILURE GIVEN SECONDARY EVENT (LOWER NUMBER)

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; anotner 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 respresenting 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

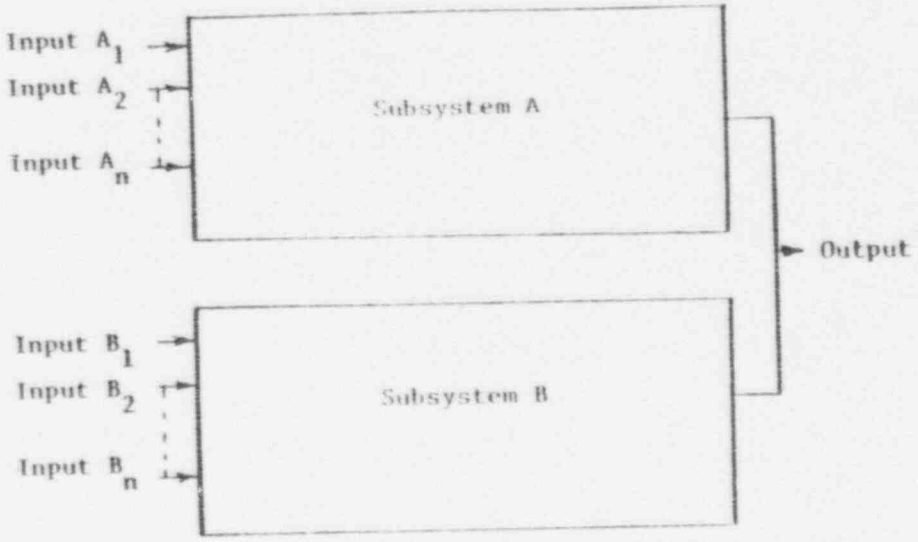


Figure 12

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

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

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. Kolaczkowski
4412	G. J. Kolb
4414	G. B. Varnado
4414	D. W. Stack
4414	R. B. Worrell
4412	D. D. Carlson

8105210096

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.

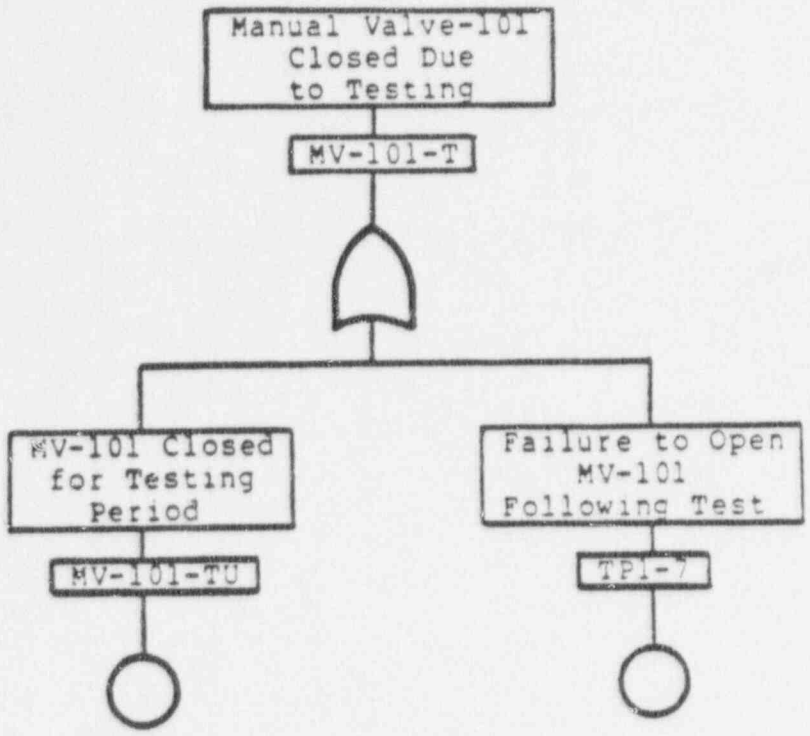
This may be done as follows. The analyst for each system reviews the testing requirements and testing procedures for the system. These should be placed in the system description notebook. For each procedure, he constructs a table of actions performed on components in the system. The table has the following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

Procedure	Step	Component	Action	Comments
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:



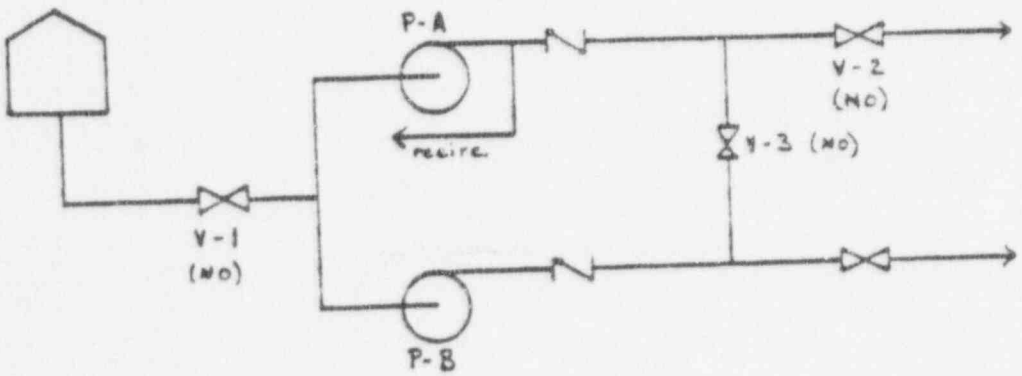
The event MV-101-TU reflects the unavailability during the test - it is assumed that the test procedure is performed correctly. The other event, TP1-7, reflects the human error which leaves the component in the failed state.

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 "TP1-7" 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.



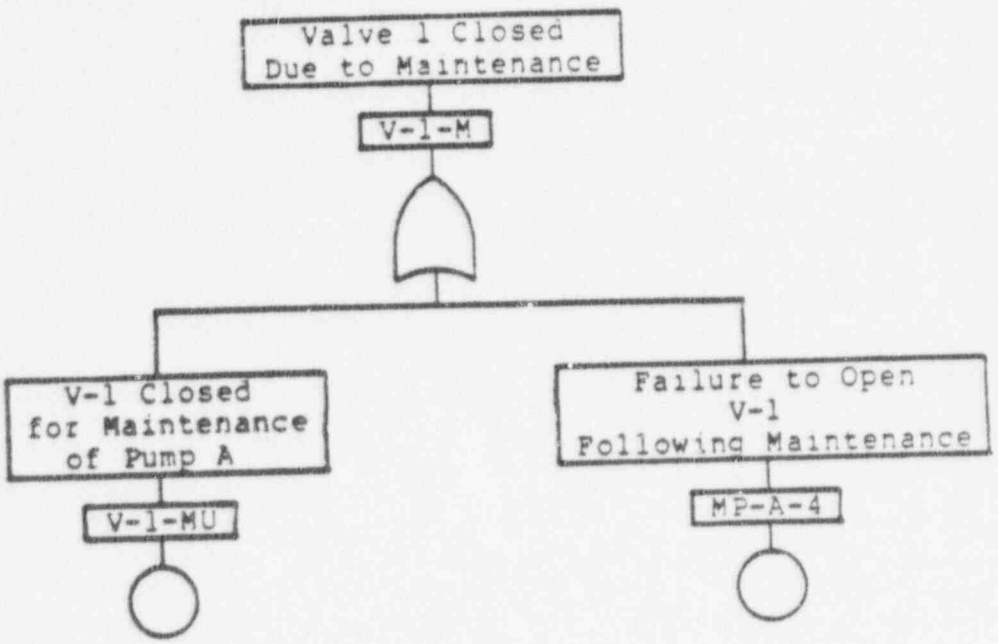
Testing of Pump A requires the following steps:

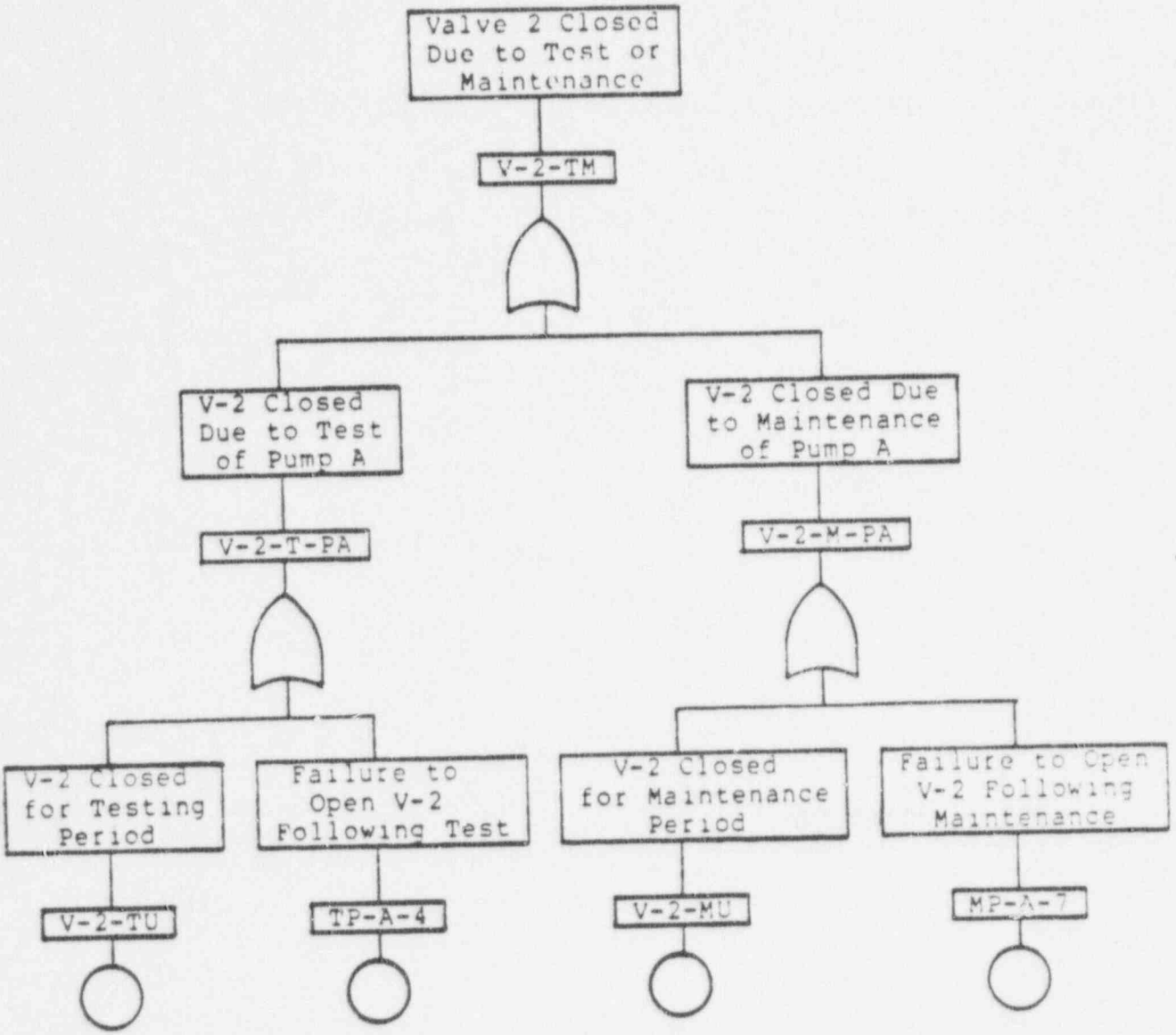
Procedure	Step	Component	Action
TP-A	1	V-2, V-3	Close
	2	P-A	Turn on
	3	P-A	Turn off
	4	V-2, V-3	Open

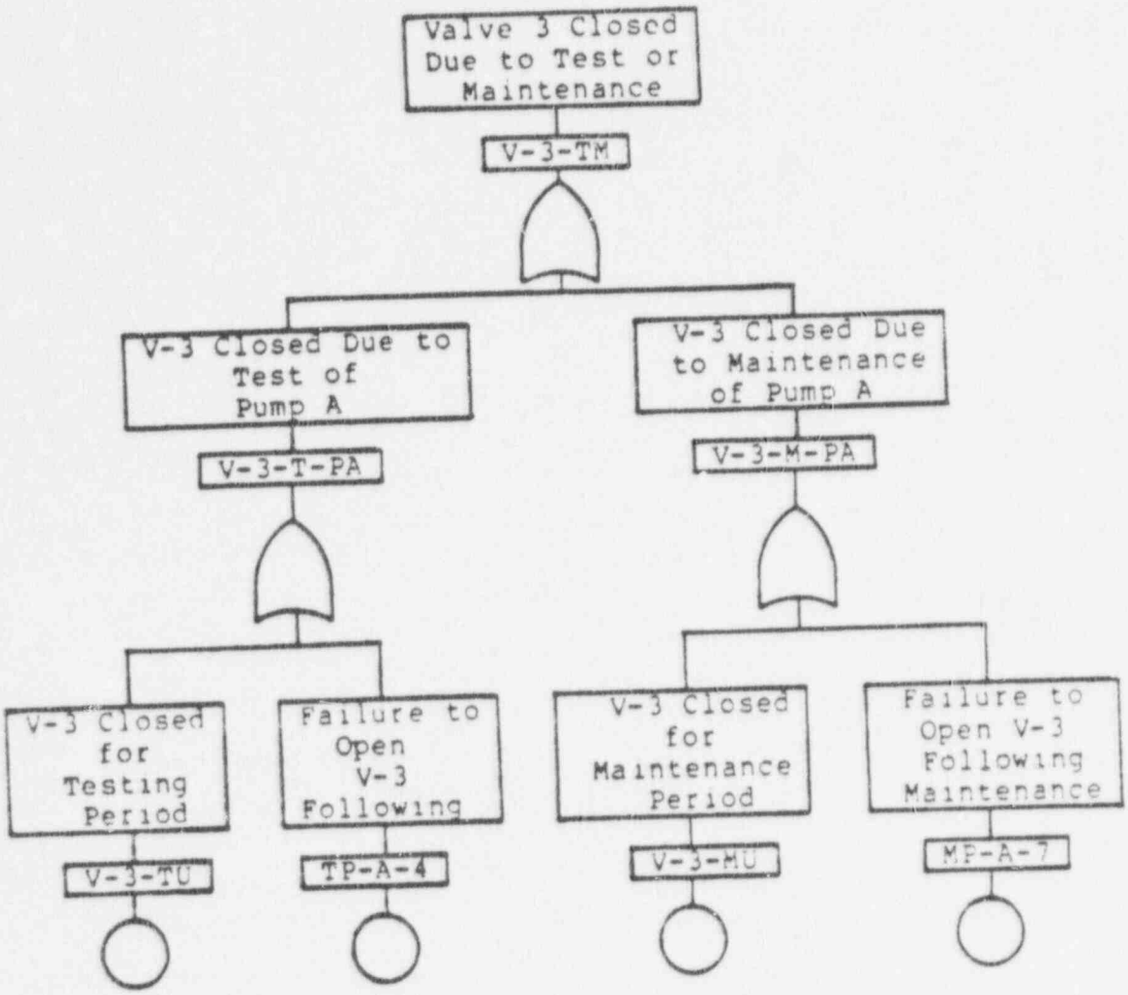
Maintenance on Pump A requires the following steps:

Procedure	Step	Component	Action
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:




Valve 2 Closed Due to Test or Maintenance
V-2-TM
V-2 Closed Due to Test of Pump A
V-2 Closed Due to Maintenance of Pump A
V-2-T-PA
V-2-M-PA
V-2 Closed for Testing Period
Failure to Open V-2 Following Test
V-2 Closed for Maintenance Period
Failure to Open V-2 Following Maintenance
V-2-TU
TP-A-4
V-2-MU
MP-A-7


Valve 3 Closed Due to Test or Maintenance
V-3-TM
V-3 Closed Due to Test of Pump A
V-3 Closed Due to Maintenance of Pump A
V-3-T-PA
V-3-M-PA
V-3 Closed for Testing Period
Failure to Open V-3 Following
V-3 Closed for Maintenance Period
Failure to Open V-3 Following Maintenance
V-3-TU
TP-A-4
V-3-MU
MP-A-7

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

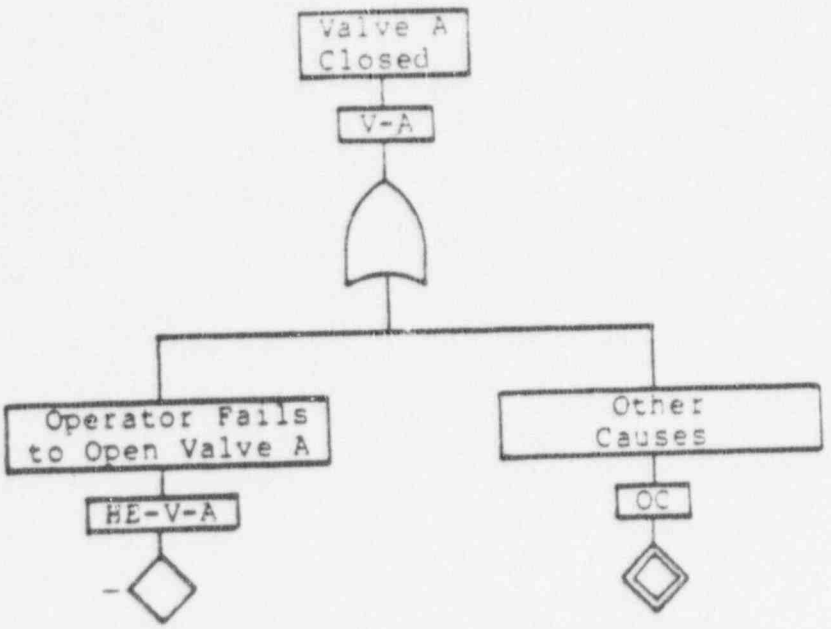
The treatment of potential human errors under accident conditions is somewhat more difficult than the treatment of errors during test and maintenance. A major difficulty in including these errors explicitly in the fault logic is that operator actions are dependent upon the particular accident sequence. 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 Operatin during test and maintenance. A major difficulty in including Procedure which the operators would use in responding to a transient or accident. To identify the components susceptible to human error during an accider a table is constructed of the following form:

Procedure	Step	Component	Action	Comments
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:

Accident Sequence	Designator	Procedures Used
Large Loca-10	ACD	EOP-1, EOP-2
Small LOCA-34	S_1C	EOP-1

Given this table and the preceeding 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 sufficien for the arrival (if not already present) of a shift supervisor and two reactor operaators. 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 collective 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 0.

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

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 inferrences 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 occuring 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. Instrinsic 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-STD 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 enountered 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:

$$Q = Q_D + \tfrac{1}{2}\lambda T$$

where: Q = Total component unavailability

Q_D = Demand unavailability

$\tfrac{1}{2}\lambda T$ = 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 occured 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 sub-classes 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 intrisic 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,

the minimal cut sets are examined to determine if any of the minimal cuts 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:

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

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 [illegible] 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.

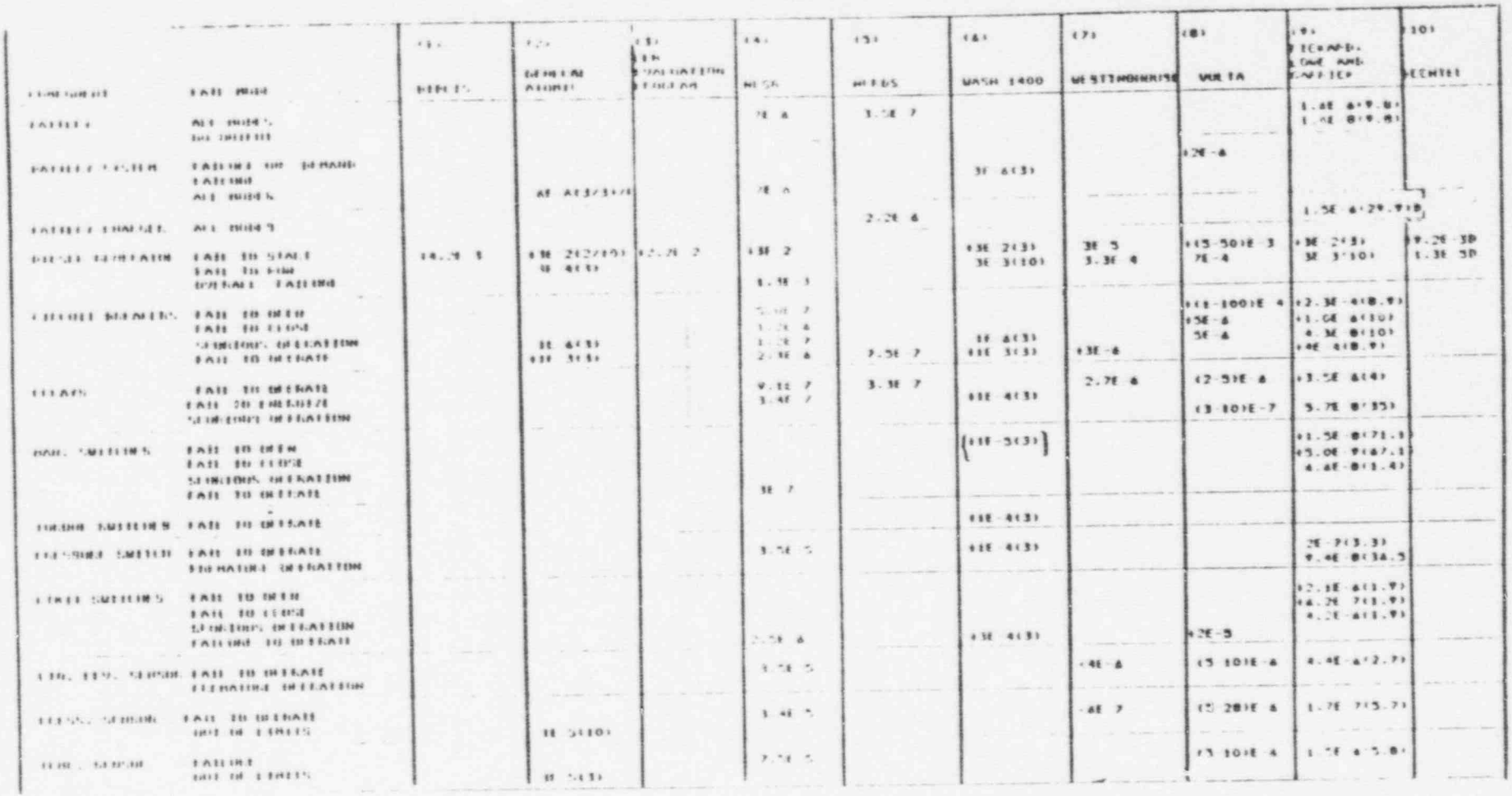
3. W. H. Hubble, C. H. Miller, Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants - January 1, 1972 to April 30, 1978, NUREG/CR-1331, EGG-EA-5079, February 1980.

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.

Table 1

COMPONENT	FAIL MODE	(1) DIMITS	(2) GENERAL ATOMIC	(3) LER EVALUATION PROGRAM	(4) NESA	(5) NPRDS	(6) WASH 1400	(7) WESTINGHOUSE	(8) VOLTA	(9) PICKARD, LOWE AND GARRICK	(10) BECHTEL
AUX FEED PUMPS	FAIL TO START FAIL TO RUN		*1E-2(3) 1E-4(3/10)					2.0E-5 1.2E-5			1.7E-5
DIESEL PUMPS	FAIL TO START FAIL TO RUN FAIL TO START & RUN	10.1E-3	*1E-3(3/10)	(2.7E-3 (2.3-12)E-4	(2E-5 3.5E-4	3.9E-5	*1E-3(3) 3E-5(10)	1.5E-5A	*1E-3 (6-200)E-6	*1E-3(3) 3E-5(10) 1E-4(3)	
MANUAL VALVES	FAIL TO OPERATE FAIL TO REMAIN OPEN (PLUG)		*1E-3(3)		6.3E-6		*1E-4(3)				
MOV'S	FAIL TO OPEN FAIL TO CLOSE SPURIOUS OPERATION ALL MODES		[*1E-3(3)]	*2E-3 10E-4	4.5E-5		*1E-3(3)	{7.5E-6A} 5E-6	*(1-50)E-4 *(1-5)E-3 (3-100)E-7	*1E-3(3) *1E-3(3) 3.5E-6(10)	
SOLENOID VALVES	FAIL TO OPEN FAIL TO CLOSE SPURIOUS OPERATION FAIL TO OPERATE				*5E-4 *5E-4 9E-6		*1E-3(3)	3.5E-7	(2-6)E-6	*1E-3(3) *1E-3(3) 3.5E-6(3)	
ALL FLUID VALVES	FAIL TO OPEN FAIL TO CLOSE SPURIOUS OPERATION ALL MODES	*1.5E-3 *1.3E-2			2E-5(3)		*3E-4(3) *3E-5(3)		*(2-500)E-5 *(2-50)E-5 *7E-3	*1.2E-5(2) *1.2E-5(2) 5.5E-6(2) 3E-5(3)	
VACUUM VALVES	FAIL TO OPEN				2.2E-6						
RELIEF VALVES	FAIL TO OPEN FAIL TO CLOSE 10% LIGHT 10% HEAVY PREMATURE OPERATION		*1E-4(10)H *5E-2(3)H 1E-3(3)H	*(4-7)E-3 *(3-6)E-3 3E-6	1.4E-6 1.2E-6 0E-6 3E-6		*1E-5(3) 1E-5(3)	5E-6	*5E-4	*1.3E-3(10) *1.0E-2(10) 3.5E-6(3)	8.4E-6
PILOT RELIEF VLVS	FAIL TO OPERATE FAIL TO RESEAT				4.5E-6			*1E-2			
PRESSURE REL VLV	FAIL TO OPERATE				7E-6					*1E-5(3) *1E-4(3) 3.5E-6(3)	
SAFETY VALVE	FAIL TO OPEN FAIL TO CLOSE SPURIOUS OPERATION	2.1E-7									
CHECK VALVES	REVERSE LEAKAGE FAIL TO OPEN FAIL TO CLOSE SPURIOUS OPERATION FAIL TO OPERATE		3E-6(3/10) *1E-4(3)	5E-7 5E-5 1E-4	1.4E-5 8.4E-6 3.2E-5		*1E-4(3)	*1.2E-5	*5E-3 1E-5	2.9E-6(1.2) *1E-4(3)	1.6E-7 1.6E-6
PIPES 3"	RUPTURE ALL MODES		1E-10(100/30)/S		1.6E-10/S 7.4E-9/S	1.5E-5	1E-10(30)/S			1E-10(30)/S	1E-10
PIPES 3"	RUPTURE ALL MODES		1E-10(100/30)/S		1.6E-10/S 7.4E-9/S	7.7E-6 1.9E-7	1E-9(30)/S *1E-4(3)		8E-7 *(1-25)E-6	1E-9(30) *1E-4(5)	1E-9
STEAM TRAPS	FAIL TO STEAM				1.6E-5		*3E-4(3) 1E-6(10)				
FLUID CLUTCH	FAIL TO OPERATE PREMATURE DISENGAGEMENT				5E-6		*3E-4(3)				
MECH. CLUTCH	FAIL TO OPERATE PREMATURE DISENGAGEMENT				4.2E-6						
GASKETS	LEAKAGE					1.0E-6					



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

TABLE -

YPS	COMPONENT & FAILURE MODE		FAIL QTY		EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF		FACTORS FOR NSSS* B	C	W	G	WASH-1400
	REACTOR SCRAM RODS(##)														
6-8	FAIL TO SCRAM TO 96%		1	D	1E-3	1E-3	3E-2	3E-5	1E-3	1	29*	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	2					
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					
			0	D	-	-	3E-2	6E-5	-		3*	6*	2*		
2-8			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					

YRS	COMPONENT & FAILURE MODE		FAIL QTY		EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF		FACTORS FOR NSSS B	C	W	G	WASH-1400
	DIESEL GENERATORS														
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	0	2E-3	5E-2	4E-1	6E-3	9E-3	6	1	2	.7	1	3E-3 10
"	" (MONTHLY TEST)		112	0	7E-3	2E-1	2E-1	3E-2	4E-2	6	1	2	.7	1	
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	D	5E-4	8E-4	6E-2	2E-5	6E-4	1	2	8**		.9	
2-8	"		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					
			13	S	9E-7	4E-6	1E-4	5E-7	2E-6	2	1	3		.1	
6-8	INADVERTENT MOTION		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					
			15	S	6E-7	4E-6	1E-4	3E-7	2E-6	3	2	3		.1	
2-8	"		27	S	2E-7	2E-6	3E-6	3E-7	7E-7	3					
"	"	(WCF)	118	S	6E-7	4W-5	1E-4	3E-6	5E-6	9	3	.8		.3	
			40	S	2E-7	3E-6	2E-6	4E-7	7E-7	4					
			12	S	1E-6	6E-6	1E-4	2E-6	3E-6	2	2	1		.2	
6-8	AGG STD T.S. PLANTS		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					
			9	S	9E-7	5E-6	6E-6	5E-7	2E-6	2	1	3		1	
6-8	AGG NONSTD T.S. PLANTS		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					
			21	S	9E-7	6E-6	1E-4	8E-7	2E-6	3	1	2		.6	
6-8	AGG FAILURES ALL		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					
			29	S	5E-7	6E-7	1E-6	6E-7	2E-6	4	1	1		.7	
2-8	AGG FAILURES ALL		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.

FPS	COMPONENT & FAILURE MODE		FAIL QTY		EXP MIN	EXP MAX	UB MAX	ALL AVE	GEOM MEAN/EF		FACTORS FOR NSSS B	C	W	G	WASH-1400	
	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	4E-1	4E-3	1E-2	6	1	1	1	.9		
"	" (TURB)		18	D	7E-3	1E-1	3E-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* B	C	W	G	WASH-1400	
	MOV															
6-8	FAIL TO OPERATE	(WCF)	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	(WCF)	7	S	6E-7	2E-6	8E-5	1E-7	1E-6	2	1	7*	1	.7	1E-8	10
	PLUGGED	(WCF)	4	S	3E-6	3E-6	8E-5	6E-5	3E-6	1	7*	4	2	2	3E-7	3
	REMOTE & MOV															
6-8	FAIL TO OPERATE	(WCF)	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	(WCF)	12	S	6E-7	2E-6	8E-5	2E-7	1E-6	2	.8	4	1	1		
	PLUGGED	(WCF)	9	S	6E-7	3E-6	8E-5	1E-7	1E-6	2	1	2	1	.5		
	AIR OPERATED VALVE															
6-8	FAIL TO OPERATE	(WCF)	3	D	7E-3	6E-2	3E-1	7E-4	2E-2	3	9	4*	.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	(WCF)	2	S	3E-6	2E-5	8E-4	2E-7	8E-6	2	22*	7*	1	2	1E-8	10
	PLUGGED	(WCF)	1	S	1E-5	1E-5	8E-4	1E-7	1E-5	1	43*	13*	2	11*	3E-7	3
	MANUAL VALVE															
6-8	FAIL TO OPERATE		3	D	1E-3	2E-3	7E-2	8E-5	2E-3	1	2	3	2*	1		
	LEAK EXTERNALLY		1	S	6E-7	6E-7	1E-4	1E-8	6E-7	1	21*	8	6*	11*	1E-8	10
	CHECK VALVE															
6-8	LEAK EXTERNALLY		3	S	4E-6	5E-6	7E-5	5E-8	4E-6	1	6	7*	2*	1	1E-8	10
	LEAK INTERNALLY		38	S	7E-7	2E-5	7E-5	7E-7	3E-6	5	.4	1	.7	2	3E-7	3
	FAIL TO OPEN		3	D	3E-3	1E-2	5E-2	1E-4	6E-3	2	8*	7*	1	1	1E-4	3
	PWR PRIMARY SAFETY															
6-8	PREMATURE OPEN		7	S	1E-5	4E-5	2E-3	3E-6	2E-5	2	3*	2	1		1E-5	3
	FAIL TO OPEN		6	D	2E-2	2E-1	8E-1	6E-3	6E-2	3	5*	2	.9		1E-5	3
	BOIL PRIMARY RELIEF															
6-8	FAIL TO OPEN		30	D	1E-2	9E-2	2E-1	8E-3	3E-2	3					1E-5	3
	FAIL TO OPEN	(WCF)	38	D	1E-2	9E-2	2E-1	1E-2	3E-2	3						
	FAIL TO RESEAT	(WCF)	18	D	2E-3	2E-2	2E-1	5E-3	6E-3	3						
	FAIL TO RESEAT		17	D	3E-3	2E-2	2E-1	5E-3	7E-3	2					1E-5	3
	PREMATURE OPEN		21	S	9E-6	4E-5	6E-5	6E-6	2E-5	2						
	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 THRUU 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. * MEANS, 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):	D (A)	3E-4	3E-3	1E-3	3	
FAILURE TO START ON DEMAND:	D	3E-6	3E-4	3E-5	10	
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENTS):	D	1E-4	1E-2	1E-3	10	
FAILURE TO RUN, GIVEN START, (EXTREME, POST ACCIDENT EVIRONMENTS INSIDE CONT.)	D	3E-5	3E-3	3E-4	10	
FAILURE TO RUN, GIVEN START (POST ACCIDENT, AFTER ENVIRONMENTAL RECOVERY)						
TURBINE DRIVEN PUMPS:	D	1E-3	1E-2	3E-3	3	A
FAILURE TO START ON DEMAND:	D	1E-5	1E-4	3E-5	3	A
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT)						
VALVES:						
MOTOR OPERATED:	D (B)	3E-4	3E-3	1E-3	3	
FAILURE TO OPERATE (INCLUDES DRIVER):	D (C)	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-7	1E-6	3E-7	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-9	1E-7	1E-8	10	
RUPTURE						
SOLENOID OPERATED:	D (D)	3E-4	3E-3	1E-3	3	
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-9	1E-7	1E-8	10	
RUPTURE:						
AIR-FLUID OPERATED:	D (A)	1E-4	1E-3	3E-4	3	
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-7	1E-6	3E-7	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-9	1E-7	1E-8	10	
RUPTURE:						
CHECK VALVES:	D	3E-5	3E-4	1E-4	3	
FAILURE TO OPEN:	D	1E-7	1E-6	3E-7	3	
INTERNAL LEAK (SEVERE):	S	1E-9	1E-7	1E-8	10	
RUPTURE:						
VACUUM VALVE:	D	1E-5	1E-4	3E-5	3	
FAILURE TO OPERATE:						
MANUAL VALVE:	D	3E-5	3E-4	1E-4	3	A
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-9	1E-7	1E-8	10	
RUPTURE:						
PRIMARY SAFETY VALVES (PWR):	D	1E-3	1E-2	3E-3	3	R
FAIL TO OPEN:	S	1E-6	1E-5	3E-6	3	R
PREMATURE OPEN:	D **	3E-3	3E-2	1E-2	3	R
FAIL TO RECLOSE (GIVEN VALVE OPENED)						
PRIMARY SAFETY VALVES (BWR):	D	3E-3	3E-2	1E-2	3	R
FAIL TO OPEN:	S	1E-6	1E-5	3E-6	3	R
PREMATURE OPEN:	D	1E-3	1E-2	3E-3	3	R
FAIL TO RECLOSE (GIVEN VALVE OPENED)						

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 + O	3E-11	3E-8	1E-9	30
PIPE > 3-INCH DIAMETER (PER SECTION): RUPTURE/PLUG	S + O	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 PER HOUR RATES, SINCE PHENOMENA ARE GENERALLY TIME DEPENDENT, BUT PLUGGED CONDITION MAY ONLY BE DETECTED UKPON 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.

ABREIVIATIONS:

(1) FOR FAILURE RATE TYPE ABREVIATIONS:

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) ABREVIATIONS:

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:	D (A)	1E-4	1E-3	3E-4	3
PREMATURE DISENGAGEMENT:	0	1E-7	1E-5	1E-6	10
MOTORS, ELECTRIC:					
FAILURE TO START:	D (A)	1E-4	1E-3	3E-4	3
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT):	0	3E-6	3E-5	1E-5	3
FAILURE TO RUN, GIVEN START (EXTREME ENVIRONMENT):	0	1E-4	1E-2	1E-3	10
RELAYS:					
FAILURE TO ENERGIZE	D (A)	3E-5	3E-4	1E-4	3
FAILURE OF NO CONTACTS TO CLOSE, GIVEN ENERGIZED:	0	1E-7	1E-6	3E-7	3
FAILURE OF NC CONTACTS BY OPENING, GIVEN NOT ENERGIZED:	0	3E-8	3E-7	1E-7	3
SHORT ACROSS NO/NC CONTACT:	0	1E-9	1E-7	1E-8	10
COIL OPEN:	0	1E-8	1E-6	1E-7	10
COIL SHORT TO POWER:	0	1E-9	1E-7	1E-8	10
CIRCUIT BREAKERS:					
FAILURE TO TRANSFER:	D (A)	3E-4	3E-3	1E-3	3
PREMATURE TRANSFER:	0	3E-7	3E-6	1E-6	3
SWITCHES:					
LIMIT:					
FAILURE TO OPERATE:	D	1E-4	1E-3	3E-4	3
TORQUE:					
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3
PRESSURE:					
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3
MANUAL:					
FAILURE TO TRANSFER:	D	3E-6	3E-5	1E-5	3
SWITCH CONTACTS:					
FAILURE OF NO CONTACTS TO CLOSE GIVEN SWITCH OPERATION:	0	1E-8	1E-6	1E-7	10
FAILURE OF NC BY OPENING, GIVEN NO SWITCH OPERATION:	0	3E-9	3E-7	3E-8	10
SHORT ACROSS NO/NC CONTACT:	0	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
TRANSFORMERS:					
OPEN CIRCUIT PRIMARY OR SECONDARY:	0	3E-7	3E-6	1E-6	3
SHORT PRIMARY TO SECONDARY:	0	3E-7	3E-6	1E-6	3
SOLID STATE DEVICES, HIPOWER APPLICATIONS (DIODES, TRANSISTORS, ETC.):					
FAILS TO FUNCTION:	0	3E-7	3E-5	3E-6	10
FAILS SHORTED:	0	1E-7	1E-5	1E-6	10

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

NOTES

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

ABBREVIATIONS:

(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) ABREVIATIONS:

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

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