PROBABILISTIC SAFETY ANALYSIS

EPRI NP-424
(Research Project 217-2-4)

Final Report

April 1977

Prepared by

Science Applications, Inc.
2680 Hanover Street
Palo Alto, California 94304

Principal Investigator
R. C. Erdmann

Project Personnel

R. R. Fullwood	F. L. Leverenz
A. A. Garcia	R. Ritzman
J. E. Kelly	E. T. Rumble
H. Kirch	C. A. Stevens

Prepared for

Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

Project Manager
G. S. Lellouche

LEGAL NOTICE

This report was prepared by Science Applications, Inc., as an account of work sponsored by the Electric Power Research Institute, Inc. (EPRI). Neither EPRI, members of EPRI, Science Applications, Inc., nor any person acting on behalf of either: (a) makes any warranty or representation, express or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or (b) assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method, or process disclosed in this report.

FOREWORD

This document is the final report of contract RP217-2. Within the original scope of the contract one may say that it was successful. A dedicated center for probabilistic analysis has been established with the abilities needed to supply the Nuclear Power Division with the desired expertise. The application of the various methodologies has started and one can anticipate fruitful results with potential impact on the perception of reactor safety as well as on the licensing process.

G.S. Lellouche, Program Manager
Statistical and Environmental Analysis

ABSTRACT

This is the final report on project RP217-2. It discusses the development of a functioning, dedicated, research group in the area of probabilistic analysis and it describes the early efforts in applying the methodologies. Work has centered on mining the Reactor Safety Study (WASH-1400), developing new computer code capabilities, and work has started on a reappraisal of the ATWS problem.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont)

SECTION 1
INTRODUCTION AND SUMMARY

This report summarizes work carried out during the second year of the Science Applications, Inc. (SAI)/Electric Power Research Institute (EPRI) dedicated contract (RP217-2) on LWR probabilistic safety analysis. Progress on a variety of tasks completed in the first year was summarized in EPRI Report 217-2-4, "Probabilistic Safety Analysis"[1]. Second-year tasks have been informally documented in quarterly reports[2,3,4]. Work reaching a significant milestone has been documented in various published reports. This annual report will provide summaries of first and second-year tasks, some of which are separately documented, and some of which are not yet documented.

The primary goal of this activity was to establish a functioning risk analysis group rooted in probabilistic safety methods. Much of the effort was spent in studying, modifying, and reapplying the analysis techniques of WASH-1400. Work was begun expanding this scope to specific areas where the contribution to risk was felt to be important. Such work has included re-evaluations of the Pressurized Water Reactor (PWR) check valve problem and anticipated transient without scram (ATWS) events.

Risk assessment and probabilistic safety analysis requires an examination of the consequence and likelihood of the deviation from normal operation of a plant or process. The appropriate combination of these two evaluations, their interpretation in both absolute and relative measures, and the definition of the measures themselves, requires knowledge of many engineering disciplines. The process is greatly simplified if the methods of analysis are standardized in the form of specified procedures, computer codes, and readily available data on relevant parameters. Establishing such a process is a continuing goal for the SAI working group.

Past work has demonstrated the validity of probabilistic safety analysis methodology in assessing levels of reactor risk. Moreover, these

levels of reactor safety appear socially acceptable when compared to other risks to which the population is exposed. Fault and event tree analysis is currently the best way to carry out this work, and it can be applied at any stage in the life of a plant. Indeed, this methodology is being applied or will be soon applied in other parts of the nuclear fuel cycle and in other industrial activities. Its ultimate incorporation into reactor licensing seems likely.

The areas which can be examined via probabilistic safety are numerous. For example, the risk reduction due to backfitting can be optimized by these techniques. Also, the effect of new regulations and guides imposed on the nuclear industry can be quantified in terms of their effect on public risk levels. These suggestions are, of course, in addition to the basic effort of continually evaluating plant accident sequences and extending the methodology into new reactor types (i.e.,HTGR, LMFBR), new site concepts (i.e.,off-shore, underground), and more inclusive types of accidents (i.e.,external events, sabotage).

Each of the following chapters of this report summarizes work in a particular area. Chapter 2 describes the summary[5] and critique[6] of the complete Reactor Safety Study Report[7].

Chapter 3 presents a summary of a detailed sensitivity/perturbation analysis[8] on two reactors. Analyses such as these allow comparison of similar systems in different plants and also comparison of the capability of various alternate systems within a plant to perform a given function. The second part of Chapter 3 contains the results of a detailed analysis[9] of the most influential PWR sequence (relative to consequences). Part of the analysis includes a comparison of various design options suggested by NRC in the Standard Review Plan. This comparison via probabilistic methods shows that the options are not equivalent, and the analysis itself points to an improved design.

Part of the detailed examination of methodology included investigation of the computer codes utilized in WASH-1400. As a result, a family of codes has been developed at SAI which are used to evaluate plant risk, both quantitatively and qualitatively. The development and capabilities of these

codes along with the improved methodologies they represent are presented in Chapter 4.

For purposes of comparing different plants, a set of event trees was developed for a large PWR different from any examined previously. While the task is incomplete, in terms of numerical evaluation due to unavailability of plant design details, some comparisons have been made. These event trees are described in Chapter 5.

A series of documents is being prepared regarding the basis for the problem of anticipated transients without scram (ATWS). The purpose of these documents is to evaluate risk due to ATWS in the light of developments subsequent to the publication of WASH-1270[10]. During this report period, draft versions of three documents[11,12,13] were completed. The work contained in these documents as well as a summary of the areas yet to be studied is reported in Chapter 6.

During the first year of the SAI/EPRI contract, work was begun on a systematic approach to gathering actual plant failure data. A computer code was written which manages the file of data being collected. The code has been modified to make it more comprehensive, and data collection continues under a parallel EPRI-sponsored program. The effort is summarized in Chapter 7.

Probabilistic analysis of safety systems can suffer somewhat due to the difficulty in showing that actual system availability is accurately predicted by reliability analysis techniques. In Chapter 8, work to date on safety analysis verifiability is presented. Included is a literature search and suggested studies which would allow the validity of the reliability analysis techniques to be evaluated.

SECTION 2

SUMMARY AND CRITIQUE OF WASH-1400 (Draft)

The first task in developing a risk analysis group to support EPRI was to evaluate and study existing work. The Reactor Safety Study report, WASH-1400[7], provided a substantial portion of the background. Utilizing personnel who participated in the study and others with appropriate background, SAI conducted a detailed review of the WASH-1400 Draft which led to the publication of two documents that provide a summary[5] and critique[6] of the Study report. This work then formed the foundation for methodology development aimed at expanding probabilistic risk analysis technology and making risk assessment tasks easier to accomplish. This expanded methodology has subsequently been used to investigate specific areas of concern in risk assessment. The following sections briefly describe the results of the summary and critique of WASH-1400.

2.1 Reactor Safety Study Objectives and Organization

The principal purpose of the Reactor Safety Study was to make a realistic quantitative assessment of the risks to the public from potential accidents at nuclear power plants of the type currently being constructed in the U.S. The Study identified a number of specific objectives necessary to reach this goal. These included the performance of analyses directed toward the quantitative determination of the probabilities and consequences of reactor accidents and the development of a methodology with which to perform these assessments.

The Study was directed by Professor Norman C. Rasmussen of MIT, who reported to the Commission. Mr. Saul Levine of the AEC provided day-to-day internal management. The staff consisted of approximately 50 people, and the project required about two years to complete.

The draft report consists of three sections: (1) a 29-page executive summary[13] in question-and-answer format, (2) a 250-page detailed report[14] which essentially summarizes the work and results, and (3) ten technical appendices[16-27] totaling several thousand pages which document the work done.

The Study covered light water reactors. The two plants analyzed were Surry #1 (PWR) of 788 MWe and Peach Bottom #2 (BWR) of 1065 MWe. The major effort was directed at inadvertent accidents at normal power which involve potential core melt. Sabotage was not considered.

2.2 Conclusions and Recommendations of the Draft Report

The Study concluded that nuclear power plants have a low level of potential accident risk. The probability of core melt for an average reactor was calculated to be 6×10^{-5} per year, based on individual probabilities of 8×10^{-5} per year for the PWR and 4×10^{-5} per year for the BWR. Any one such event has a probability of 1×10^{-9} per reactor year of causing the following consequences:

a.	Acute fatalities	2,300 or more
b.	Acute illnesses (or injuries)	5,600 or more
c.	Long term (cancer) fatalities	3,200 or more
d.	Property damage	$6 billion or more

The study showed that the occurrence of core melt does not necessarily result in large public consequences. Should a core melt occur, the most likely consequences are expected to be a smaller number of fatalities than occasionally occur in commercial jet airplane crashes. Furthermore, core melt was calculated to be less probable than a jet crash event. Comparison of the results of this study with previous conservative work showed the most severe consequences of core melt accidents are about 100 to 1000 times less likely to occur than previously estimated. Furthermore, the most likely consequences of a core melt accident are expected to be 100 to 1000 times smaller than the most severe consequences possible.

An important study result was that core melt due to a large LOCA was determined to be a factor of 10 less probable than core melt from other causes. The study determined the significant contributors to the probability of core melt for the PWR were the small LOCA and transient events, and for the BWR, the transient events followed by failure of the decay heat removal systems. The factors which most affect accident consequences were determined to be: (1) occurrence of the accident, (2) unfavorable weather conditions, and (3) the exposure of a high population density to the released radioactivity.

Finally, the principal results of the study reveal that:

1. Potential core melt accidents do not always result in a severe consequence. They can result in a range of possible consequences with a more likely probability of modest consequences and a low probability of severe consequences.

2. Reactor accident consequences are much smaller than previously believed, and they are smaller than the consequences of many other accidents to which we are already exposed.

3. The probability of reactor accidents is much smaller than the probability of accidents of similar consesequences from other causes, e.g., dam failures.

4. The determination of an acceptable level of risk from nuclear accidents was not addressed in this study; however, it was shown, by implication, that the current level of risk from such accidents is in the region of public acceptability.

2.3 Critique of WASH-1400 (Draft)

The goal of the Reactor Safety Study was to quantify the safety of nuclear reactors, specifically those that had already been through the licensing procedure. One BWR and one PWR were examined. Other reactors or reactor types, such as the HTGR and FBR, were not considered. The conceptual design for these study plants was initiated around 1966 and received the first major licensing review for construction permits shortly thereafter. In the intervening years, many regulations and standards have been developed to upgrade plant design. Additional methods for design review and control have been developed to confirm design adequacy. Because of the subsequent development of these new standards, regulations, and review techniques, the present day nuclear plant receives an even more thorough review during the engineering design and various licensing processes than was possible for the two plants studied. Hence, it seems likely that recently designed plants will expose the public to proportionately less risk than the two plants examined in WASH-1400.

Where possible, the study made realistic (rather than conservative) evaluations; however, conservative evaluations were made when necessary to bound uncertainty. The study did not attempt to quantify the conservatism used in its analysis. Indeed, little sensitivity work was performed to show the effect of variation in significant parameters on the results.

The WASH-1400 report does not make clear how to break down risk contributors. For example, it is important to know whether the major contributors to risk were due to mechanical malfunctions of plant equipment due to intrinsic failure rates, external events, or human interaction (operator error or test and maintenance crew error). This type of information would be valuable in improving future reactor designs, and could also have an impact on maintenance operations and possibly on certain common-mode problems.

Common-mode failure paths were continuously sought, but no systematic procedure for their discovery was developed. More methodology will have to be developed in this area in the future. A computerized component search routine would be valuable for locating components common to more than one system. The study discussed such a capability.

The consequence calculations were done for an average site having an average meteorology and population distribution. Picking one plant and carrying through the individual consequence calculations for that plant on a variety of sites may have been more realistic. In any case, the meteorology and population averaging raises concern when it is claimed to be conservative. Future analysis should be uniquely site-related as well as uniquely plant-related.

Not all of the event trees and fault trees developed by the study were presented in the draft report. Unfortunately, the missing material makes reading and utilizing the report a rather difficult task.

Although the effect of initiating events at multi-unit sites was not specifically addressed in the report, it is expected that such sites and site events can be treated in the same manner as done by the study. There are, of course, factors which may be common to several reactors at a site, e.g., the emergency diesels or the heat sink. External events could also affect several plants simultaneously at a given site. Just how much multi-unit sites may modify the risk estimates presented is unclear.

Population trends around a reactor site are significant since they can change over the 30 to 50-year life of a reactor. Moreover, evacuation may be significant in mitigating the consequences of a reactor accident. Thus, it is essential that population trends be reviewed in detail in a risk study. Hopefully, with some additional effort, a population trend model and an improved evacuation model can be developed for use in future risk assessments for reactors.

The use of "categories" to group the various accident sequences and the "smoothing" of these categories was examined in detail.

The smoothing process increases the probabilities of less probable sequences and increases the total contribution of the more probable sequences. In the smoothing process, 10% of the accident sequence's probability value was placed in each of the adjacent categories, and 1% into each of the categories that are next adjacent, e.g., if category 3 was the assigned release category, 10% of the accident sequence value was added to categories 2 and 4, and 1% to categories 1 and 5. This distribution was intended to account

for the uncertainty involved in placing the sequence in the original category; however, the factor of 0.78 was approximated by unity (1.0) because of the minor change compared to the uncertainties. Therefore, a total of as much as 122% of some accident sequences is contained within the release categories.

Other concerns relating to the use of categories are:

1. Only consequences for large pipe break accidents were generated for the draft report. Similar consequences were inferred for small pipe break and transient events, and these inferred consequences were plotted against the actual small pipe break and transient sequence probabilities.

2. Examination of plots[1] of the fractions of core inventory released versus sequence probability reveals that, for the BWR, sequence definition may be incomplete, or there was little credit given for partial safety system success. This is shown by the fact that no matter what sequence leads to a core meltdown and containment failure, the consequent releases are almost identical.

3. The complete melt assumption leaves a gap between the no-core melt event and the complete core melt event of: (1) five orders of magnitude in inventory fraction release in the BWR, and (2) three orders of magnitude in inventory fraction release in the PWR. Shift of the more extreme points toward lower probability and lower release fractions could result if the binary nature of the melt event is replaced by partial melting, leading to partial releases.

2.4 Changes Included in the Final Report[28] of the Reactor Safety Study

The final version of the Reactor Safety Study report was issued a little more than a year after the draft version. Comments were received during the interim from various federal agencies, environmental groups, groups critical of nuclear power, industrial organizations, architect engineering firms and electric utilities. The comments received were used

in preparation of the final report, and a new appendix, Appendix XI,[26] was added to indicate the Safety Study's response to the comments received. In general, the changes had no significant impact on the result.

For the final version, a more extensive consequence analysis was accomplished, resulting in a new computer code, CONSEQUENCE. This new code has not been released; hence, a detailed examination has not been accomplished. However, the published results reflect little change in resultant consequence predictions. Specific changes in this portion of the analysis include an increase in the number of isotopes considered, from 45 to 54, and a reorganization of BWR sequences to reduce the number of release categories from six to five.

SECTION 3

SENSITIVITY ASSESSMENTS OF REACTOR SAFETY STUDY RESULTS

The results of the Reactor Safety Study presented in the various volumes of WASH-1400 do not provide detailed information which allows understanding of the contribution to risk of plant functions, plant systems, and component groups such as test and maintenance, human error, or various types of hardware. For this reason, a study was undertaken during the first year of this contract to establish sensitivity measures and apply them to the BWR.[1] During the past year, it was discovered that the measures of sensitivity chosen, termed sensitivity indicators, were themselves quite sensitive to round off of the probabilities used in the calculation of the indicators. For this reason, the BWR sensitivity indicators were recalculated along with evaluating for the first time the PWR indicators. The detailed results of this study are reported in Reference 8, and a brief summary follows as Section 3.1 of this report.

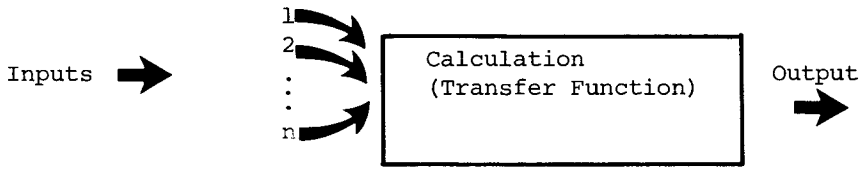
The most important PWR sequence in terms of risk is the interfacing-systems LOCA. This sequence is concerned with the failure of check valves which allow direct release of the primary system outside containment. Because of its importance, a special probabilistic assessment of the system analyzed in WASH-1400 was accomplished by SAI, together with an analysis of other systems proposed by the NRC to help eliminate this risk contributor. Reference 9 examines this problem in detail and is summarized in Section 3.2 of this report.

3.1 Sensitivity Assessment

3.1.1 Development of Sensitivity Indicators

The sensitivity indicators were developed to provide insight into the effect of a change in the value of input parameter on the result of a risk assessment calculation. The basic formulation was taken from control system

analysis techniques as given in Reference 29. In block diagram form, the calculations are the transfer function:



The sensitivity indicator is of the form:

$$I_{\gamma\beta} = \frac{\frac{\Delta\gamma}{\gamma}}{\frac{\Delta\beta}{\beta}} \qquad (3.1)$$

where γ is the dependent variable (output) and β is the independent variable (input).

For all calculations examined in this study, the transfer function can be represented by a linear function:

$$\gamma = f(a)\ f(x) + f(y)$$

In this expression, γ is the output and "a" is a specific independent variable (β) for which the sensitivity of the output is to be determined. The functions f(x) and f(y) represent all other functions of variables which are part of the transfer function but not a function of "a". For this study, "a" is always changed by a multiplication factor, k, and the new result for f(a) is denoted f(a)*.

Thus,

$$\Delta\gamma = f(a)f(x) + f(y) - f(a)^*f(x) + f(y)$$

$$\Delta\beta = a - ka$$

In terms of the general formulation:

$$I_{\gamma\beta} = \frac{\frac{\Delta\gamma}{\gamma}}{\frac{\Delta\beta}{\beta}} = \frac{\frac{f(a)f(x) + f(y) - f(a)^*f(x) + f(y)}{f(a)f(x) + f(y)}}{\frac{a - ka}{a}}$$

$$= \frac{\frac{f(a)f(x) - f(a)^*f(x)}{f(a)f(x) + f(y)}}{1 - k}$$

$$= \left[\frac{f(x)}{f(a)f(x) + f(c)}\right] \left[\frac{f(a) - f(a)^*}{1 - k}\right]$$

The first part of this expression is a constant, so that the general expression could be written:

$$I_{\gamma\beta} = C \frac{f(a) - f(a)^*}{1 - k} \qquad (3.2)$$

If, furthermore, $f(a)^* = kf(a)$, equation 3.2 becomes independent of the proportional change, k, by reducing to:

$$I_{\gamma\beta} = C\, f(a) \qquad (3.3)$$

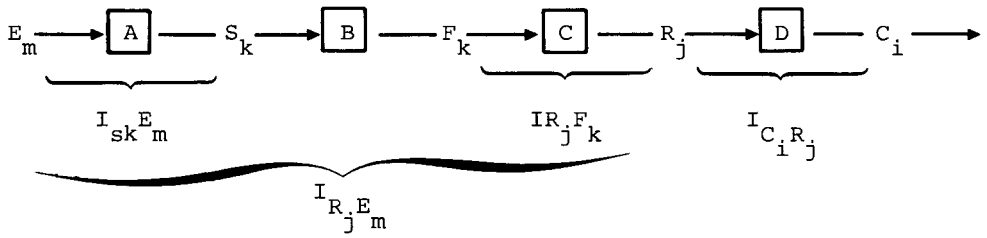
Using the general definition (equation 3.1), three sensitivity indicators were defined and evaluated for the WASH-1400 BWR and PWR:

1. The consequence indicator, $I_{C_iR_i}$, which provides the relative importance of any release category[a] to consequence types[b];

2. The release indicators, $I_{R_jF_k}$ and $I_{R_jE_m}$, which show the release category sensitivity to plant function[c], F_k, availability and event[d], E_m, occurrence; and

3. The system indicator, $I_{S_kE_m}$, which shows the sensitivity of a plant system[e], S_k, to events, E_m.

Two of these, $I_{C_iR_j}$ and $I_{R_jF_k}$, are of the type defined by equation 3.3 and hence, the indicator is constant for all values of input change. Tables 3-1, 3-2, 3-5,and 3-7 (in the following sections) have only one entry for each $I_{\gamma\beta}$ to reflect this fact. The block diagram shown below gives the general relationship between the variables examined. Blocks A through D represent an appropriate transfer function.



Note that any number of indicators could be defined depending on the items of interest.

---

a) Release categories are groupings of accident sequences and are used in this study exactly as defined in WASH-1400[22].

b) Consequence types are specific consequences of accidents such as "Lung Fatalities" and "Thyroid Illnesses".

c) Plant functions are logical combinations of plant safety systems which act to mitigate the consequences of an accident.

d) Events are basic occurrences which affect system operation; examples are hardware failures, testing, human error, etc.

e) Plant systems are specific groups of hardware designed for a specific purpose and designated as a system, e.g., Auxiliary Feedwater System, Low Pressure Injection System, etc.

3.1.2 Sensitivity Indicators for the BWR

The consequence modeling in this study used the same approach as WASH-1400 to compute accident consequences and associated probabilities, except that small modifications to the WASH-1400 draft version of the CONSEQUENCE code were necessary to obtain the consequences for each release category rather than the total for all categories[8].

The transient initiated accident sequences for the BWR account for essentially 100% of the total probability within five out of the six BWR release categories in WASH-1400. These were modeled from the available description of the transient initiated accidents by constructing fault trees for the plant functions W (failure to remove decay heat), C (failure of reactor shutdown system), and QUV (unavailability of make-up inventory of water)[8].

Once the fault trees and appropriate probabilities were obtained, the trees were modeled on the WAM-BAM computer code[30]. (See also Section 4.1 of this report.)

Table 3-1 gives the evaluated consequence indicators for the BWR. This table contains only one entry per indicator as the indicator is of the type defined by equation 3.3.

The integrated effect is largest from release category 4 accidents, while the smallest effect is from accidents in category 6. The dominance of category 4 in the BWR study results from the high probability of occurrence of this class of accident (1.1×10^{-5} per reactor-year) and the relatively large release fractions associated with it.

Using the WAM-BAM code, the effects of changes in the probabilities for plant functions W, C, and QUV for BWR transient-initiated accident sequences were studied. Numerical values for the indicators $I_{R_iF_k}$ and $I_{R_iE_m}$ are shown in Table 3-2. Also shown in Table 3-2 are events for human error and for unavailability due to test and maintenance. Note that the indicator $I_{R_iF_k}$ is constant for all changes in input while $I_{R_iE_m}$ is not; again, equation 3.3 describes $I_{R_iE_k}$. In the case of $I_{R_iE_m}$, the ratio of the changes in E_m is shown along with the resultant indicator value.

TABLE 3-1. Consequence Indications ($I_{ci}R_i$) for the BWR of WASH-1400 (Draft)

	RELEASE CATEGORY, R_i					
Consequence, C_i	1	2	3	4	5	6
50Y WBD Man-Rem	.038	.033	.240	.689	0.	0.
Lung Man-Rem	.053	.033	.276	.639	0.	0.
30D WBD Man-Rem	.046	.037	.201	.714	0.	0.
Thyroid Man-Rem	.034	.040	.102	.824	0.	0.
50Y WBD Fatalities	.017	.098	.189	.696	0.	0.
Lung Fatalities	0.	.095	.264	.640	0.	0.
30D WBD Fatalities	.023	.128	.153	.695	0.	0.
Thyroid Illnesses	.037	.050	.094	.818	0.	0.
Land Cost in Dollars	.030	.037	.293	.634	0.	0.
Evacuation Cost in Dollars	.025	.038	.241	.696	0.	0.
Total Cost in Dollars	.025	.034	.262	.678	0.	0.

TABLE 3-2. Release Indicators ($I_{R_i F_k}$ and I_{RE_m}) for the BWR of WASH-1400 (Draft)

PLANT FUNCTION FAILURE, F_k		RELEASE CATEGORY, R_i			
		1	2	3	4
QUV		0.0228	0.0956	0.0223	0.0264
W		0.7853	0	0.6127	0.9736
C		0.1919	0.9044	0.3650	0
EVENT FAILURE E_m	$\frac{P^*(E_m)}{P(E_m)}$ [a]				
HUMAN ERROR	0.05	0.3476	0.9918	0.4972	0.1829
	0.1	0.3550	1.0266	0.5112	0.1829
	0.5	0.4140	1.3048	0.6235	0.1829
	2.0	0.6353	2.3479	1.0443	0.1829
TEST AND MAINTENANCE	0.05	0.1646	0.1879	1.1554	0.1772
	0.1	0.1650	0.1897	0.1558	0.1777
	0.5	0.1685	0.2041	0.1592	0.1817
	2.0	0.1814	0.2585	0.1718	0.1967
ALL HARDWARE	0.05	0.8366	0.2121	0.6845	1.0053
	0.1	0.8409	0.2145	0.6880	1.0105
	0.5	0.8754	0.2346	0.7158	1.0529
	2.0	1.0091	0.3282	0.8245	1.2169

a) This ratio is part of the denomination of the indicator equation, 3.1; $\frac{\Delta\beta}{\beta} = \frac{P(E_m) - P^*(E_m)}{E_m} = 1 - \frac{P^*(E_m)}{P(E_m)}$

b) On the C tree, the two errors were of order 10^{-6} and 10^{-2} while the ones for W and QUV were of order 10^{-5} and 10^{-3}, respectively.

TABLE 3-3. System Indicators ($I_{S_r E_m}$) for the BWR of WASH-1400 (Draft)

E_m	$\frac{P^*(E_m)}{P(E_m)}$ [a]	System, S_k: QUV	W	C
Active Failures Motor Operated Valves	0.05	0.4307	0.0076	No Change
	0.1	0.4331	0.0076	↓
	0.5	0.4528	0.0076	↓
	2.0	0.5302	0.0076	↓
Passive Failures Motor Operated Valves	0.05	0.0780	0.0076	↓
	0.1	0.0781	0.0076	↓
	0.5	0.0782	0.0076	↓
	2.0	0.0814	0.0076	↓
Pump Failures	0.05	0.2954	0	↓
	0.1	0.2962	0	↓
	0.5	0.3028	0	↓
	2.0	0.3282	0	No Change
Test and Maintenance	0.05	0.9736	0.1557	0.1052
	0.1	0.9926	0.1557	0.1052
	0.5	1.1448	0.1557	0.1052
	2.0	1.7154	0.1557	0.1052
Human Error [b]	0.05	0.5485	0.1730	1.038
	0.1	0.5485	0.1730	1.077
	.5	0.5485	0.1730	1.384
	2.0	0.5485	0.1730	2.537

a) This ratio is part of the denomination of the indicator equation, 3.1; $\frac{\Delta\beta}{\beta} = \frac{P(E_m) - P^*(E_m)}{E_m} = 1 - \frac{P^*(E_m)}{P(E_m)}$

b) On the C tree, the two errors were of order 10^{-6} and 10^{-2} while the ones for W and QUV were of order 10^{-5} and 10^{-3}, respectively.

TABLE 3-4. PWR Systems

Abbreviation	System Name
CSIS	Containment Spray Injection System
B	Electrical Power System
CHRS	Containment Heat Removal System
RPS	Reactor Protection System
AUX FEED	Auxiliary Feedwater
LPRS	Low Pressure Recirculation System
CSRS	Containment Spray Recirculation System
HPIS	High Pressure Injection System
LPIS	Low Pressure Injection System
ACCUM	Accumulator

TABLE 3-5. Consequence Indicators ($I_{ci}R_j$) for the PWR of WASH-1400 (Draft), After Smoothing

	RELEASE CATEGORY, R_j								
Consequence, C_i	1	2	3	4	5	6	7	8	9
50Y WBD Man-Rem	.008	.773	.215	0.	.001	.003	0.	0.	0.
Lung Man-Rem	.010	.762	.225	0.	0.	.002	0.	0.	0.
30D WBD Man-Rem	.009	.787	.198	0.	.001	.004	.001	0.	0.
Thyroid Man-Rem	.007	.829	.145	0.	.002	.015	.001	0.	0.
50Y WBD Fatalities	.007	.761	.231	0.	0.	0.	0.	0.	0.
Lung Fatalities	.003	.665	.332	0.	0.	0.	0.	0.	0.
30D WBD Fatalities	.008	.801	.191	0.	0.	0.	0.	0.	0.
Thyroid Illnesses	.008	.860	.119	0.	.002	.011	.001	0.	0.
Land Cost in Dollars	.008	.860	.131	0.	.001	.001	0.	0.	0.
Evacuation Cost in Dollars	.007	.848	.144	0.	0.	0.	0.	0.	0.
Total Cost in Dollars	.007	.841	.150	0.	.001	0.	0.	0.	0.

TABLE 3-6. Release Indicators ($I_{R_j E_m}$) for Event Failures for the PWR of WASH-1400 (Draft)

Event, E_m	$\frac{P^*(E_m)}{P(E_m)}$[a]	Release Category, R_i						
		1	2	3	4	5	6	7
Human Error	0.05	.291	.050	.747	.737	.620	.297	.454
	0.10	.292	.050	.747	.748	.620	.297	.454
	0.50	.296	.050	.750	.836	.621	.300	.455
	2.00	.313	.052	.761	1.177	.621	.314	.458
Test and Maintenance	0.05	.606	.105	.125	.133	.050	.625	.220
	0.10	.606	.105	.125	.133	.050	.625	.220
	0.50	.606	.105[b]	.129	.139	.050[b]	.625	.220
	2.00	.607	.104[b]	.144	.164	.049[b]	.625	.220
Pumps	0.05	.081	.008	.102	.067	.001	.049	.011
	0.10	.082	.008	.106	.069	.001	.049	.011
	0.50	.093	.009	.134	.086	.001[b]	.050	.011
	2.00	.145	.009	.272	.175	.000[b]	.050	.011

a) This ratio is part of the denomination of the indicator equation, 3.1;

$$\frac{\Delta\beta}{\beta} = \frac{P(E_m) - P^*(E_m)}{E_m} = 1 - \frac{P^*(E_m)}{P(E_m)}$$

b) Apparent decrease due to roundoff prior to calculation of indicators.

TABLE 3-7. Release Indicators ($I_{R_j F_k}$) for Functions - PWR

PLANT FUNCTION FAILURE, F_k	RELEASE CATEGORY, R						
	1	2	3	4	5	6	7
LPIS.∪[a].ACCUM	0.	0.	.0025	0.	.0159	0.	.0187
CSIS.∩[a].(LPIS.∪.ACCUM)	.0003	0.	0.	.2898	0.	0.	0.
HPIS.∩.CHRS	0.	0.	0.	.1055	0.	0.	0.
CSIS.∩.HPIS	.0009	0.	0.	0.	0.	.0012	0.
CSIS.∩.LPIS.∩.CSRS	0.	0.	0.	0.	0.	0.	0.
CSRS.∩.(HPIS.∪.ACCUM)	0.	0.	0.	0.	0.	0.	0.
CSIS	0.	0.	.7193	0.	0.	0.	0.
HPIS.∪.ACCUM	0.	0.	.0063	0.	.0818	0.	.0476
CSIS.∩.(HPIS.∪.ACCUM)	.0003	0.	0.	.6047	0.	0.	0.
B	.0028	.0004	0.	0.	0.	.0027	0.
CHRS	.0261	0.	.0685	0.	0.	0.	0.
RPS	0.	0.	.0207	0.	.0048	0.	.1559
AUX FEED	.9467	.1665	.0501	0.	.0139	.9959	.2263
LPRS	0.	0.	.0558	0.	.6729	0.	.4197
CSRS	.0226	0.	.0593	0.	0.	0.	0.
HPIS	0.	0.	.0170	0.	.2104	0.	.1279
CSRS.∩.LPRS	0.	.0002	0.	0.	0.	.0002	0.
V (LPIS CHECK VALVE)	0.	.8328	0.	0.	0.	0.	0.
R (VESSEL RUPTURE)	0.	0.	.0005	0.	0.	0.	.0028

[a] ∪ = Logical OR
∩ = Logical AND

The analysis for the sensitivity of systems due to changes in the probability of failure of different events is done in a manner similar to that for the release indicators, except that subtrees of the larger fault trees for QUV, W, and C are required. The effects of changes in the failure probability for pumps and for motor-operated valves are presented in Table 3-3 along with human error events and test and maintenance errors. It is seen from Table 3-3 that QUV is most strongly affected by test and maintenance errors, and then with decreasing importance by human error, active failures of motor-operated valves, and pump failures. System W appears not to be dominated by any of the events for the indicators shown. Yet, in Table 3-2 W appeared to be strongly driven by hardware failure in both categories 1 and 4. If one determines the indicator for W by perturbing all the hardware events not shown on Table 3-3, one would obtain the results which are an order of magnitude larger than any in the W column of Table 3-3. Therefore, as suspected, W is strongly dominated by hardware events but not specifically the hardware events involving pumps and motor-operated valves.

3.1.3 Sensitivity Indicators for the PWR

Modeling of the PWR was carried out to the detail of the reduced fault trees in Appendix II of WASH-1400[19] for the systems of Table 3-4. This was necessary as the PWR accident sequences are not as strongly dominated by a small set of sequences as in the BWR case. The systems were combined into sequences, which are grouped into seven core melt categories that correspond to WASH-1400 nomenclature. As with the BWR indicators, $I_{C_i R_j}$ and $I_{R_j F_k}$ are constant for changes in R_j and F_k, respectively.

Table 3-5 gives the consequence indicators for the PWR. As seen in that table, category 2 provides most of the contribution to the consequences with category 3 being of secondary importance.

The release indicators $I_{R_j E_m}$ for PWR categories 1 through 7 were calculated and the results are in Tables 3-6 and 3-7; indicator values for sensitivity to systems are available in Reference 8.

From the sensitivity indicators in Table 3-6, it was found that changes in probabilities for human error most strongly affect releases in

categories 3, 4 and 5, while alterations in test and maintenance failure probabilities are significant for release categories 1 and 6. From the sensitivity indicators, $I_{R_jF_k}$, in Table 3-7, the probability of failure of the Containment Spray Injection System is found to be very significant for releases in category 3, while probabilities affecting the Auxiliary Feedwater System have a pronounced effect on release categories 1 and 6. The Low Pressure Injection System check valve probabilities affect releases in category 2.

Presented in Table 3-8 are the PWR system indicators, $I_{S_iE_m}$, which show system changes due to dominant event changes.

3.1.4 Conclusions

This examination of the two reactors described in the draft version of WASH-1400, shows that sensitivity methods can provide useful information on the makeup of contributors to plant risk and the importance of subsystem failure modes. Specifically, it is noted that human error is not a dominant contributor to plant risk in either the PWR or BWR; rather risk seems to be dominated by hardware failure, with human error playing a secondary role.

3.2 PWR Sensitivity to Alterations in the Interfacing-Systems LOCA

3.2.1 Introduction

The WASH-1400 evaluation of the Surry PWR found that the most influential sequence (relative to consequences) was the Interfacing-Systems LOCA, which was termed V. In an attempt to simplify the risk analysis, however, they approximated their second-order, time-dependent result by a first-order equation allowing for a static risk analysis which was exact at only one point in time, that being when the plant had operated five years.

The "V" sequence is concerned with the failure of any one of the three sets of two check valves which separate the Low Pressure Injection System (LPIS) and the primary coolant lines. Figure 3-1 illustrates this system. Failure of both check valves in one leg results in a LOCA and release of the coolant outside of containment because the LPIS is designed for lower pressure than the primary system and can be expected to rupture.

TABLE 3-8. System Indicators ($I_{S_k E_m}$) for the PWR of WASH-1400 (Draft)

		Systems, S_k									
Events, E_m	$\frac{P^*(E_m)}{P(E_m)}$[a]	CSIS	B	CHRS	RPS	AUX FEED	LPRS	CSRS	HPIS	LDIS	ACCUM
Human Error	0.05	.913	0.	.239	0.	.297	.761	.126	.347	.611	0.
	0.10	.913	0.	.241	0.	.297	.761	.129	.347	.611	0.
	0.50	.913	0.	.259	0.	.300	.761	.148	.348	.611	0.
	2.00	.914	0.	.339	0.	.313	.761	.219	.351	.611	0.
Test and Maintenance	0.05	.071	0.	0.	.344	.627	.025	.532	.054	.025	.391
	0.10	.072	0.	0.	.344	.627	.025	.533	.054	.026	.391
	0.50	.077	0.	0.	.344	.627	.025	.540	.054	.028	.391
	2.00	.095	0.	0.	.344	.627	.025	.567	.054	.034	.391
Pumps	0.05	.016	0.	.518	0.	.049	0.	.888	0.	.006	0.
	0.10	.016	0.	.537	0.	.049	0.	.921	0.	.006	0.
	0.50	.017	0.	.700	0.	.050	0.	1.207	0.	.006	0.
	2.00	.018	0.	1.546	0.	.050	0.	2.544	0.	.007	0.

a) This ration is part of the denomination of the indicator equation, 3.1;

$$\frac{\Delta\beta}{\beta} = \frac{P(E_m) - P^*(E_m)}{E_m} = 1 - \frac{P^*(E_m)}{P(E_m)}$$

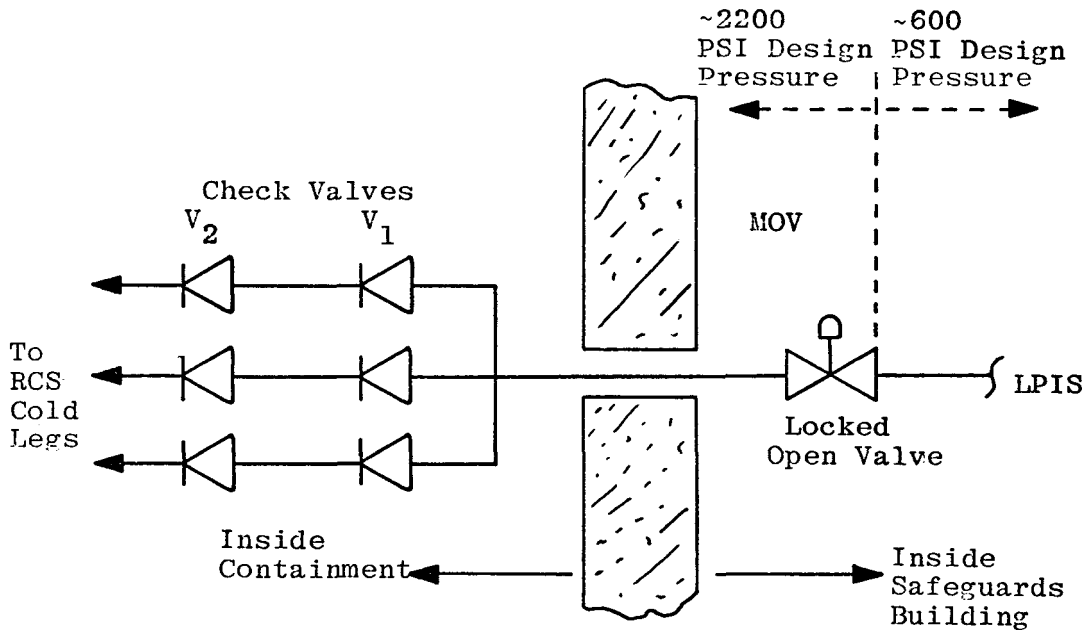


Figure 3-1. Simplified LPIS Check Valve Schematic

While this particular design may not exist in a large number of PWR's, every PWR requires interfacing of low and high pressure systems. This interface is similar to that examined in WASH-1400 in that it utilizes check valves (often in combination with other flow control devices). Thus, the methodologies employed to evaluate this particular interface are also applicable to the evaluation of interface designs at other plants. Reference 9 examines the WASH-1400 configuration in detail and evaluates various other designs as well. Three of these alternate designs appear in the Nuclear Regulatory Commission's Standard Review Plan[31]. A fourth alternative is suggested and analyzed as well.

3.2.2 Comparison of SAI and WASH-1400 Evaluations

Figure 3-2 compares the WASH-1400 and SAI results[9,32] for one set of two check valves. As can be seen, the WASH-1400 quadratic approximation is in excellent agreement with the SAI result over the normal life (0 to 40 years) of the plant. However, WASH-1400 took the five year result and divided by five in order to normalize the result on a per-year basis. The final result was a linear estimate for the event probability which overestimates from zero to five years, but underestimates for greater than five years. Perhaps a better method of obtaining a linear estimate is to choose it so as to have an average value between 0 and 40 years equal to the average value (0 to 40 years) of the exact solution. This would have resulted in an estimate of 5.8×10^{-6} per year instead of the 1.3×10^{-6} per year (per set of two valves) estimate used in WASH-1400. Of course, the time period should be shorter if it is known that a design change will be implemented at some future time in plant life which will reduce the check valve contribution to insignificance.

3.2.3 Evaluation of Alternate Designs

A list of designs acceptable to NRC, intended to reduce the risk of an interfacing-system LOCA, is provided in NRC's recently-issued Standard Review Plan[31]. The following is an excerpt from Section 6.3, "Emergency Core Cooling System", of that document. A similar description also appears in Section 5.4.7 on the "Residual Heat Removal Systems".

> "The design of ECCS injection lines is reviewed to confirm that the isolation provisions at the interface with the

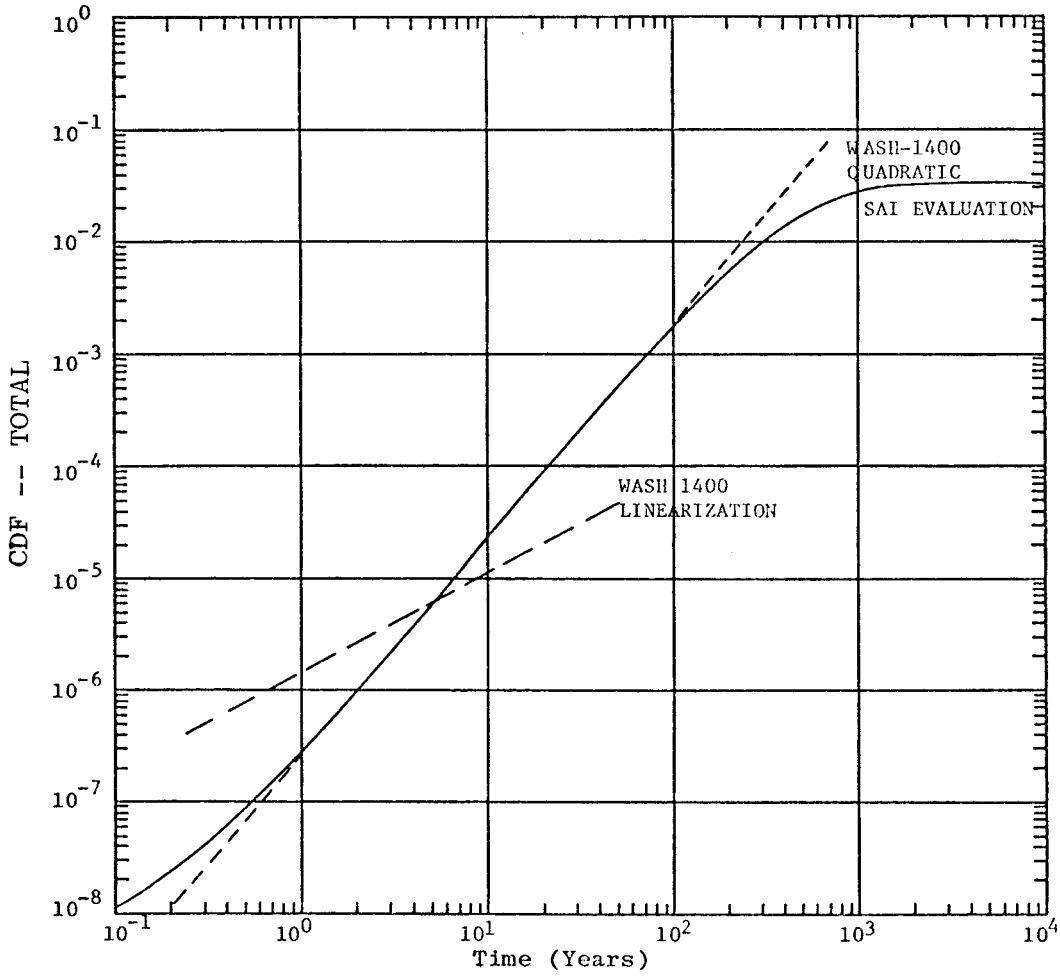


Figure 3-2. Cumulative Failure Distribution Function for Two Check Valves with Four Shutdowns per Year

reactor coolant system are adequate. The number and type of valves used to form the interface between low pressure portions of the ECCS and the reactor coolant system must provide adequate assurance that the ECCS will not be subjected to a pressure greater than its design pressure. This may be accomplished by any of the following provisions:

a. One or more check valves in series with normally closed motor-operated valve. The motor-operated valve is to be opened upon receipt of a safety injection signal once the reactor coolant pressure has decreased below the ECCS design pressure.

b. Three check valves in series.

c. Two check valves in series, provided that there are design provisions to permit periodic testing of the check valves for leaktightness and the testing is performed at least annually."

The implication of presenting alternatives is they each provide probabilistically-acceptable designs.

The three options can be compared by examining their 40-year linearized estimates determined using the methodology discussed in Reference 9. These linearized estimates are:

a. 1.9×10^{-5} per year
b. 4.5×10^{-7} per year
c. 5.5×10^{-9} per year

The somewhat surprising result is that the option of two check valves with test (option c) is almost two orders of magnitude better than three check valves (option b). However, if the designer assumes that each option is equally acceptable, he will most likely choose the most cost-effective option. Thus, the most reliable system may not be chosen.

3.2.4 Alternate Designs

The analysis of the two check valve and three check valve systems suggests other design options. Reference 9 shows that the "leak" failure mode in check valves is much more significant than the "(disk) rupture" failure mode. Thus, elimination of the leak failure mode would greatly

reduce the probability of an interfacing-systems LOCA. If a reduction of the rupture mode probability was also accomplished, the probability of an interfacing-system LOCA could be minimized (or reduced to insignificance). As an example, instrumentation could be added to the two check valve systems which would indicate: (1) the seated (or unseated) condition of each check valve (on a continuous basis), and (2) the existence of ruptured check valve disks (at shutdown). Assuming four shutdowns per year, such a system would have a 40-year linear probability estimate of 4.1×10^{-12} per year for an interfacing system LOCA.

3.2.5 Conclusions

The WASH-1400 report correctly identified the importance of the interfacing-system LOCA to the total PWR risk. The Nuclear Regulatory Commission has recognized the need to properly design against an interfacing-system LOCA and has given three options for the design of interfaces between high and low pressure systems in the Standard Review Plan. However, rigorous analysis of these options shows they are not probabilistically equivalent. Furthermore, the analysis herein described points out the key failure modes, thus directing the designer to a design which is probabilistically much better.

While the solution of this problem is important in itself, the result also demonstrates the need to perform complete analyses in order to make the design constraints on important systems precise.

SECTION 4

COMPUTER CODE ASSESSMENT AND DEVELOPMENT

The Reactor Safety Study utilized several computer codes in the accomplishment of the study. Some of these codes existed, some were derived from existing codes; and some were developed during the course of the study. Included in the effort of these past two years at SAI were tasks to make operational the codes utilized on the Reactor Safety Study and to investigate other existing codes which have potential use to risk analysis. Following this investigation effort, codes were developed to implement advanced methodology in the specific analysis areas found lacking.

Two types of codes have been investigated; namely, probabilistic system analysis codes and codes which predict core inventory release and the consequences of releases for specific accidents. The following sections discuss the work to date on the codes relating to these areas. In developing and implementing advanced technology in these areas, SAI has developed the capability to quickly and efficiently perform a complex risk analysis in its various aspects.

4.1 Probabilistic Assessment Methodology and Code Development

Part of the detailed examination of WASH-1400 included examination of the probabilistic assessment methodology of the Reactor Safety Study. It was found that the basic methodology was not a limitation, but its full capabilities were not utilized. Basically, this limitation can be traced to limitations in the computer codes employed. These codes could not evaluate the logical, probabilistic models (fault trees and event trees) that modeled all the complex relationships within and between systems. Because complex systems require the evaluation of complex models, considerable effort has been expended in developing a code, WAM-BAM, which can evaluate a complex model, providing a point estimate for the top event.

Following the development of this code, it seemed desirable to develop the ability to qualitatively evaluate these same complex models, and furthermore develop methodology and a code to calculate the effect on the top event of data uncertainty. The WAM-CUT code has been developed to provide the qualitative evaluation requirement, and work is in progress to add to WAM-CUT the ability to calculate top event uncertainty.

The following sections review the development of WAM-BAM as described in References 30 and 33 and present the work to date on WAM-CUT.

4.1.1 WAM-BAM Development

The WAM-BAM code development can be described in three steps: (1) development of specific requirements, (2) development of the mathematics and implementation in a code, and (3) comparison of WAM-BAM to those codes used on the Reactor Safety Study.

The new code developed incorporates many features of existing codes. Development of the new code was accomplished by: (1) evaluation of existing codes and the methdologies they employ, and (2) evolution of a new code which handles the type of problems encountered in the Reactor Safety Study.

The numerical evaluation program called BAM* utilizes basic Boolean techniques as in the GO[34] computer code. The preprocessor, WAM**, is designed to ease the amount of user effort required in modeling a system. It is similar to that used in PREP-KITT[35]. This code is more completely documented in a users manual[33].

Principles of the BAM Computer Code

The BAM code uses Boolean algebra minimization techniques to find the resultant logic expressions from an input tree and then calculates the associated point unavailability. BAM first forms all possible combinations

---

*Boolean Arithmetic Model
**WAM is not an acronym

of events and then forms a truth table that describes each event and gate as a function of these combinations. This basic methodology is computationally optimized based on techniques used in the GO computer code.

Fault tree construction in WASH-1400 employed AND or OR logic operations (called gates). In addition, the INHIBIT gate, which acts as a switch to turn on specific logic when a conditional input is satisfied, was also utilized. The basic events identified in these fault trees correspond to independent events for the purpose of quantification. Dependent conditions are bounded and otherwise approximated by modification of the assigned probability values.

BAM allows for additional modeling capabilities by incorporation of the NOT operation capability with the use of AND and OR gates. This extension allows all of the sixteen logical operations for two variables to be included. The inclusion of NOT gates makes possible the explicit modeling of dependent events, including disjoint events and common-mode events.

SAI has used BAM to quantify fault trees developed on the Reactor Safety Study as well as other examples to ascertain the code's capabilities and limitations[30]. These studies show that BAM is capable of quantifying completely integrated detailed accident logic sequences which include common mode, dependent and disjoint events. Thus, parametric and sensitivity investigations of sequence probability can be accomplished to assess the impact of: (1) changing assumed independent events to dependent events, and (2) variations in event probabilities.

Capabilities of the Pre-Processor (WAM)

A preprocessor for BAM, named WAM, has been developed to allow a system analyst to easily communicate with the BAM code. WAM accepts the logical tree with components and gates input with alphanumeric names and allows up to 8 inputs for AND and OR gates. A cross reference list is generated which shows the total number of gates and the specific gates for which each component is an input. Many checks are performed to advise the user of mistakes in his model, and the input of BAM is optimized to reduce the running time and maximize result accuracy. The preprocessor also allows the input of combinational failures, i.e.,when a system fails because at

least N of M branches fail, the input to WAM is the names of all the "M" branches and how many (N) must fail to fail the system. Up to eight branches are allowed.

Event Probability Preprocessor - WAMTAP

At the user's option, the input to BAM can be saved from a WAM run and subsequently called by WAMTAP. WAMTAP allows probabilities to be changed for specified components, or group of components identified by common alpha-numeric characters in the component name. For example, if the event code used letters "HE" as the first two letters of every Human Error component, WAMTAP could search for these and change the failure rate for each component starting with "HE" by a multiplication factor or set them to a specific value, then re-evaluate the tree via the BAM code. Such a capability allows sensitivity studies or common-mode studies to be easily accomplished.

4.1.2 Comparison of Logic Sequence Codes

A comparison study was made with a simple example problem using PREP-KITT[35], SAMPLE[36], GO[34] and BAM programs.

The four computer codes give similar results for the system evaluated as indicated in Table 4-1. Each computer code requires a thorough understanding of the system, the system description for use by the computer code (fault tree, GO chart,or Boolean expression), and the specific type of results desired. It was found that after having this knowledge, the study proceeded in a straightforward manner. The input probabilities to PREP-KITT, GO,and BAM utilized the component medians as point estimates rather than means, thus exact agreement with SAMPLE could not be expected.

TABLE 4-1. Fault Tree Computer Code Results

CODE	SYSTEM UNAVAILABILITY (PER DEMAND)
PREP-KITT	2.32×10^{-3} (asymptotic)
GO	2.32×10^{-3} (minimum cutoff - 10^{-13} per demand)
BAM	2.32×10^{-3} (minimum cutoff - 10^{-13} per demand)
SAMPLE	3.11×10^{-3} mean
	2.81×10^{-3} median
	1.40×10^{-3} standard deviation
	1.53×10^{-3} to 5.76×10^{-3} (90% confidence interval)

The PREP-KITT code in conjunction with fault trees offers a method by which one can partially check his work. The resulting minimal cut sets can be checked using the fault tree. For large and highly redundant systems, however, it becomes increasingly difficult to obtain these minimal cut sets. One is normally not able, with PREP-KITT, to compute cut sets of four or more components in these systems due to the amount of computer time required. In any event, the contribution from cut sets of more than three components is not important in many cases since the contribution from a minimal cut set is proportional to the n^{th} power of its component probabilities (where n is the number of components in the cut set).

The SAMPLE program evaluates an arithmetic probability expression which represents the system logic. It is convenient to first make a PREP run to determine the minimal cut sets for developing the arithmetic expression. The arithmetic expression can then be approximated as the sum of the significant minimal cut sets' probabilities.

The GO program provides results consistent with the other calculations. The main disadvantage appears to be the transformation of the system diagram into the GO chart. This task requires particular attention since one cannot check the resultant schematic against other factors. The user must follow not only the logic of the system, but also the logic limitations and procedures for constructing the GO chart.

The BAM code offers an attractive alternative since it employs the computational techniques used in GO and is constructed to input the system

logic strictly from fault trees containing any possible logical operation. The GO code has the capability of describing AND and OR operations between two events and thus can be used to model fault trees containing these operations. Confidence in the analysis of this simple example using GO and the GO chart was enhanced by also evaluating the system using a fault tree.

During the computation of the system unavailability characteristics, the computational techniques used in GO, and BAM do have some advantages over the PREP-KITT analysis. Instead of first requiring the calculation of minimal cut or path sets, GO, and BAM solve the entire system while dropping events that are below a user specified level of significance.

KITT-1, however, provides the time dependent reliability characteristics of the system whereas SAMPLE, GO and BAM cannot give time dependent results except by repeated runs. (WAMTAP could be useful for this.) SAMPLE gives, in addition, a confidence interval for the point estimate for an assumed distribution of the component reliability data. Since SAMPLE requires that a representative arithmetic expression for the system logic be input, further work is necessary to extend the ability to calculate confidence intervals of more complex systems.

4.1.3 Cut Set Code Development

In order to allow qualitative analysis of a fault tree and provide a formulation of the fault tree most easily transformed into a probability polynomial, an efficient cut-set code was sought. First, the most promising codes were examined, and then, when found insufficient, a better cut-set code was developed.

Development of WAM-CUT

The code WAM-CUT was developed to fill the need for faster identification of minimal cut sets in large fault trees. It was conceived after an examination of existing cut set codes revealed several shortcomings in the area of cost and flexibility. The existing codes, MOCUS[37] and ALLCUTS[38] accept only AND, OR, and INHIBIT gate types which limit the flexibility of the system analyst utilizing fault tree methodology. The number of events per cut set is limited to ten, and the cost rises exponentially with any

number greater than three in the case of MOCUS. WAM-CUT, on the other hand, accepts the same input as the WAM-BAM code and is able to solve large trees which, if solved by MOCUS, would require either an indeterminable amount of computer time or much hand work reducing the tree into numerous subtrees to be solved separately.

The MOCUS code was examined in considerable detail to determine its usefulness for large trees.* When it was found lacking, a new algorithm was developed based on the MOCUS algorithm "inverted". Briefly, MOCUS works from the top gate down the tree resolving each gate into its inputs, adding cut sets if it is an OR gate and adding events to a cut set if it is an AND gate until all the gates have been resolved into primary events. Tests are made at several points in this process to delete duplicate events in a cut set and to delete sets that are subsets of others. WAM-CUT works from the bottom up forming the cut sets of a gate from the cut sets of its inputs until the top gate is reached. Duplicates, supersets, and cut sets whose probability is less than a specified minimum are deleted as the set is being built.

Description of WAM-CUT

WAM is the same preprocessor used in WAM-BAM to check the input fault tree for errors and to resolve all the gates into gates with only two inputs each.

If the input is error free, NEWTREE is called to resolve all gate types into AND or OR gates using their Boolean relationships to accomplish this. NEWTREE operates in either of two modes specified by an input switch. Under mode 1 all of the NOTs are rippled down through the tree to the components resulting in the creation of new components which are the NOTs of the input components. This "rippling" process makes use of the following Boolean algebra identities.

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Figure 4-1 illustrates this process.

*The ALLCUTS code was not examined in this detail since the code itself was not available.

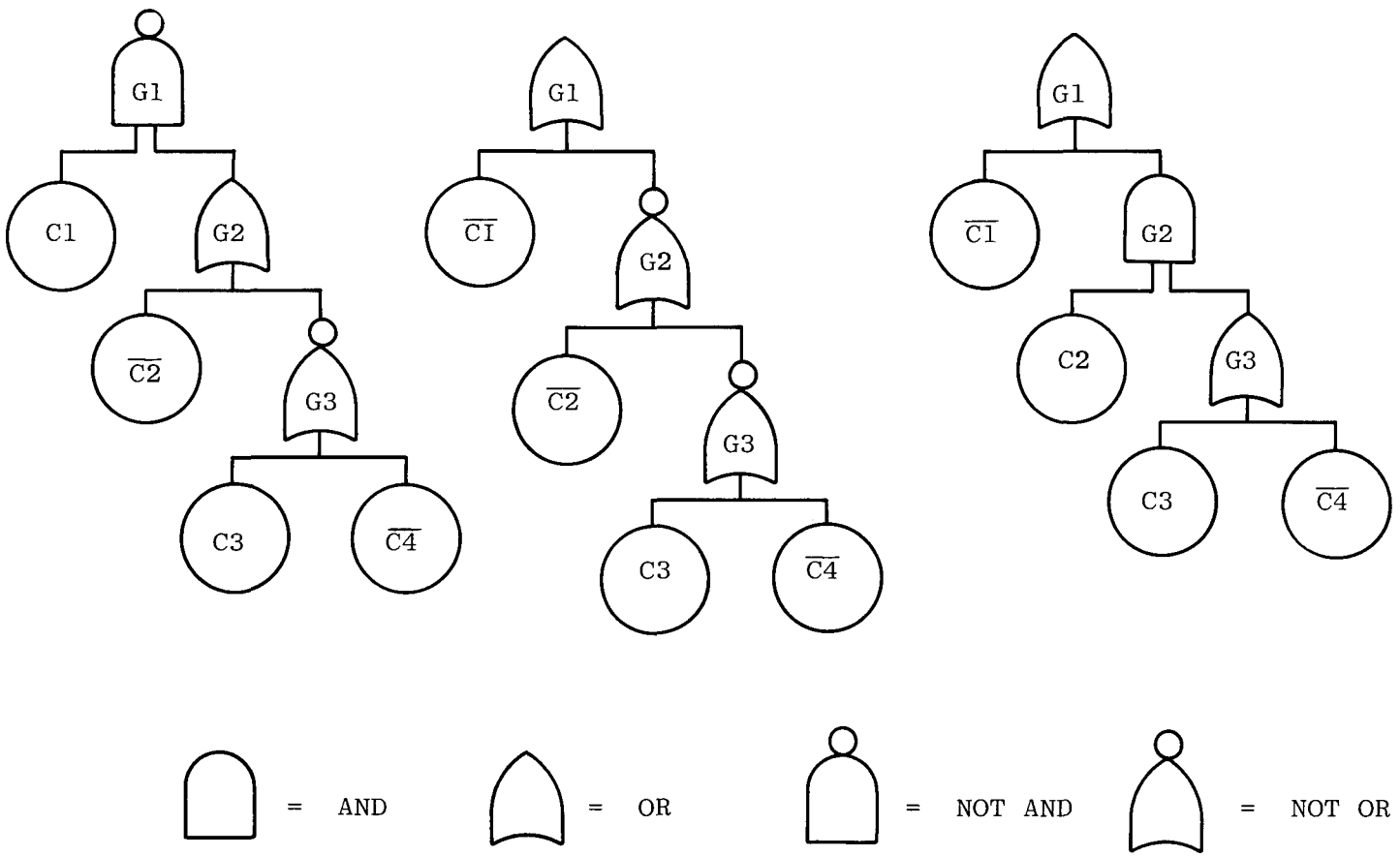


Figure 4-1. Example of Rippling NOT Gates TO Components

Under mode 2, whenever a NOT gate is encountered, a pseudo-component is created and included in the tree in place of the NOT gate. A probability of 1.0 is assigned and from this point on the pseudo-component is treated as a component. This effectively prunes the tree by deleting branches with probabilities smaller than a user-defined minimum. Thus, branches with small probabilities are deleted without the time-consuming process of finding all the cut sets first. Fault trees with only a few NOT gates can be processed using mode 2 to prune the tree and to determine which NOTed gates are needed for the final resolution. If no pseudo-components (NOTed gates) appear in the final cut sets, all have been pruned from the tree and the problem is finished. If pseudo-components do appear, the cut sets of these gates will also be printed and a new tree must be constructed from these cut sets and the revised tree processed using mode 1 to determine the final cut sets.

CUT is called by NEWTREE after all gates have been converted to AND or OR gates and the new components created. CUT then begins with a bottom gate, a gate with only components as input, and works up the tree forming the cut sets of a gate from the cut sets of its inputs until the top gate is reached.

OREM, ANDEM, SQUASH,and PRCUT are called by CUT at various points in the cut set building process. OREM ORs the cut sets of two gates. ANDEM ANDs the cut sets of two gates. SQUASH checks the cut sets of a gate for duplicates, supersets, probabilities less than the minimum, and cut sets containing a component with its NOT after which sets or components are deleted where applicable. PRCUT prints the cut sets of the gates specified by the input as well as the gates which appear as pseudo-components if mode 2 is used.

4.1.4 Comparison of Cut Set Codes

Caution should be exercised when determining cut sets of a tree with many NOT gates since the number of cut sets and the number of components per cut set can be quite large. WAM-CUT can currently handle up to forty components per cut set and fifteen hundred cut sets per gate. The concern is whether this much information, once it has been determined, is needed for system evaluation.

The basic drawback of WAM-CUT is that it is not system independent. It must be exercised on a computer system with approximately 63,000 words of directly addressible large core memory in addition to the 65,000 words of small core memory required for code and data storage. There is no readily apparent way to overcome this handicap. Also, computer systems with high I/O charges would increase the cost of running WAM-CUT considerably since data is constantly shuffled in and out of small core memory during the cut set determination process. The code is currently programmed on a CDC 7600 computer.

Two fault trees were processed by WAM-CUT, MOCUS, and BAM. The timing comparisons appear in Table 4-2 below.

Table 4-2

Fault tree size # of gates	# of components	Min. Prob. for WAM-CUT	BAM run time (secs)	MOCUS run time (secs)	WAM-CUT run time (secs)
39	23	0	1.600	1.507	0.558
39	23	10^{-10}			0.367
39	23	10^{-8}			0.135
187	124	10^{-5}	13.1	$3x10^{11}$ (estimated)	34.4

The WAM-CUT time for the larger tree is the sum of two passes through the code. Since this tree contained many NOT gates, it was first necessary to prune the tree (5.8 sec) and construct a new tree from the cut sets resulting from the first pass before the final cut sets could be determined.

4.1.5 Future Code Development

Numerical Evaluation of Cut-Sets

The cut-sets which represent the fault tree are elements of the Boolean expression for the system. Thus, numerical evaluation cannot be accomplished directly from the cut sets, except as an approximation. The mean of the top event can be approximated by forming the product of the means of the components in each cut set, then summing these products. This approximation assumes that the intersection of the various cut sets is small.

Another approach is to form the algebraic polynomial representing the system from the cut sets taking into account these intersections. This polynomial can then be used to calculate either the top event moments (and thus the mean and standard deviation) from event moments or as the model in a Monte Carlo simulation. Formation of the polynomial will be the next step in the development of the WAM-CUT computer code.

Automatic Fault Tree Drafting

To complete the WAM series of fault tree codes, a WAM-DRAW is being considered. This code will use the same input such as WAM-BAM and WAM-CUT, but its output will be a drawing of the fault tree. This will save drafting of large trees for reports and provide a check of the input tree vs the system analyst's model.

4.2 SAI Accident Consequence Calculations

A major portion of risk assessment is concerned with determining the consequences of the various accidents which can occur. As a first step in building this capability, the CONSEQUENCE computer code, developed by the Reactor Safety Study and used to produce the results presented in Appendix VI of WASH-1400[23], was obtained and made operational. Some of the consequence calculations in WASH-1400 were redone using the same parameters which were used for the Safety Study and, because of the elimination of several programming errors, the results differed modestly from those presented in the draft version of WASH-1400. The differences observed were not sufficient to change the basic conclusions of the Safety Study.

In addition to repeating some of the WASH-1400 calculations, considerable information was obtained from additional computer runs. The probability distributions for the occurrence of each of several accident consequences were obtained not only for a typical PWR and BWR, but also for each of the nine PWR and six BWR release categories defined in WASH-1400. This additional information, not included in WASH-1400, can be used to better identify accident sequences whose probability of occurrence should be reduced by additional engineering design as well as those whose probability of occurrence is already sufficiently low.

It would be desirable to obtain the updated version of the CONSEQUENCE code from NRC; however, they have not yet made this code available. The draft CONSEQUENCE code, used as described above, has been the subject of criticism by SAI and others; nevertheless, we believe that the general trends and relative magnitudes will not change drastically when improved consequence models are available. In the future, the CONSEQUENCE code will be used to support further risk assessment which will include evaluation of site-specific consequences rather than for an "average" site as done on the Reactor Safety Study.

Included in subsequent sections are example probability distributions (PWR and BWR 50-Year Whole Body Dose) for specific consequences (average site) as obtained from the SAI-modified CONSEQUENCE code. A complete set of figures showing all the accident consequences listed below can be found in Reference 1:

1. Fifty-year (essentially infinite) whole body dose
2. Lung dose
3. Thirty day whole body dose
4. Thyroid dose
5. Fatalities from fifty-year whole body dose
6. Fatalities from lung dose
7. Fatalities from thirty-day whole body dose
8. Fatalities from thyroid dose
9. Land cost
10. Evacuation cost (including relocation cost)
11. Total cost

Other outputs, e.g., genetic effects, can be calculated if the need arises.

4.2.1 PWR Accident Consequence Probabilities

An example cumulative probability distribution of accident consequences is shown in Figure 4-2. In this figure, the number on each curve designates the release category and the symbol "T" designates the total for all categories. The curve was drawn by a plotting subroutine which was linked to the CONSEQUENCE code. The results were extrapolated to the left and right to make certain that no significant structural changes occurred at either

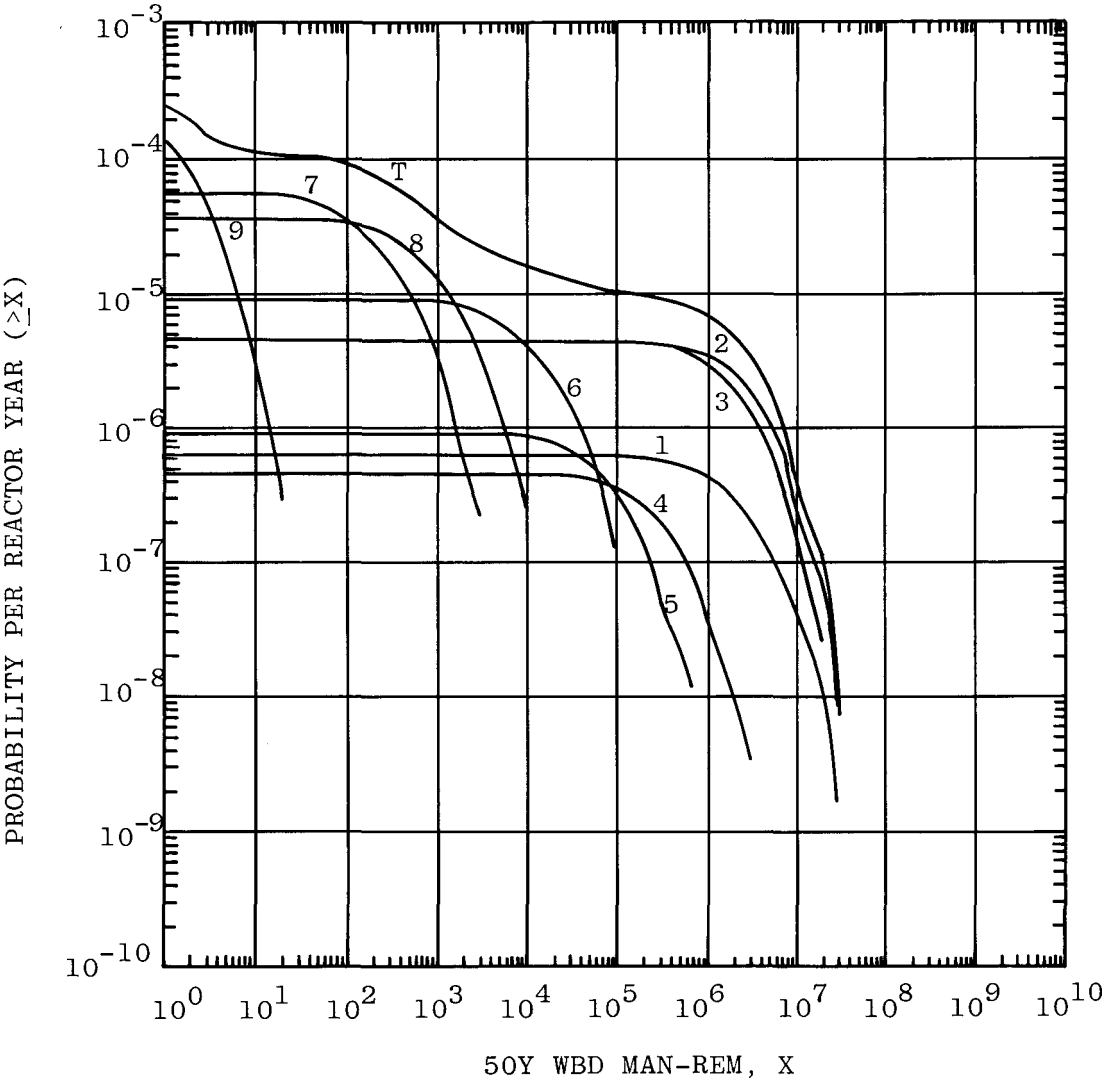


Figure 4-2. Probability Distribution of 50 Year Whole Body Dose from PWR Accidents

Note: Numbers on the curves designate release categories and "T" designates the total for all categories.

extremity which might be sufficient reason to re-examine the basis for the WASH-1400 conclusions.

Although the shapes of the distributions differ for the various consequence types, some features are common to all. For PWR accidents, releases in categories 2 or 3 are the most likely to cause the very large consequences. (Given a category 1 release, the consequences are larger; however, the total consequences of category 1 accidents are smaller than the total for category 2 because accidents in category 1 are less probable and they are predicted to result in releases at an elevation of 25 meters.) Accidents with relatively small consequences are probabilistically most likely, and result from category 9 release.

Since these data are generated after the category results were "smoothed"* by mixing 10% in the adjacent and 1% in second nearest neighbor categories, the corresponding accident sequence curves based on raw data may be different. The breakdown of the cumulative (T) curve is possible either by categories (as shown in Figure 4-1) or by accident sequences. For example, in Figure 4-1, it can be seen that T is dominated, progressively from left to right, by the categories 9, 7, 8, 6, 2, 3 and 1. Hence, it should be possible to learn which accident sequence contributes to a given impact and to what extent it contributes.

The probability density function for each type of consequence was obtained by numerically differentiating the cumulative probability distributions. These curves* are normalized so that the area under each is the probability of fission product release (source term) for the corresponding accident category. The density function predicts large consequences (with small probabilities) for the low-numbered release categories and small consequences (with larger probabilities) for the high-numbered release categories. The probability density functions for other accident consequences show similar trends. No effort was made to smooth the curves. Rather, we are seeking to determine the reasons for the occasionally erratic behavior of the probability density function obtained from the analysis of the CONSEQUENCE code results.

---

*Section 2.2.1 of this report contains a description of the smoothing technique.

4.2.2 BWR Accident Consequence Probabilities

An example cumulative probability distribution for the BWR release categories is shown in Figure 4-3. Large consequences are most likely to result from category 4 accidents, while small consequences are most likely from accident of category 6. The dominance of category 4 in the BWR study results from the high probability of occurrence of this accident (3×10^{-5} per reactor-year) and the relatively large release fractions associated with it.

In Figure 4-3, we observe that the density function shapes for release categories 1 through 5 are almost identical except for normalization. In other words, given a release of category 1, 2, 3, 4 or 5, the CONSEQUENCE code predicts the same 50-year whole body dose for each release. Density functions for other consequences show similar behavior. This result is different from that for PWR release consequences, and should probably be examined more carefully.

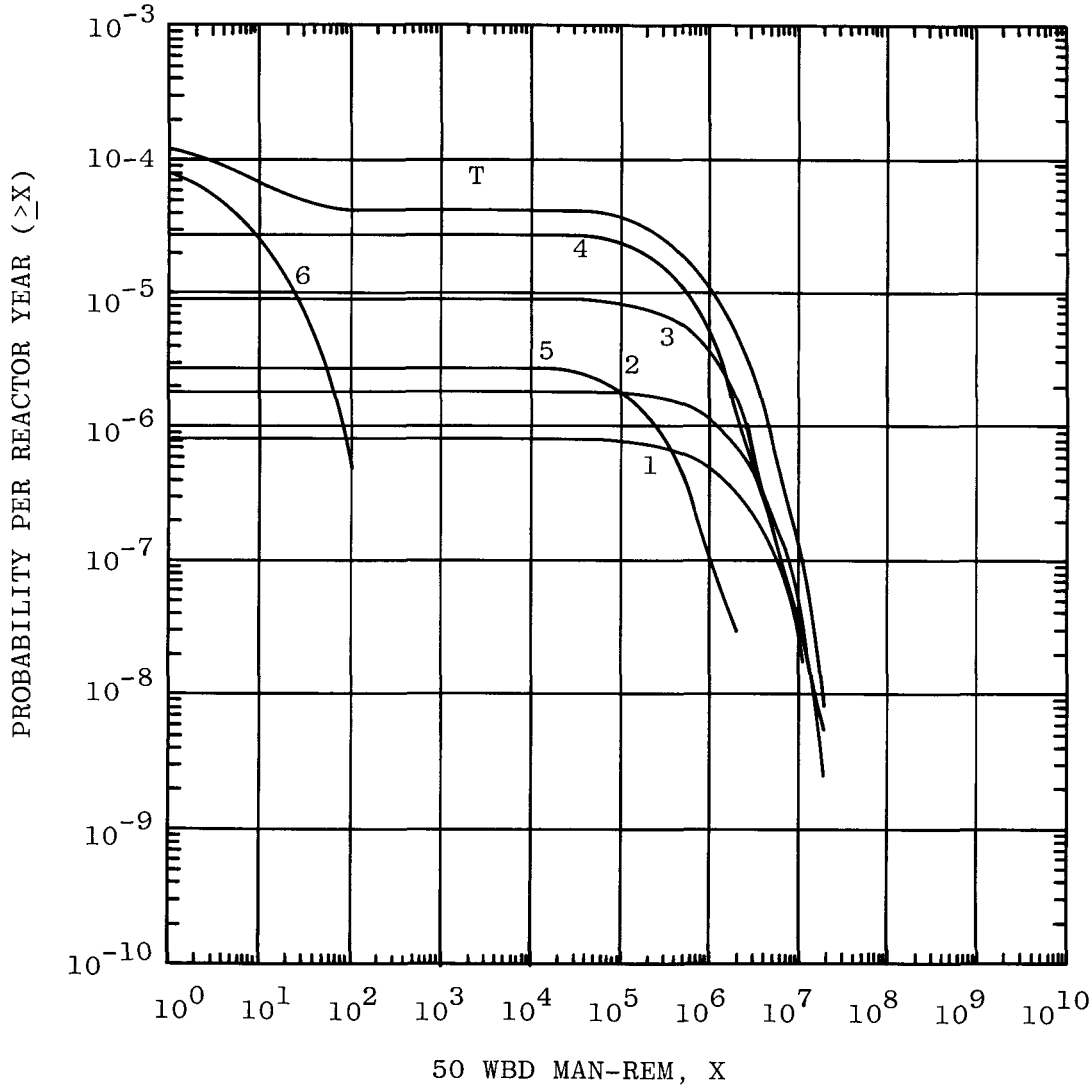


Figure 4-3. Probability Distribution of 50 Year Whole Body Dose From BWR Accidents

Note: Numbers on the curves designate release categories and "T" designates the total for all categories.

SECTION 5

EVENT TREE DEVELOPMENT FOR A LARGE PWR

5.1 Objective

The initial overall goal of this analysis was to examine the utility of event tree methodology as a generic tool for application in risk assessments of large and complex high-technology systems such as nuclear power plants. This goal was defined by three specific interdependent objectives: (1) to develop a set of event trees for a large PWR that could be compared, at the level of accident sequences, with the event trees for the Surry PWR in WASH-1400[16]; (2) to examine the problems and difficulties involved in constructing and evaluating such event trees*; and (3) to determine the types and quantities of detailed plant information required for the construction of these trees. The work proceeded concurrently toward all three objectives.

5.2 Preliminary Event Trees Developed for the Selected PWR

The objective was approached in a realistic manner by the selection of a particular PWR for analysis which is different in several respects from the Surry plant. The selected PWR is a four-loop design (versus the three-loop design of Surry). The plant is larger (>1000 MWe versus 788 MWe) and contains a different set of engineered safeguard features (ESFs) with which to respond to accidents. These differences, coupled with the use early in the analysis of an out-of-date Final Safety Analysis Report (FSAR) for the selected PWR, caused some difficulties in the analysis. A more complete FSAR was obtained near the end of the analysis and changes which affected earlier work were largely incorporated into the material included herein.

The event trees which are developed in this report have not been evaluated. Neither the substitution of systems into functional event trees

*Event trees, like fault trees, may be evaluated qualitatively and/or quantitatively if sufficient data is available.

nor the evaluation of these systems is a straightforward task. Although the substitution of systems for functions in two of the LOCA event trees was accomplished, some changes may be required if additional details of information change the basis of the initial substitutions. System evaluations may be even more difficult due to the necessity of defining system success (or failure) in terms of specific hardware operation (or non-operation) and the need to have access to detailed drawings of system designs which are not included in the FSAR. Other necessary information not included in the FSAR includes the details of items such as procedures for test and maintenance operations, emergencies, various operational situations, etc. Nevertheless, it should be possible to make rough approximations on the basis of information which is available. This has been done to some extent, but the task was not completed. In addition, at some point in the future, separation of the problems of core melt and containment failure, so that the various failure modes of the containment can be treated separately, is intended.

5.2.1 Functional Event Trees and System Interrelationships

An examination of the functional requirements for LOCA-type initiating events for the Surry plant, when compared to the functional requirements to reach a safe shutdown in the selected PWR, reveals that the two plants are identical in the functional sense. Figures* 5-1 and 5-2,extracted from WASH-1400, show functional event trees for the large and small LOCA events in their final reduced form. Numerous sequences have been eliminated in the process of tree construction due to the existence of functional interrelationships which cause the eliminated sequences to become impossible, illogical, or of no consequence. The functional events shown in these trees are defined in Table 5.1.

In order to develop more meaningful event trees, it is necessary to incorporate the specifics of individual plants into the trees by defining the systems used to perform the required functions and substituting. In this process, it is also necessary to account for interrelationships between the various systems. When this was done for the LOCA event tree in WASH-1400,

*All figures and tables in this section are presented at the end of the section for the convenience of the reader.

the result was Table 5-2, which also indicates the three LOCA sizes which were separately considered. A similar analysis has been accomplished for the selected PWR. The results, shown in Table 5-3, are discussed in the following paragraphs. Table 5-4 provides a comparison of ECI success requirements for the two plants in terms of hardware.

5.2.2 System Event Trees

Preliminary event trees have been developed by SAI for two LOCA events in the selected PWR, with due consideration given to the specific design of the ESF systems and the detailed analyses presented in the FSAR. These event trees are shown in Figures 5-3 and 5-4. Descriptions of the individual sequences in these figures are provided in Tables 5-5 and 5-6, respectively. It is noted that the containment integrity (CI) event has been retained in these trees and that emergency core cooling functionability (ECF) and sodium hydroxide addition (SHA) are not included as they are in the event trees for the WASH-1400 PWR. The specific event trees for each of the three LOCA sizes developed in WASH-1400 (for Unit 1 of the Surrey Power Station) are included in this report as the appendix to Section 5.

The ECF* event in the large LOCA event tree, which is discussed in WASH-1400, has been intentionally excluded from the SAI event trees. The additional conservation factor which this event contributes to the large LOCA evaluation is considered unnecessary, and, in any case, made no significant contribution to the final WASH-1400 consequences.

The sodium hydroxide addition event, although shown in the WASH-1400 event trees, was actually not a significant contributor to final consequences. In fact, SHA is described in WASH-1400 as a beneficial factor which improves the efficiency of the containment spray system in removing iodine from the containment atmosphere. The spray, without sodium hydroxide, is a satisfactory iodine removal mechanism. For that reason, SHA has not been included in these preliminary event trees.

---

* ECF is concerned with failures in the reactor coolant system caused by LOCA blowdown forces which could adversely affect ECCS performance, e.g., excessive core bypass flow due to structural failure of the core shroud.

The design of the systems in the selected PWR which remove heat from the containment atmosphere and from water collected in the containment sump are substantially different from the systems with similar functions in the Surry plant. The major areas of difference lie in: (1) the inclusion of an additional system, the containment fan cooler system, into the ESFs, (2) the design of the containment spray system, (3) the location of the containment heat removal system (CHRS) heat exchangers (in different systems in the two plants), and (4) the design of the emergency coolant recirculation (ECR) system.

The selected PWR actually has two separate systems, the containment fan cooler system and the containment spray system, which can independently remove sufficient heat from the containment atmosphere to prevent containment overpressurization. The fan cooler system consists of five fan units with their associated heat exchangers (cooled by service water). The function of this system is to reduce containment pressure in the post-accident environment. It accomplishes this function by removing heat from the containment atmosphere directly to the environment through the service water system. It is noted, however, that the function of the fan cooler system does not include removal of iodine from the containment atmosphere.

With regard to the containment spray system, the WASH-1400 PWR has its spray injection function performed by a two-leg redundant system and the spray recirculation function by a four-leg redundant system. The two systems have no common ties of hardware, and no other functions (excluding sodium hydroxide addition by the spray injection system). The selected PWR, on the other hand, has a three-leg redundant spray injection system which has no other function; however, the spray recirculation system injects into the containment through the spray heads of only two of the three injection legs. Furthermore, the containment spray recirculation system (CSRS) does not have its own pumps. Water is supplied to it from the two pumps of the low pressure recirculation system (that also function in the LPIS) which recirculate the water from the containment sump through heat exchangers cooled by service

water. Thus, both the fan cooler system and the CSRS depend on the service water system for heat rejection. The service water system may later prove to be a common mode concern in detailed system evaluations.

5.3 Unavailability of Various Systems in the Selected PWR

A number of the systems in the selected PWR were found to be significantly different in design from similar systems in the Surry plant. In addition, one of the systems in the selected plant does not exist at all in Surry. Preliminary analyses have been completed for the electric power (EP) system, the containment fan cooler system, and the service water systems utilizing the data base in WASH-1400. Both electric power and service water have common mode possibilities, as they provide power and cooling to all plant systems.

The EP system is similar to the Surry system except that Surry has two independent power systems, i.e., one dedicated and one shared diesel; while the selected PWR has three independent power systems, which consist of two dedicated diesels and one shared diesel. However, these three power systems are not fully redundant, as two of three are required to satisfy most ESF systems.

The service water system in the selected PWR draws water from a lake and requires the operation of two of six pumps to supply enough water to shutdown both units in the event of an accident. The system supplies cooling water to most of the plant's pumps and also serves to remove heat from the containment. Loss of service water will cause the immediate or eventual loss of many systems. The unavailability of this system is almost totally made up of the unavailability of electric power to the system pumps. Results of the system evaluation for the unavailability at LOCA of 2 of 6 service water pumps is 1.7×10^{-6} per demand.

The containment fan cooler system in the selected PWR does not have a comparable system in the Surry plant. The function of this system is to reduce containment pressure in the post-accident environment by removing heat from the containment atmosphere. The system consists of five fan units with their associated heat exchangers. The system thus requires electric power and service water. The function of the fan cooler system overlaps

that of the containment spray recirculation system (CSRS), which also removes heat from the containment atmosphere. Heat collected by the CSRS, like that collected by the fan cooler system, is removed from containment by the service water system.

System failure for the fan cooler system is defined as failure to provide full operation of three of five of the fan cooler units. Results of the system evaluation for the unavailability at LOCA of 3 of 5 fan cooler units is 2.0×10^{-3} per demand.

5.4 Conclusions

The major objectives of this analysis were not completely achieved largely due to a lack of sufficient detailed plant information; however, the work performed satisfied much of the original goal. In particular, it was determined that a substantial amount of detailed plant information is required for the construction of useful event trees. The level and extent of detailed plant design information provided in the FSAR is insufficient for this purpose, particularly for the development of accident sequences for initiating events which may initially appear to be of lesser importance than a design basis accident. Furthermore, since the determination of system interrelationships and dependencies requires a complete understanding of the design and operation of the systems concerned, it is necessary to have access to: (1) detailed drawings of system designs and (2) plant procedures for test and maintenance operations, emergencies, various operational situations, etc., all of which are not included in the FSAR and which will be required, in any event, to numerically evaluate the systems which will input to the accident sequences defined by the event tree(s). Thus, the development of event trees for a nuclear power plant may be generally described as dependent on the cooperation of the plant operator and, to a lesser extent, the NSSS vendor. It is noteworthy that the Reactor Safety Study staff had this cooperation from both parties for both of the reactor types analyzed in WASH-1400.

The two LOCA event trees constructed for the PWR selected for this analysis form an incomplete and unevaluated set for the reasons described above. Nevertheless, it is clear that the event tree technique is a valuable and useful tool in risk assessment methodology since it provides an

overview framework from which to approach a complex analytical task. The real value of this technique can best be described as the reduction of the number of accident sequences which must be further analyzed to a manageable level and the insight and understanding provided by the analysis regarding the relationships and interdependencies which exist among the systems involved in the accident sequences.

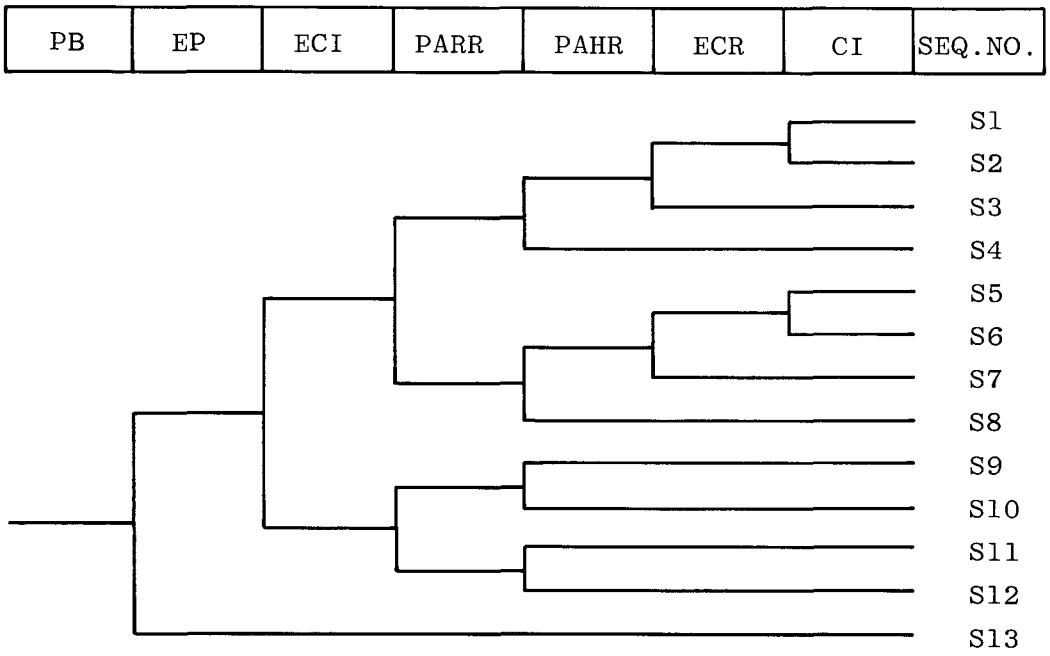


Figure 5-1. PWR Large LOCA Functional Event Tree (Draft WASH-1400)

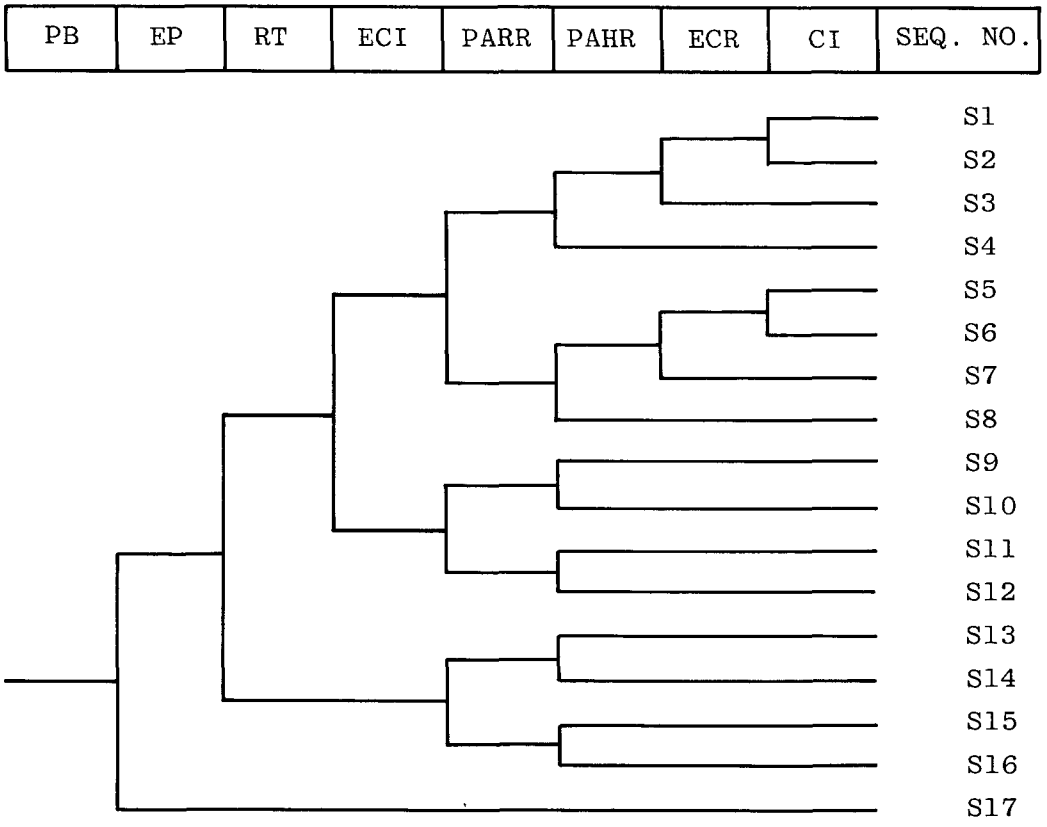


Figure 5-2. PWR Small LOCA Functional Event Tree (Draft WASH-1400)

Table 5-1. Definition of Functional Events

PB	Pipe Break. A break in the reactor coolant system pressure boundary; the cause of a loss of coolant accident (LOCA).
EP	Electric Power. Provides electric power to the engineered safeguard features so that they may perform their essential functions.
RT	Reactor Trip. Reactor shutdown to stop significant power generation due to the fission process during the LOCA.
ECI	Emergency Coolant Injection. The initial (or reflooding) phase of emergency core cooling.
PARR	Post Accident Reactivity Removal. Removal from the containment atmosphere of the radioactivity released from the core.
ECR	Emergency Coolant Recirculation. The long term recirculation phase of emergency core cooling, or the maintenance of the reflooded state achieved by ECI.
CI	Containment Integrity. Preventing the dispersal into the environment of radioactivity not removed by PARR.

Table 5-2. WASH-1400 PWR ESF Functions to ESF System Interrelationships.

	RT	ECI	PARR	PAHR	ECR*
PWR LARGE LOCA 6" diam.		ACC and LPIS	CSIS or CSRS + SHA CSIS or LPIS or HPIS	CSRS and CHRS	LPRS CSRS and CHRS
PWR SMALL LOCA 2" - 6" diam. break	RPS	ACC and HPIS	Same	Same	LPRS CSRS and and HPRS CHRS
PWR SMALL LOCA 1/2"-2" diam. break	Same	HPIS and AFW	Same	CSRS and CSIS CHRS	Same

*CI is omitted here.
or = Optional; success either way.
and = Both systems required for success.
\+ = Adds improvement in function.
= System interdependencies that affect principal system operation.

Definition of Terms

ACC - Accumulators
AFW - Auxiliary Feedwater (System)
CHRS - Containment Heat Removal System
CI - Containment Integrity
CSIS - Containment Spray Injection System
CSRS - Containment Spray Recirculation System
ECI - Emergency Coolant Injection
ECR - Emergency Coolant Recirculation
HPIS - High Pressure Injection System
LPIS - Low Pressure Injection System
LPRS - Low Pressure Recirculation
PAHR - Post Accident Heat Removal
PARR - Post Accident Reactivity Removal
RT - Reactor Trip
SHA - Sodium Hydroxide Addition

Table 5-3. Selected PWR Preliminary ESF Functions to ESF System Interrelationships.

	RT	ECI	PARR	PAHR	ECR*
PWR Large LOCA >6" diam.		ACC and SIP or ACC and LPIS	CSIS or CSRS + SHA CSIS	CSRS and CHRS or CFCS or combination	LPRS CHRS
PWR Small LOCA >4" to ≤ 6" diam. break	RPS	CP and SIP and ACC	Same	Same	LPRS and CHRS HPRS
PWR Small LOCA 1/2" to 4" diam. break	Same	CP or SIP or comb.	Same	Same CSIS**	Same

*CI is omitted here.
or = Optional; success either way.
and = Both systems required for success.
+ = Adds improvement in function.

= System interdependencies that affect principal system operation.

**CSIS initiation may not occur automatically, particularly for break sizes near the small end of the range, but the slow rise in containment pressure should allow a relatively long time (≥ 30 min) for operator initiation of the system.

Definition of Terms

ACC - Accumulators
SIP - Safety Injection Pumps
CP - Charging Pumps
LPIS - Low Pressure Injection System
CSIS - Containment Spray Injection System
CSRS - Containment Spray Recirculation System
LPRS - Low Pressure Recirculation System
CHRS - Containment Heat Removal System
CFCS - Containment Fan Cooler System
SHA - Sodium Hydroxide Addition

Table 5-4. Comparison of ECI Success Requirements[1]

LOCA Size	SURRY	Selected PWR
1. Large	≥6"[2] a) 2/3 accumulators AND 1/2 LPIS pumps	> 6" a) 3/4 accumulators AND 2/2 SI pumps b) 3/4 accumulators AND 1/2 LPIS pumps
2. Small	2 to 6" a) 1/3 HPIS pumps AND 2/3 accumulators	>4 to ≤6" a)[3] 1/2 charging pumps AND 1/2 SI pumps AND 3/4 accumulators
3. Small-Small	1/2 to 2" a) 1/3 HPIS pumps	1/2 to 4" a)[4] 1/2 charging pumps AND 1/2 SI pumps b)[5] 2/2 SI pumps c) 2/2 charging pumps
4. Very Small		<1/2" a) 1/2 charging pumps
Various System Discharge Pressures	HPIS: 2750 psig Accumulators: 650 psig LPIS: 300 psig	Charging: 2670 psig Safety Injection: 1500 psig Accumulators: 600 psig LPIS: 170 psig

[1]Read numbers such as 1/3 shown in this Table as "one out of three".
[2]In equivalent diameters.
[3]There may be other success combinations not yet defined.
[4]May require operator action.
[5]It is not certain that this success definition is good for the entire range of 1/2 to 4".

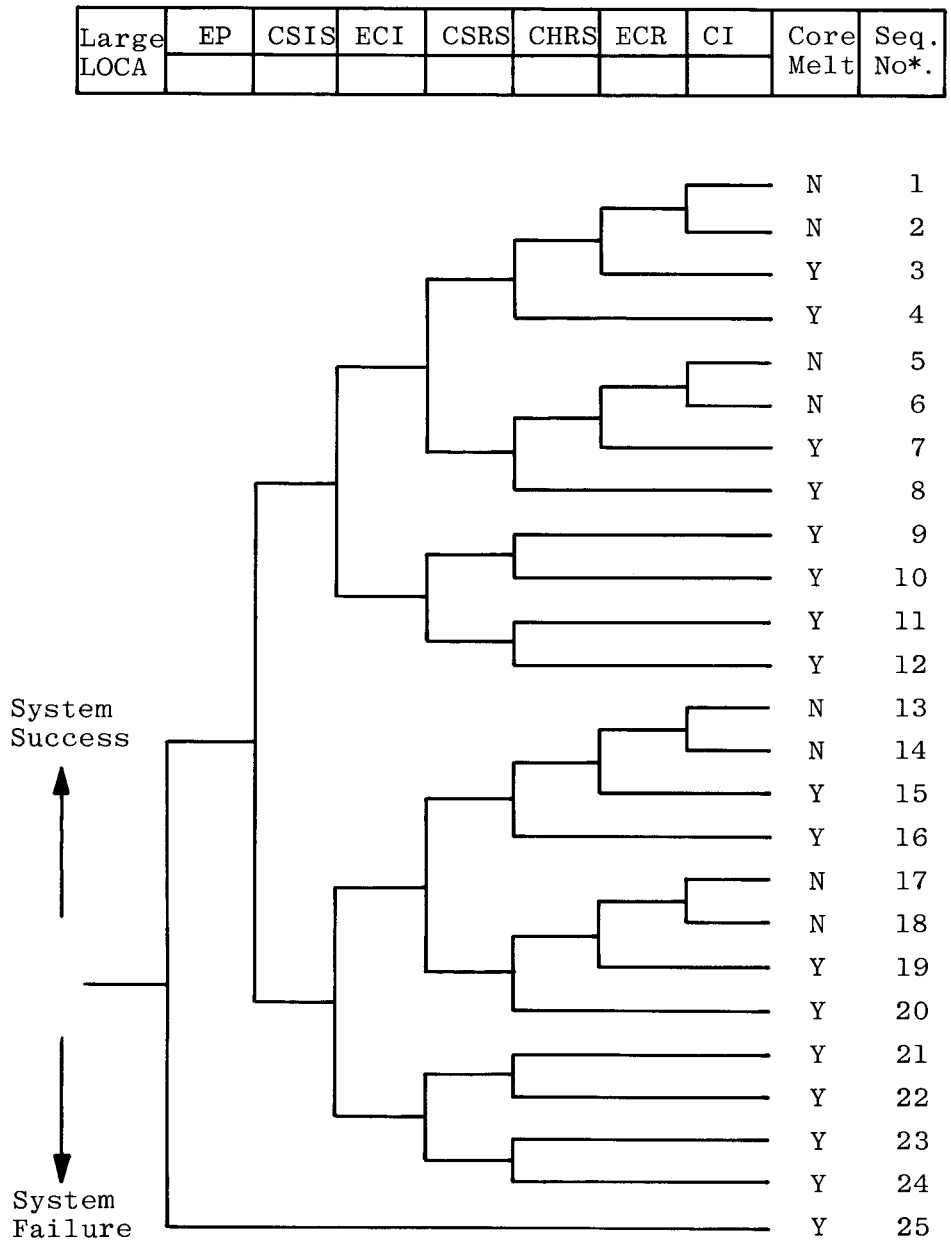


Figure 5-3. Preliminary Large LOCA Event Tree for the Selected PWR.

*Sequence descriptions are provided in Table 5-5.

Table 5-5. Description of Sequences* in Figure 5-6.

1. All systems operate normally. The core does not melt and no radioactive release occurs.**

2. The core does not melt, but some containment leakage results from CI failure.

3. ECR failure results in core melt and CI failure (CL, OP, MT, VSE, CSE).

4a. CHRS failure results in CI failure (OP-?) and eventual core melt-which is delayed by initial ECR success until ECR pump failure occurs due to cavitation caused by (1) high sump water temperature, (2) sump water loss due to boiloff from core, or (3) a combination of (1) and (2).

4b. CHRS failure and (independent) ECR failure result in core melt and CI failure.

5. CSRS failure complicates plant shutdown but core melt and CI failure do not occur, even though the containment remains at a relatively high pressure until CSRS can be repaired and placed in operation.

6. Like #5, but containment leakage occurs.

7. CSRS failure occurs. ECR failure results in core melt and eventual CI failure.

8a. CSRS failure occurs. CHRS failure results in CI failure and eventual core melt which is delayed as in sequence 4a.

8b. CSRS failure occurs. CHRS failure and (independent) ECR failure result in core melt and CI failure.

9. ECI failure results in core melt and CI failure (MT-?). ECR pre-empted by ECI, but operation of CSRS has mitigating effect on radioactive release due to removal of radioactivity in the containment atmosphere prior to CI failure. In the event CI failure results from OP, operation of CHRS delays the failure and allows more radioactivity removal by the CSRS.

10. ECI failure results in core melt and CI failure. CHRS failure hastens CI failure, in the event it results from OP, as containment pressure increases faster.

*Sequence descriptions assume occurrence of P.B.
**"No radioactive release" is defined as no release greater than the allowed release under current regulations.

Table 5-5 (con't)

11. Like #9; however, CSRS failure tends to increase the size of the eventual release. CHRS operation tends to decrease release size, particularly in the event of CI failure due to OP.

12. Like #10; however, CSRS and CHRS fail, thus causing the eventual release to be larger and occur sooner.

13. CSI failure occurs. All other systems operate normally. Core melt and CI failure do not occur.

14. CSI failure occurs. Core melt does not occur, but some containment leakage results from CI failure.

15. CSI failure occurs. ECR failure results in core melt and CI failure (CL, OP, MT, VSE, CSE).

16a. CSI failure occurs. CHRS failure results in CI failure (OP-?) and eventual core melt which is delayed as in sequence 4a.

16b. CSI failure occurs. CHRS failure and (independent) ECR failure result in core melt and CI failure.

17. CSI and CSRS failures occur. CSRS failure complicates plant shutdown, but core melt and CI failure do not occur.

18. Like #17, but some containment leakage occurs.

19. CSI and CSRS failure occur. ECR failure results in core melt and CI failure.

20a. CSI and CSRS failure occur. CHRS failure results in CI failure (OP-?) and eventual core melt which is delayed as in sequence 4a.

20b. CSI and CSRS failure occur. CHRS failure and (independent) ECR failure result in core melt and CI failure.

21. CSR and ECI failures result in core melt and CI failure (OP, MT-?). ECR pre-empted by ECI, but operation of CHRS has mitigating effect on radioactive release due to delay of CI failure.

22. CSI and ECI failures result in core melt and CI failure. CHRS failure hastens CI failure in the event it occurs as OP failure, as containment pressure increases faster.

23. CSI, ECI and CSRS failures result in core melt and CI failure, (remainder like #21).

Table 5-5 (con't)

24. CSI, ECI, CSRS and CHRS failures result in core melt and CI failure. CHRS failure hastens CI failure in the event it occurs as OP failure, as containment pressure increases faster.

25. EP failure results in core melt and CI failure.

General Notes

1. ECR failure always results in core melt and CI failure.

2. CHRS failure (may result in ECR failure and) always results in CI failure.

3. ECI failure pre-empts ECR and CI.

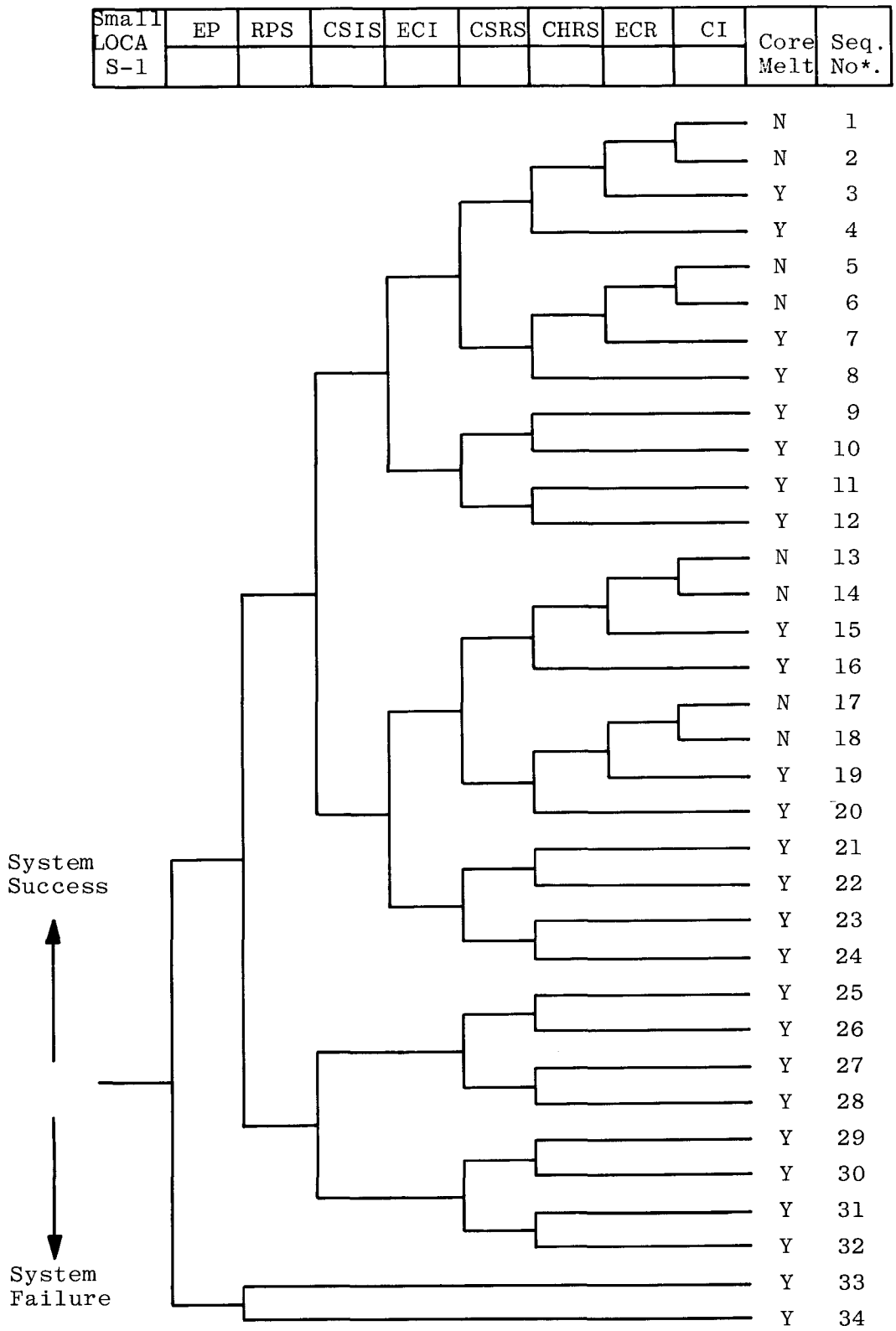


Figure 5-4. Preliminary S-1 Small LOCA Event Tree for the Selected PWR.

* Sequence descriptions are provided in Table 5-6.

Table 5-6. Description of Sequences* in Figure 5-7.

1. All systems operate normally. The core does not melt and no radioactive release occurs**.

2. The core does not melt, but some containment leakage results from CI failure.

3. ECR failure results in core melt and CI failure (CL, OP, MT, VSE, CSE).

4a. CHRS failure results in CI failure (OP-?) and eventual core melt-which is delayed by initial ECR success until ECR pump failure occurs due to cavitation caused by (1) high sump water temperature; (2) sump water loss due to boiloff from core; or (3) a combination of (1) and (2).

4b. CHRS failure and (independent) ECR failure result in core melt and CI failure.

5. CSRS failure complicates plant shutdown but core melt and CI failure do not occur, even though the containment remains at a relatively high pressure until CSRS can be repaired and placed in operation.

6. Like #5, but containment leakage occurs.

7. CSRS failure occurs. ECR failure results in core melt and eventual CI failure.

8a. CSRS failure occurs. CHRS failure results in CI failure and eventual core melt which is delayed as in sequence 4a.

8b. CSRS failure occurs. CHRS failure and (independent) ECR failure result in core melt and CI failure.

9. ECI failure results in core melt and CI failure (MT-?). ECR pre-empted by ECI, but operation of CSRS has mitigating effect on radioactive release due to removal of radioactivity in the containment atmosphere prior to CI failure. In the event CI failure results from OP, operation of CHRS delays the failure and allows more radioactivity removal by the CSRS.

10. ECI failure results in core melt and CI failure. CHRS failure hastens CI failure, in the event it results from OP, as containment pressure increases faster.

*Sequence descriptions assume occurrence of P.B.
**"No radioactive release" is defined as no release greater than the allowed release under current regulations.

Table 5-6. (con't)

11. Like #9; however, CSRS failure tends to increase the size of the eventual release. CHRS operation tends to decrease release size, particularly in the event of CI failure due to OP.

12. Like #10; however, CSRS and CHRS fail, thus causing the eventual release to be larger and occur sooner.

13. CSI failure occurs. All other systems operate normally. Core melt and CI failure do not occur.

14. CSI failure occurs. Core melt does not occur, but some containment leakage results from CI failure.

15. CSI failure occurs. ECR failure results in core melt and CI failure (CL, OP, MT, VSE, CSE).

16a. CSI failure occurs. CHRS failure results in CI failure (OP-?) and eventual core melt which is delayed as in sequence 4a.

16b. CSI failure occurs. CHRS failure and (independent) ECR failure result in core melt and CI failure.

17. CSI and CSRS failures occur. CSRS failure complicates plant shutdown, but core melt and CI failure do not occur.

18. Like #17, but some containment leakage occurs.

19. CSI and CSRS failures occur. ECR failure results in core melt and CI failure.

20a. CSI and CSRS failures occur. CHRS failure results in CI failure (OP-?) and eventual core melt which is delayed as in sequence 4a.

20b. CSI and CSRS failures occur. CHRS failure and (independent) ECR failure results in core melt and CI failure.

21. CSI and ECI failures result in core melt and CI failure (OP, MT-?). ECR pre-empted by ECI, but operation of CHRS has mitigating effect on radioactive release due to delay of CI failure.

22. CSI and ECI failures result in core melt and CI failure. CHRS failure hastens CI failure in the event it occurs as OP failure, as containment pressure increases faster.

23. CSI, ECI and CSRS failures result in core melt and CI failure, (remainder like #21).

Table 5-6 (con't)

24. CSI, ECI, CSRS and CHRS failures result in core melt and CI failure. CHRS failure hastens CI failure in the event it occurs as OP failure, as containment pressure increases faster.

25. RPS failure results in core melt. ECI and ECR may be prevented from operating due to steam binding.

26. Like #25, but CHRS also fails.

27. Like #25, but CSRS also fails.

28. Like #25, but both CSRS and CHRS also fail.

29. Like #25, but CSI also fails.

30. Like #29, but CHRS also fails.

31. Like #29, but CSRS also fails.

32. Like #29, but both CHRS and CSRS also fail.

33. EP failure prevents operation of the ESF systems.

34. Failure of RPS, given EP failure, results from mechanical failures only.

APPENDIX 5A

THE WASH-1400 PWR EVENT TREES

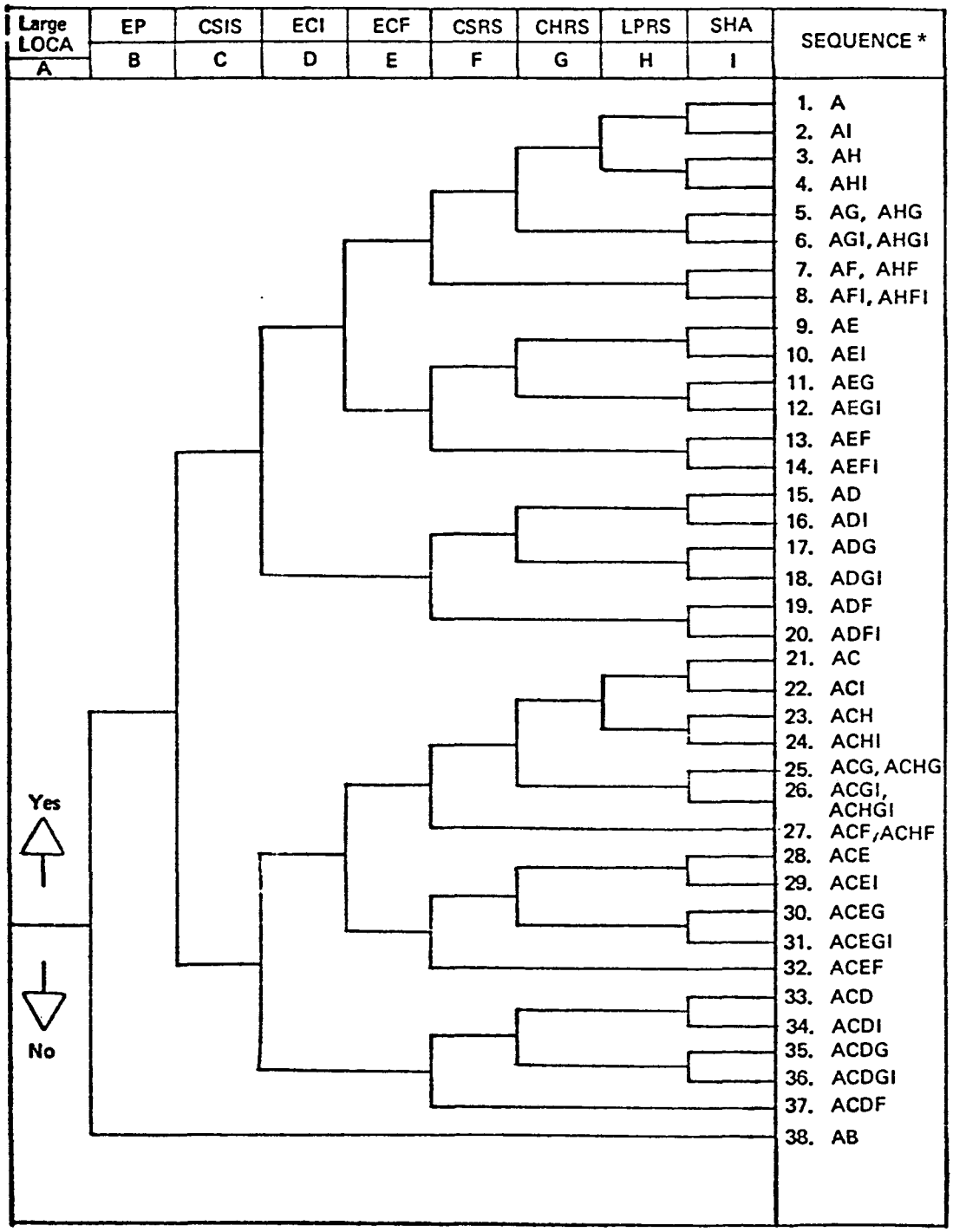


FIGURE 5A-1. PWR Large LOCA Event Tree (Draft WASH-1400)

* The reasoning underlying the various sequences, particularly with regard to dependent system failures, is described in Tables 5A-1 and 5A-2.

TABLE 5A-1. PWR Large LOCA Systems Status and Containment Failure Modes (Draft WASH-1400).

SEQUENCE	SNO	A LPB	B EP	C CSIS	D ECI	E ECF	F CSRS	G CHRS	H LPRS	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOT NOTES
A	1	f									N		X				DBA
AI	2	f								f	N		X				
AH	3	f							f		Y	X	X			X	
AHI	4	f							f	f	Y	X	X			X	
AG	5a	f					f_G	f	f_G	O_F	Y	X			X		1,2,3
AHG	5b	f					f_G	f	f_G	f_F	Y	X	X		X	X	4
AGI	6a	f					f_G	f	f_G	f_F	Y	X			X		1,2,3
AHGI	6b	f					f_G	f	f_G	f	Y	X	X		X	X	4
AF	7a	f					f_G	O_F	f_F	f_F	Y	X			X		1,2,3
AHF	7b	f					f	O_F	f_F	f_F	Y	X	X	X	X	X	4
AFI	8a	f					f	O_F	f_F	f_F	Y	X			X		1,3
AHFI	8b	f					f	O_F	f_F	f	Y	X	X	X	X	X	4
AE	9	f				f			O_E		Y	X	X			X	5
AEI	10	f				f			O_E	f	Y	X	X			X	5
AEG	11	f				f	f_G	f	O_E	f_F	Y	X	X		X	X	1,5
AEGI	12	f				f	f_G	f	O_E	f_F	Y	X	X		X	X	1,5
AEF	13	f				f	f_G	O_F	O_E	f_F	Y	X	X		X	X	1,5
AEFI	14	f				f	f	O_F	O_E	f_F	Y	X	X		X	X	1,5
AD	15	f			f	O_D			O_D		Y	X	X			X	6
ADI	16	f			f	O_D			O_D	f	Y	X	X			X	6
ADG	17	f			f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	1,6
ADGI	18	f			f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	1,6
ADF	19	f			f	O_D	f_G	O_F	O_D	f_F	Y	X	X			X	1,6
ADFI	20	f			f	O_D	f	O_F	O_D	f	Y	X	X			X	1,6
AC	21	f		f							N		X				
ACI	22	f		f						f	N		X				
ACH	23	f		f					f		Y	X	X			X	
ACHI	24	f		f					f	f	Y	X	X			X	
ACG	25a	f		f			f_G	f	f_G	O_F	Y	X			X		1,2,3
ACHG	25b	f		f			f_G	f	f_G	f_F	Y	X	X		X	X	4
ACGI	26a	f		f			f_G	f	f_G	f_F	Y	X			X		1,2,3
ACHGI	26b	f		f			f_G	f	f_G	f	Y	X	X		X	X	4
ACF	27a	f		f			f_G	O_F	f_F	O_{CF}	Y	X			X		1,3,7
ACHF	27b	f		f			f	O_F	f_F	O_{CF}	Y	X	X	X	X	X	4
ACE	28	f		f		f			O_E		Y	X	X			X	5
ACEI	29	f		f		f			O_E	f	Y	X	X			X	5
ACEG	30	f		f		f	f_G	f	O_E	f_F	Y	X	X		X	X	1,5
ACEGI	31	f		f		f	f_G	f	O_E	f_F	Y	X	X		X	X	1,5
ACEF	32	f		f		f	f_G	O_F	O_E	O_{CF}	Y	X	X	X	X	X	5,7
ACD	33	f		f	f	O_D			O_D		Y	X	X			X	6,8
ACDI	34	f		f	f	O_D			O_D	f	Y	X	X			X	6
ACDG	35	f		f	f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	1,6,8
ACDGI	36	f		f	f	O_D	f_G	f	O_D	f_F	Y	X	X		X	X	1,6
ACDF	37	f		f	f	O_D	f_G	O_F	O_D	O_{CF}	Y	X	X	X	X	X	6,7
AB	38	f	f	Z_B	Z_B	O_D	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	9

Key: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF "N" FAILURE
Z_N - FAILURE PREDICATED BY FAILURE OF "N"
Y - YES
N - NO
X - POTENTIAL CONTAINMENT VESSEL FAILURE MODE
FOOTNOTES ARE ATTACHED

TABLE 5A-2. Footnotes to PWR Large LOCA System Status Table (Draft WASH-1400)

Note 1: Failure to remove heat through the recirculation spray heat exchangers causes the containment to pressurize and ultimately to fail due to the almost adiabatic addition of decay heat to the containment atmosphere. As discussed in Appendix VIII,[23] containment failure is predicted to occur at a pressure of about 100 psi. Since the water in the containment sump will be at the saturation temperature associated with the partial pressure of steam within containment, the rapid depressurization which occurs upon containment failure will cause the water in the sump to flash and cause cavitation of the CSRS and LPRS pumps. It is assumed that this cavitation will damage the pumps, preventing operation of either the CSR or LPR systems following containment failure.

Note 2: Note CSRS and SHA are available only prior to the occurrence of core melt.

Note 3: For this sequence, containment failure causes eventual core melt. A steam explosion, which occurs as the molten fuel drops into the residual water in the lower pressure vessel head, will increase the "puff" release of activity from the already failed containment.

Note 4: Independent LPRS failure. Loss of heat removal through a failure of the recirculation spray heat exchangers leads to containment overpressurization. Containment failure may occur because of such overpressurization or because of the interactions with the molten core and meltthrough.

Note 5: Since the emergency core cooling injection system does not function to cool the core, core meltdown will result. Success of LPRS will have no effect on core damage since melting would be in progress when LPRS is available.

Note 6: If the emergency core cooling injection system fails to operate, the question of functionability is moot. Since core meltdown results if ECI fails, LPRS operation would not succeed in preventing the core melt.

Note 7: Failures of CSIS and CSRS eliminate all means of reducing containment pressure or washing fission products from the containment atmosphere.

Note 8: Partial ECI operation is required in order to inject NaOH into the water used in the CSRS system.

Note 9: EP failure prevents operation of other systems.

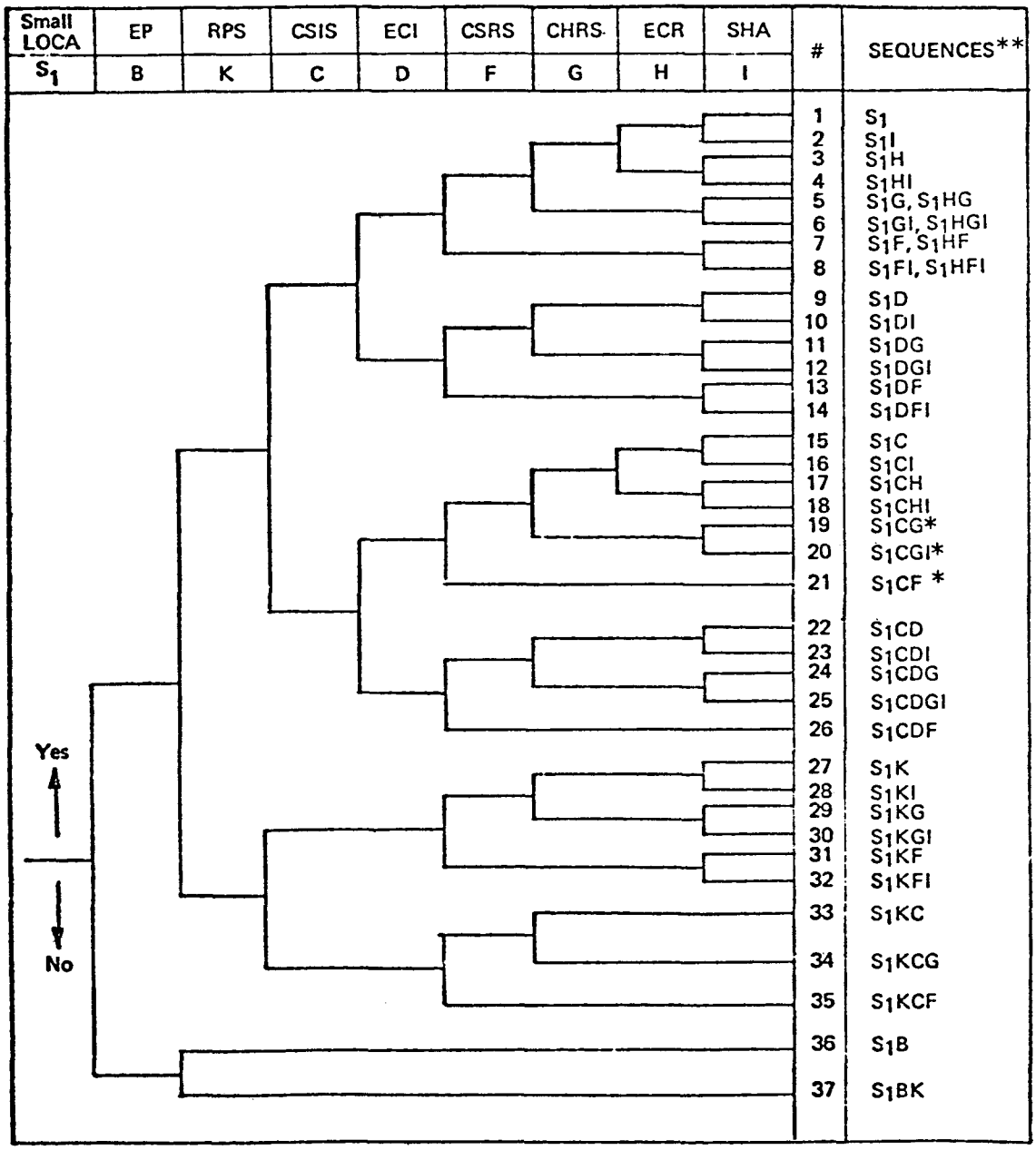


FIGURE 5A-2. PWR Small Rupture (S1, 2-6 inch diameter) in RCS (Draft WASH-1400)

*Sequences #19, 20 and 21 should also show, respectively, S_1CHG, S_1CHGI and S_1CHF.

** The reasoning underlying the various sequences, particularly with regard to dependent system failures is described in Tables 5A-3 and 5A-4.

TABLE 5A-3. PWR Small LOCA S_1-System Status and Containment Failure Modes (Draft WASH-1400)

SEQUENCE	SNO	S1	B EP	K RPS	C CSIS	D ECI	F CSRS	G CHRS	H ECR	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	FOOT NOTES
S_1	1	f									N		X				
S_1I	2	f								f	N		X				
S_1H	3	f							f		Y	X	X			X	
S_1HI	4	f							f	f	Y	X	X			X	
S_1G	5a	f					f_G	f	f_G	O_G	Y	X			X		1,2,3,7
S_1HG	5b	f					f_G	f	f_G	O_G	Y	X	X		X	X	4
S_1GI	6a	f					f_G	f	f_G	f_G	Y	X			X		1,2,3
S_1HGI	6b	f						f	f_G	f	Y	X	X		X	X	4
S_1F	7a	f					f	O_F	f_F	O_F	Y	X			X		5,6,7
S_1HF	7b	f					f	O_F	f_F	f_G	Y	X	X		X	X	4,5,7
S_1FI	8a	f					f	O_F	f_F	f_G	Y	X			X		1
S_1HFI	8b	f					f	O_F	f_F	f	Y	X	X		X	X	1,5
S_1D	9	f				f			O_D		Y	X	X			X	8
S_1DI	10	f				f			O_D	f	Y	X	X			X	8
S_1DG	11	f				f		f	O_D		Y	X	X		X	X	8
S_1DGI	12	f				f		f	O_D	f	Y	X	X		X	X	8
S_1DF	13	f				f	f	O_F	O_D		Y	X	X		X	X	1,5,8
S_1DFI	14	f				f	f			f	Y	X	X		X	X	
S_1C	15	f			f						N		X				
S_1CI	16	f			f					f	N		X				
S_1CH	17	f			f				f		Y	X	X			X	
S_1CHI	18	f			f				f	f	Y	X	X			X	
S_1CG	19a	f			f		f_G	f	f_G	O_F	Y	X			X		1,2,3,7
S_1CHG	19b	f			f		f_G	f	f	f_G	Y	X	X		X	X	4
S_1CGI	20a	f			f		f_G	f	f_G	f_G	Y			X	X		1,2,3,7
S_1CHGI	20b	f			f		f_G	f	f_G	f	Y	X	X		X	X	4
S_1CF	21a	f			f		f_G	O_F	f_F	O_F	Y			X	X		1,2,3,7
S_1CHF	21b	f			f		f	O_F	f_F	O_F	Y	X	X	X	X	X	4
S_1CD	22	f			f	f			O_D		Y	X	X			X	8
S_1CDI	23	f			f	f			O_D	f	Y	X	X			X	8
S_1CDG	24	f			f	f		f	O_D		Y	X	X		X	X	8
S_1CDGI	25	f			f	f		f	O_D	f	Y	X	X		X	X	8
S_1CDF	26	f			f	f	f	O_F	O_D	O_{CF}	Y	X	X	X	X	X	5,8,9
S_1K	27	f		f		O_K			O_K		Y	X	X			X	10
S_1KI	28	f		f		O_K			O_K	f	Y	X	X			X	10
S_1KG	29	f		f		O_K		f	O_K		Y	X	X		X	X	10
S_1KGI	30	f		f		O_K		f	O_K	f	Y	X	X		X	X	10
S_1KF	31	f		f		O_K	f	O_F	O_K		Y	X	X		X	X	5,10
S_1KFI	32	f		f		O_K	f	O_F	O_K	f	Y	X	X		X	X	5,10
S_1KC	33	f		f	f	O_K			O_K	O_{CD}	Y	X	X			X	9,11
S_1KCG	34	f		f	f	O_K		f		O_{CD}	Y	X	X		X	X	9,11
S_1KCF	35	f		f	f		f	O_F	O_K	O_{CF}	Y	X	X	X	X	X	9,10
S_1B	36	f	f		Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	12
S_1BK	37	f	f	f	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	12,13

KEY: f - FAILURE
f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF FAILURE OF "N"
Z_N - FAILURE PREDICATED BY FAILURE OF "N"
Y - YES
N - NO
X - POTENTIAL CONTAINMENT VESSEL FAILURE MODE

TABLE 5A-4. Footnotes to Sequence Description Chart for Small LOCA S1 (Draft WASH-1400)

Note 1: Failure of CHRS leads to containment failure at high pressures. The subsequent flashing of high temperature water in the sump results in CSRS and ECR pump cavitation, rendering CSRS and ECR inoperable.

Note 2: CSRS and SHA are available only prior to the occurrence of core melt.

Note 3: Containment failure causes eventual core melt. A steam explosion which occurs as the molten fuel drops into the residual water in the lower head of the pressure vessel will increase the "puff" release of activity from the already failed containment.

Note 4: Independent ECR failure. ECR fails prior to containment failure due to depressurization.

Note 5: Failure of CSRS prevents delivery of sump water to the CHRS heat exchangers; therefore, operation of CHRS has no effects.

Note 6: Failure of CSRS leads to containment failure at high pressure. The resultant flashing of high temperature sump water cavitates the ECR pumps.

Note 7: Failure of CSRS prevents the spray of NaOH through the containment atmosphere following core melt. Therefore, SHA operation does not matter.

Note 8: Failure of ECI to operate obviates the need for ECR.

Note 9: Failure of CSIS and CSRS prevents spray operation, eliminating the need for SHA.

Note 10: Failure of RPS leads to core melt regardless of ECI or ECR operation.

Note 11: Failure of CSIS and ECI prevents NaOH addition to containment.

Note 12: EP failure prevents operation of other systems.

Note 13: Failure of RPS, given EP failure, results from mechanical failures only.

Small LOCA	EP	RPS	SSR& AFWS	CSIS	ECI	CSRS	CHRS	ECR	SHA	#	SEQUENCE*
S_2	B	K	L	C	D	F	G	H	I		

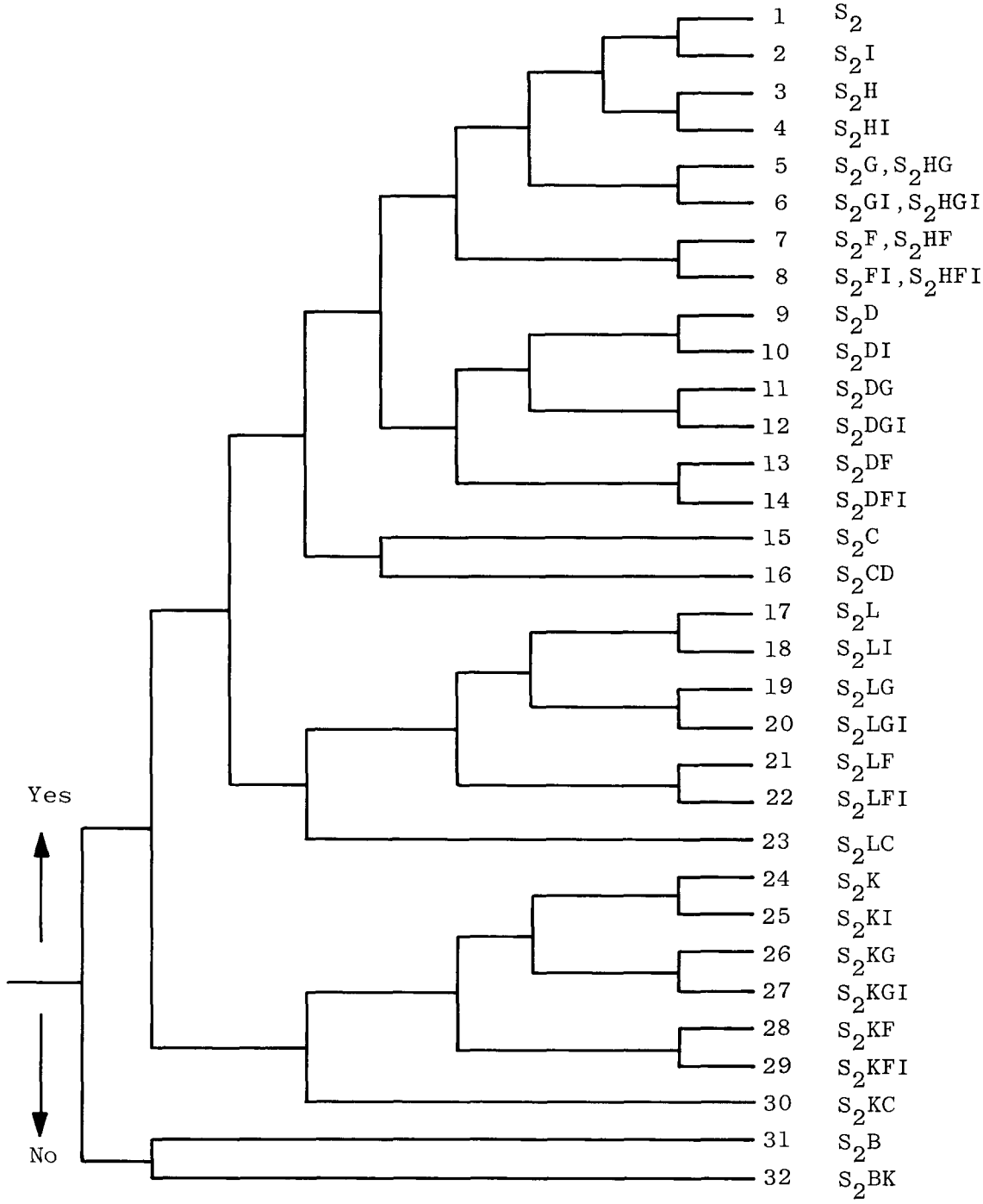


FIGURE 5A-3. PWR Small Rupture (S2, 1/2-2 inch diameter) in RCS (Draft WASH-1400)

* The reasoning underlying the various sequences, particularly with regard to dependent system failures, is described in Tables 5A-5 and 5A-6.

TABLE 5A-5. PWR Small LOCA S_2 System Status and Containment Failure Modes (Draft WASH-1400)

SEQUENCE	SNO	S2	B EP	K RT	L SSR& AFW	C CSIS	D ECI	F CSRS	G CHRS	H ECRS	I SHA	CORE MELT	α VSE	β CL	γ H_2C	δ OP	ε CVMT	F NOTES
S_2	1	f										N		X				
S_2I	2	f									f	N		X				
S_2H	3	f								f		Y	X	X			X	
S_2HI	4	f								f	f	Y	X	X			X	
S_2G	5a	f						f_G	f	f_G	O_G	Y	X			X		1,2,3
S_2HG	5b	f						f_G	f	f_G	f_G	Y	X	X		X	X	4
S_2GI	6a	f						f_G	f	f_G	f	Y	X			X		1,2,3
S_2HGI	6b	f						f_G	f	f	f	Y	X	X		X	X	4
S_2F	7a	f						f	O_F	f_F	O_F	Y	X			X		5,6,7
S_2HF	7b	f						f	O_F	f	f_F	Y	X	X		X	X	4,5,7
S_2FI	8a	f						f	O_F	f_F	f	Y	X			X		5,6
S_2HFI	8b	f						f	O_F	f	f	Y	X	X		X	X	5
S_2D	9	f					f			O_D		Y	X	X			X	8
S_2DI	10	f					f			O_D	f	Y	X	X			X	8
S_2DC	11	f					f		f	O_D		Y	X	X		X	X	8
S_2DGI	12	f					f		f	O_D	f	Y	X	X		X	X	8
S_2DF	13	f					f	f	O_F	O_D		Y	X	X		X	X	5,8
S_2DFI	14	f					f	f	O_F	O_D	f	Y	X	X		X	X	5,8
S_2C	15	f				f		Z_C	O_F	Z_C	O_{CF}	Y	X	X	X	X	X	5,9,14
S_2CD	16	f				f	f	Z_C	O_C	O_D	O_{CF}	Y	X	X	X	X	X	5,9,11,14
S_2L	17	f			f		O_L			O_L		Y	X	X			X	15
S_2LI	18	f			f		O_L			O_L	f	Y	X	X			X	15
S_2LG	19	f			f		O_L		f	O_L		Y	X	X		f	X	15
S_2LGI	20	f			f		O_L		f	O_L	f	Y	X	X		X	X	15
S_2LF	21	f			f		O_L	f	O_F	O_L		Y	X	X		X	X	5,15
S_2LFI	22	f			f		O_L	f	O_F	O_L	f	Y	X	X		X	X	5,15
S_2LC	23	f			f	f	O_L	Z_C	O_C	O_L	O_C	Y	X	X	X	X	X	5,7,14,15
S_2K	24	f		f	O_K		O_K			O_K		Y	X	X			X	10
S_2KI	25	f		f	O_K		O_K			O_K	f	Y	X	X			X	10
S_2KG	26	f		f	O_K		O_K		f	O_K		Y	X	X		X	X	10
S_2KGI	27	f		f	O_K		O_K		f	O_K	f	Y	X	X		X	X	10
S_2KF	28	f		f	O_K		O_K	f	O_F	O_K		Y	X	X		X	X	5,10
S_2KFI	29	f		f	O_K		O_K	f	O_F	O_K	f	Y	X	X		X	X	5,10
S_2KC	30	f		f	O_K	f	O_K	Z_C	O_C	O_K	O_C	Y	X	X	X	X	X	14,15
S_2B	31	f	f		Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	12
S_2BK	32	f	f	f	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Z_B	Y	X	X	X	X	X	12,13

KEY:
- f - FAILURE
- f_N - DEPENDENT TIME-DELAYED FAILURE CAUSED BY FAILURE OF "N"
- O_N - DOES NOT MATTER, SYSTEM HAS NO EFFECT BECAUSE OF FAILURE OF "N"
- Z_N - FAILURE PREDICATED BY FAILURE OF "N"
- Y - YES
- N - NO
- X - POTENTIAL CONTAINMENT VESSEL FAILURE MODE

TABLE 5A-6. Footnotes to Sequence Description Chart for Small LOCA S2 (Draft WASH-1400)

Note 1: Failure of CHRS leads to containment failure at high pressures. The subsequent flashing of high temperature water in the sump results in CSRS and ECR pump cavitation, rendering CSRS and ECR inoperable.

Note 2: CSRS and SHA are available only prior to the occurrence of core melt.

Note 3: Containment failure causes eventual core melt. A steam explosion which occurs as the molten fuel drops into the residual water in the lower head of the pressure vessel will increase the "puff" release of activity from the already failed containment.

Note 4: Independent ECR failure. ECR fails prior to containment failure due to depressurization.

Note 5: Failure of CSRS prevents delivery of sump water to the CHRS heat exchangers; therefore, operation of CHRS has no effects.

Note 6: Failure of CSRS leads to containment failure at high pressure. The resultant flashing of high temperature sump water cavitates the ECR pumps.

Note 7: Failure of CSRS prevents the spray of NaOH through the containment atmosphere following core melt. Therefore, SHA operation does not matter.

Note 8: Failure of ECI to operate obviates the need for ECR.

Note 9: Failure of CSIS and CSRS prevents spray operation, eliminating the need for SHA.

Note 10: Failure of RT leads to core melt regardless of ECI or ECR operation.

Note 11: Failure of CSIS and ECI prevents NaOH addition to containment.

Note 12: EP failure prevents operation of other systems.

Note 13: Failure of RT, given EP failure, results from mechanical failures for the rods only.

Note 14: Failure of CSIS prevents the addition of large quantities of borated water to the containment. Since only a small portion of the reactor coolant system inventory leaks to the sump, sufficient elevation head is not available and LPRS and CSRS pump cavitation will occur.

TABLE 5A-6 (Cont'd)

Note 15: Failure to dissipate decay heat through the secondary system results in the reactor coolant pressure increasing to the safety valve setting. Upon opening of the RCS safety valves, the reactor coolant system water inventory cannot be maintained and a core melt eventually follows. The ECCS cannot operate against the system pressures anticipated.

SECTION 6

A REAPPRAISAL OF THE ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS) PROBLEM

A series of documents are being prepared which examine the basis for the problem of anticipated transients without scram (ATWS). The purpose of these documents is to evaluate risk due to ATWS in the light of developments subsequent to the publication of WASH-1270[10] and to re-evaluate the probabilistic basis for ATWS. Much of the methodology developed during the two years represented by this biannual report has been utilized in the ATWS reappraisal, and furthermore the detailed assessments could not have been accomplished without some of the methodology tools previous work has made available.

The project's goals include estimates of: the actual probability of failure to scram; the probabilities of initiating events, such as MSIV closure; and the risk due to ATWS. The series of documents is expected to consist of four parts, as listed below; each of these may consist of several volumes.

ATWS: A Reappraisal

Part I:	An Examination and Analysis of WASH-1270, the "Technical Report on ATWS for Water-Cooled Power Reactors"
Part II:	Evaluation of Societal Risks Due to Reactor Protection System Failure
Part III:	Reactor Accident Probabilities
Part IV:	Summary Document on Plants Potentially Requiring Backfitting

There is also the possibility, in the very long term, of a cost-benefit evaluation for specific plant modifications.

The purpose of Part I is to update the numerical information presented in WASH-1270 by correcting deficiencies in that document and updating

input data. The two additions in the present approach are the use of a demand failure model instead of a time-dependent model for the scram system and the incorporation of Bayesian priors into the probabilistic treatment of the data.

The purpose of Part II is an evaluation of societal risks due to RPS failure based on more current data and methodology than used in WASH-1270. Volume 1 examines and documents the potential contribution to societal risk due to ATWS in the BWR. Volume 2 provides the basis for the calculation and contains a detailed description of the re-evaluation and expansion of the RPS fault tree for the WASH-1400 BWR. Volume 3 will describe a similar analysis for the PWR.

In Sections 6.1 and 6.2 summaries of the draft versions of ATWS: A Reappraisal, Part I, and Part II,Volume 1 and Volume 2 are provided.

6.1 Summary of Part I: An Examination and Analysis of WASH-1270

In 1973, the Atomic Energy Commission published WASH-1270 entitled, "Anticipated Transients Without Scram for Water-Cooled Power Reactors". This document was the end product of discussions on common-mode failures (CMF's) which started in the late 1960's. It is particularly important in that it attempts to introduce a rational (statistical/probabilistic) basis for validating consideration of an ATWS as being important enough to require regulatory action.

6.1.1 Observations on WASH-1270

The following observations are the result of a careful review of the WASH-1270 document.

1. WASH-1270 is the first nuclear regulatory document to specifically incorporate probabilistic risk.

2. It defines a negligibly small risk criterion as having a probability of 10^{-6}/reactor-year that 10CFR100 guidelines will be exceeded. Risks below this risk criterion may be ignored.

3. The reactor accident subclass Anticipated Transient Without Scram (ATWS) is allocated one-tenth of the probability of the full population of potential reactor accidents. Therefore, the allocated probability for all modes of ATWS must be less than or equal to 10^{-7}/reactor-year.

4. The technical report is of indefinite status. It calls for regulations to clarify its conclusions, but such regulations have not been published. It is being treated as having nearly the status of a Regulatory Guide.

5. It presumes analysis methods of CMF as inadequate and accepts only nuclear power plant experience as a measure of scram system reliability. However, it finds that a scram system unavailability of 10^{-7}/ reactor-year cannot be demonstrated on the basis of experience and that such experience will not be attained in the near future.

   Although the report called for independent scram systems to resolve this problem, this approach has since been dropped. There seems to be no choice but to use all viable methods for probability estimation.

6. It estimates the present ATWS probability (A) as the product of the probability per year of a severe transient (P_A) and the unreliability (U) of the scram system. P_A is conservatively approximated as 1/year. The scram unreliability (U) is estimated based only on experience, using a constant failure rate model for a standby type system. The WASH-1270 conclusion, based on data prior to April 1973, is $A \leq 1.6 \times 10^{-4}$ (with 85% confidence).

   In our review of this assessment, the scram system failure was modeled as failure on demand. Based on industrial reporting through December 1975, we calculated that $U \leq 2.1 \times 10^{-5}$/D even if the one potential scram failure of the foreign reactor is counted as a potential failure mode in the future in spite of the changes in design and procedures resulting from it. Our calculation of scram system unavailability was performed for both a constant failure rate Class I censored testing model as well as a binary model[a]. The statistical procedures employed in WASH-1270 are conservative in that

---

(a) See Appendix A of Reference 11.

rectifiability[b] of the data resulting from changes in regulations and design improvements have not been credited, nor has the continuous evolution in the form of a learning curve been credited. A further conservatism is that the classical statistical models used in WASH-1270 are based on test data only. No credit is given for engineering prior information. Using as a Bayesian prior results from a fault tree analysis of the scram system, and assuming one failure, we find $U \leq 8.0 \times 10^{-6}$/demand for the BWR and $U \leq 4.4 \times 10^{-5}$/demand for the PWR, both at 95% confidence. A similar calculation assuming zero failures (on the basis of rectifiability) results in $U \leq 3.7 \times 10^{-6}$/demand for the BWR and $U \leq 4.1 \times 10^{-5}$/demand for the PWR, again at 95% confidence. Since P_A has been conservatively assumed to be one per reactor-year, the annual ATWS probability (A) for each of these cases has the same numerical value as U, with units of per reactor-year.

7. The staff review presented in WASH-1270 concludes that the four present scram system designs have sufficient reliability for random failure modes but that methods are lacking for treating unknown common-mode effects.

   We have performed a fault tree analysis of the BWR scram system and confirm the ability of the present design to provide adequate protection against random failures. We take exception to the statement that there are no good methods for treating CMF's. The subject of dependency analysis using fault trees has progressed considerably since publication of WASH-1270. We suggest that, if a careful and thorough analysis of the reactor protection system fails to disclose CMF's or causes the elimination of those that are found, the remaining CMF's are not significant risk contributors. Our sensitivity analyses[8] based on WASH-1400 methodology suggest that there are more effective ways to reduce nuclear power plant societal risks than by making improvements in scram system reliability.

(b) The concept that certain types of potential common-mode failures (CMF), once identified, can be almost entirely prevented from occurring in the future. This may be accomplished, for example, by devising a special test scheme which will force the discovery (and repair) of the basic fault(s) underlying a potential CMF as they occur. Thus, the probability of system failure from this cause will be substantially reduced - practically to the point where that particular CMF initiator may be eliminated from consideration.

6.1.2 Critique of WASH-1270 Methodology

Now that probabilistic analysis is being recognized as valid, it is imperative that the statistical treatment of the historical data on related systems be utilized properly and consistently. Moreoever, wherever possible, these data should be compared to failure analysis predictions to obtain additional confidence in our understanding of system failure modes and operational behavior.

According to WASH-1270, an examination of experience data indicates that the scram system availability is less than 1.6×10^{-4}/test and greater than 1.9×10^{-5}/test, both at 95% confidence. These estimates take into consideration the only two instances of scram system unavailability; i.e., two failures are assumed. Furthermore, the WASH-1270 analysis allowed for only 12 tests of the system per year, but some systems are tested more frequently and all systems experience actual (non-test) scrams in addition to the tests specified by test and maintenance (T&M) procedures. The actual number of scrams above 12 per year is quite significant, especially if one includes Naval reactor experience data.

The two instances of scram system unavailability mentioned above are: (1) the Kahl reactor* incident in Germany where it was discovered, during a test, that a scram signal would not have been initiated if required due to a CMF of the scram relays, and (2) the 1970 shutdown system failure of the N reactor at the AEC Hanford Facility. This incident was the result of the CMF of four blocking diodes in the scram rod control circuitry.

Our analysis of data through December 1975 shows that use of the WASH-1270 statistical methodology (but neglecting the N reactor failure)** results in a scram system unavailability of less than 2.1×10^{-5}/demand and greater than 2×10^{-7}/demand, both at the 95% confidence level. One can also question the usefulness of insisting on 95% confidence bounds. The maximum likelihood estimate for the data (keeping one failure) yields a value of 8.7×10^{-6}/demand, and for example, at the 50% confidence level the data sample supports an unavailability below 7.4×10^{-6}/demand.

---

*A U.S. Designed BWR.

**The N reactor scram system does not belong to the same populations as Naval or commercial LWR's.

However, the methodology used by WASH-1270 is in fact not applicable precisely because of rectifiability. The WASH-1270 approach is ultimately based on the assumption of the validity of the Poisson process which can be used to validate the Exponential Failure Model, but the process is not applicable if the future is affected by our knowledge of the past. That is, if we accept that modifications in design, QA or T&M, which occur alter the characteristics of the failure portion of the population, then the WASH-1270 results are not statistically accurate. Practically speaking one must start the data base all over again. In the present case, almost all of the data occurs post-Kahl. Hence, the numerical conclusions arrived at in the previous paragraph are not seriously altered.

Finally, we point out that the methodology used in WASH-1270 is inadequate to account for our prior knowledge. For this we have to pass over to a Bayesian framework. If we do this, and use any one of three types of prior knowledge, we achieve a further factor of 2 changes in unavailability over that predicted by the WASH-1270 methods. We can say, finally, that an analysis of presently available data using a more comprehensive statistical method, i.e., a Bayesian analysis, results in the posterior upper bounds RPS unavailabilities shown in Table 6-1 below.

TABLE 6-1. Bayesian Posterior Upper Bound RPS Unavailabilities

Confidence Level	BWR	PWR
95%	3.5×10^{-6}/D	1.9×10^{-5}/D
50%	6.3×10^{-7}/D	9.2×10^{-6}/D

On the basis of our examination and review of WASH-1270, we recommend the following:

1. Development of reactor risk criteria commensurate with similar industries. The risk criterion of 10^{-6}/reactor year for the probability of exceeding 10CFR100 criteria suggested in WASH-1270 should be carefully examined before receiving further acceptance. To this end, we recommend an evaluation of risk imposed on society by similar industries in order to obtain a balance risk

perspective so that risk criteria for reactors may be made consistent with other sources of societal risk.

2. Detailed scram system safety analyses. We recommend a careful, detailed analysis of the current scram system designs to determine the scram failure probability of existing systems, including appropriate confidence bounds.

3. Maximized transient protection improvement. With the thorough understanding of present scram reliability that would result from point 2, and with a comprehension of the implications of point 1,we recommend an examination of transient accident sequences to determine the most effective areas for future improvement based upon an estimate of the risk reduction so obtained. Should further improvements in scram reliability be deemed necessary, an analysis of present reliability evaluations should be used as a guide to determine where the most effective improvements can be made.

6.2 Summary of Part II: Evaluation of Societal Risks Due to Reactor Protection System Failure, Volumes 1 and 2; BWR Risk Analysis and Fault Evaluation

6.2.1 Introduction

This work contains the results of a study of the potential risk due to Reactor Protection System (RPS) failure in a BWR. It is divided into two volumes; the first contains the quantification of the potential risk while the second contains a detailed description of the re-evaluation and expansion of the WASH-1400 BWR RPS fault tree.

The methods used here and the analysis presented are based on the draft WASH-1400 report. The draft version was utilized because of the unavailability of the final version consequence model. It is not expected that use of the final WASH-1400 study would change any of the conclusions presented here.

The reactor examined was Peach Bottom No. 2, as documented in the WASH-1400 report. Since accidents that might violate 10CFR100[39] were of interest, work was concentrated on sequences that lead to some degree of core meltdown. Non-meltdown accidents, although potential violators of 10CFR100, were not considered since it was argued that these less severe incidents would not significantly add to the risk from meltdown.

Accident consequences were compared for the 30 Day Whole Body Dose scale. Other consequences can be compared should a need arise, but all consequences appear to be affected by about the same percentage.

Initially, the analysis provided information regarding transient-caused meltdowns and that fraction that could be attributed to reactor protection system failure. This analysis used as its basis the failure data and fault tree evaluations of WASH-1400. Subsequently, the fault trees for the BWR RPS were reconstructed and re-evaluated. This process indicated a more reliable RPS than was used in WASH-1400. The impact of both this improved system reliability value and of even further improvements are described.

6.2.2 Analysis

Although we are confident from previous experience that the WASH-1400 analysis is basically sound, this work examines details of the RPS evaluation to assure ourselves of this perception. The results of the sensitivity study given in Figure 6-1 show a reduction of one order of magnitude in RPS unavailability diminishes this system's risk contribution from 23% to 3% of the total. Thus, small changes in RPS unavailability result in significant impact upon total risk.

In order to accomplish this analysis, the WASH-1400 assumptions must be carefully followed both in the determination of the RPS unavailability and in the application of any new RPS results to the WASH-1400 risk model. This is true since the overall model includes balanced conservative assumptions in each of the system models which are based on engineering judgement.

In this analysis, therefore, the following WASH-1400 assumptions are retained: (1) failure to scram is defined as three adjacent rod failures; (2) a common-mode human error is assumed in the reactor protection logic system due to miscalibration or damage to logic circuit switches; and (3) possible direct fault initiators such as sabotage, fires, floods, earthquakes, and other natural disasters are not included in the detailed system trees. This does not reflect the most recent methods of organizing and modeling common failure modes and external initiating events, but to perform on all new analysis using a different approach (i.e., wherein conservatism

in WASH-1400 that is not justified on the basis of new information or design changes is removed) would not be correct if inter-system risk comparisons using WASH-1400 are to be made.

The re-evaluation of the BWR RPS system yielded a fault tree in which the contribution from three adjacent rod failures was found to be the only major contributor altered. This change is due to the re-evaluation of the data base for the failure rate of single BWR control rods and from the incorporation of a more detailed model to calculate the combined three-rod failure likelihood.

The WASH-1400 data base for single control rod failures uses combined PWR and BWR 1972 data to obtain an average failure rate for all reactors considered. The present work used control rod failure data through December 1975 which were obtained from the Nuclear Safety Information Center. Analysis of the BWR data contained therein resulted in a median failure probability of 8.9×10^{-6}/demand.

The new results for RPS unavailability shown in Figure 6-2 and Table 6-2, show that the median value is now approximately a factor of six smaller than that in WASH-1400 and the mean value an order of magnitude smaller. The new standard deviation is also smaller since the tree adjacent rod failure contribution was modeled as a normal distribution with less dispersion than the log-normal distribution used in WASH-1400.

TABLE 6-2. Comparison of WASH-1400 and New Results for RPS Total Unavailability per Demand

	WASH-1400 Results	New Results
Median	1.3×10^{-5}	2.3×10^{-6}
Mean	5.3×10^{-5}	5.2×10^{-6}
Standard Deviation	2.1×10^{-4}*	9.6×10^{-6}
90% Confidence Interval Bounds		
Upper:	4.8×10^{-5}	2.0×10^{-5}
Lower:	4.3×10^{-6}	5.2×10^{-7}

*Not reported, calculated by SAI.

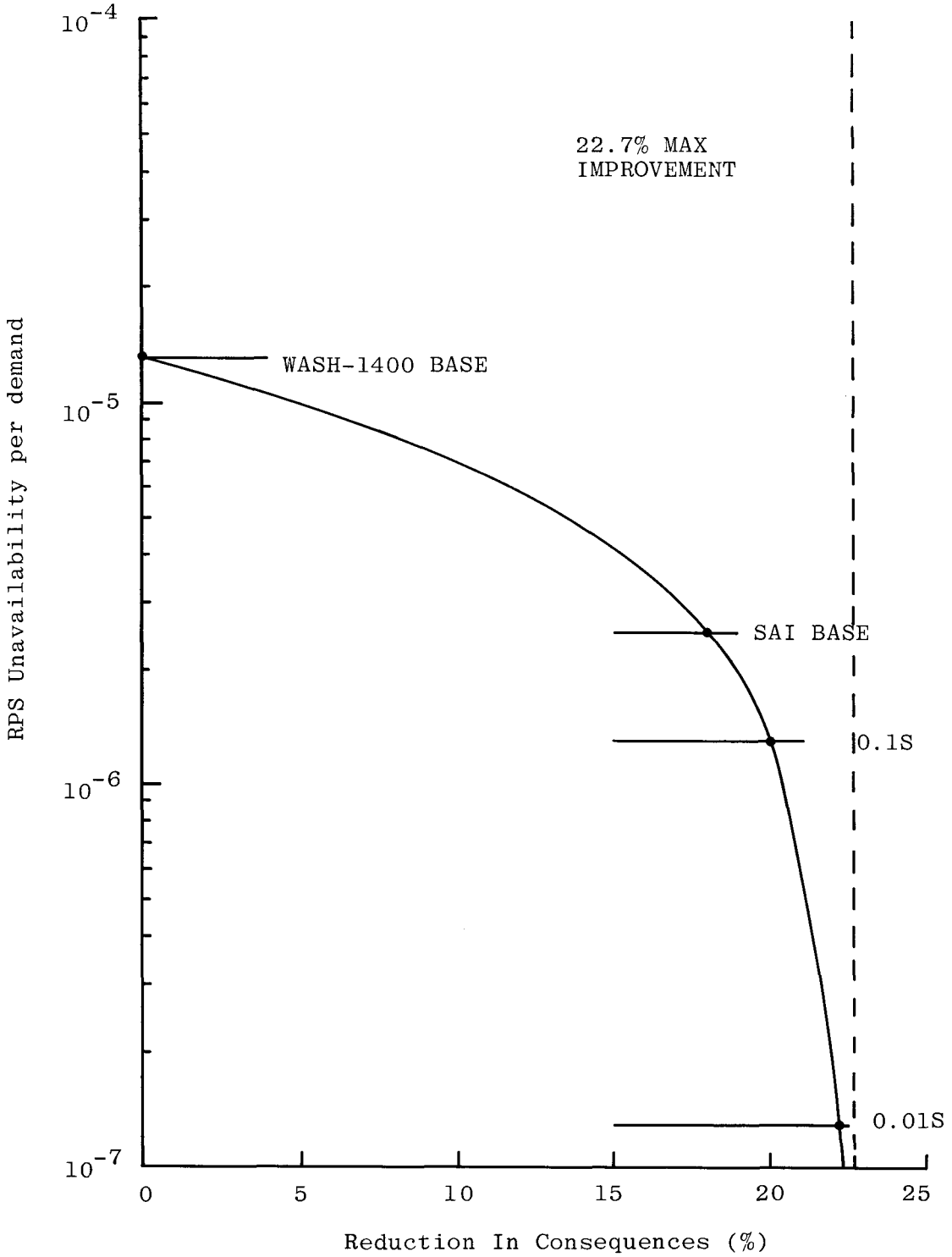


Figure 6-1. Reduction In Consequences Versus RPS Unavailability for the BWR

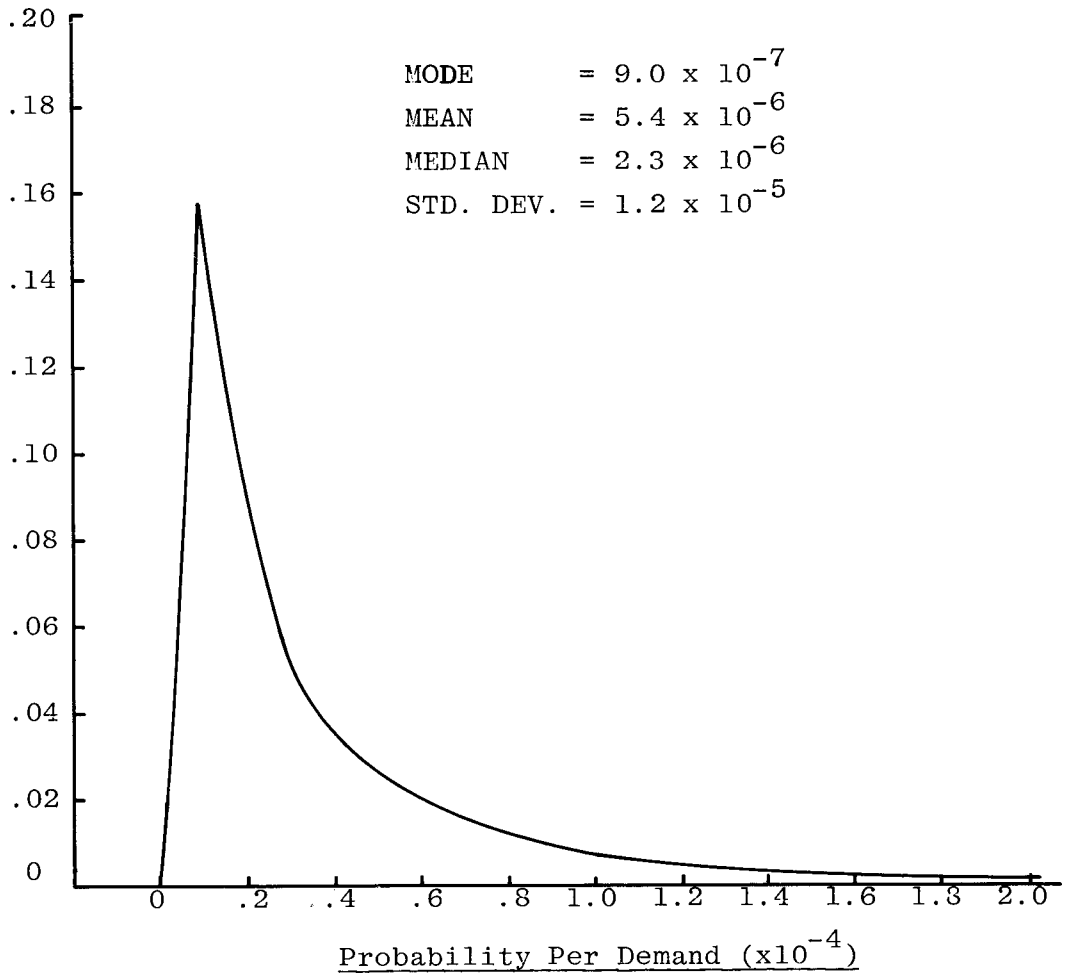


Figure 6-2. BWR RPS Unavailability Probability Density Function Using SAMPLE-A Code with 4,000 Monte Carlo Trials.

The most significant contributors to the new RPS unavailability (about 98.6% of the total) are: common-mode human error arising from miscalibration or damage to switches that directly or indirectly produce a trip signal (~83.8%) and a test and maintenance fault (~14.8%). Failure to insert three adjacent rods contributes an insignificant 1.4% to the total unavailability.

The principal contributor to the RPS unavailability, the common-mode human error in the RPLS, did not receive an extensive analysis in this evaluation as sufficient detailed information was not available. It was, thus, necessary to incorporate the fault directly from WASH-1400 in order to complete the quantitative evaluation; however, it must be noted that the unavailability value for the common-mode error described is based upon a test error rate which includes the entire set of miscalibration errors. These include calibration errors which result in very late actuation or complete failure to actuate will result in failure to achieve a reactor trip. Hence, the common-mode unavailability value which results is conservative and may be reduced by a more complete evaluation. Even so, common-mode unavailability may remain as a major contributor to RPS unavailability if the other major contributors should be similarly reduced in future evaluations.

6.2.3 Impact

Figure 6-1 shows that the SAI RPS failure probability of 2.3×10^{-6}/ demand causes about an 18% reduction in the total consequences. Further improvement in scram system reliability will yield only a small additional reduction in consequences. This logic requires further qualification, however, since we are comparing a mixture of SAI and WASH-1400 models.

Similar calculations might produce the same relative reductions in the other systems. The contribution of the RPS system to overall risk would then remain the same, although the total risks would be reduced. We believe this not to be the case, however, for the following reasons:

1. Referring to the RPS fault tree analysis, it is seen that equivalent levels of conservatism were maintained. Any differences are due mainly to technical changes which are quite unique to the RPS system.

2. The use of separate BWR and PWR control rod failure data is founded on the basis that these components are physically quite different in their operation. This is not true for the majority of other system components.

3. The counting technique for finding the likelihood of three adjacent rod failures is also unique to the RPS system and thus,model changes and distribution mixing alterations applied here should not have a large impact on the quantification of other systems.

Thus, the qualifications, the overall risk impact of BWR scram failure is seen to diminish by SAI analysis to the point that further RPS system availability improvement by design or analysis would be nearly meaningless. Errors in this statement induced by using the remaining WASH-1400 system models appear not to be large although similar analysis of these systems is suggested before the extent of these changes is known.

SECTION 7

RELIABILITY DATA BASE AND FEED COMPUTER CODE

Any probabilistic analysis requires data describing the reliability of the elements of the system. The quality of the data and its applicability to the analysis being accomplished is directly reflected in the result and thus is critical to the analysis. For this reason, a study of the feasibility of developing an operational nuclear data base from actual plant experience was accomplished, resulting in the development of a FORTRAN program named the File of Evaluated and Event Data (FEED) for the management of reliability data. FEED, written for the CDC 7600 computer, provides the means of storing current and future data on personnel, component, and system failure rates for use in safety and availability analyses. In addition, it provides storage of the information necessary to determine new failure rate assessments, i.e., (1) individual failure events, and (2) the number of components at risk. The individual failure events are drawn from the abnormal occurrence Regulatory Guide 1.16[40]. Significant low failure rate data, such as pipe rupture, is obtained from other sources such as the Navy and the Department of Transportation.

In a sense, the event data part of this work is a computer-assisted continuation of work began for the Reactor Safety Study and reported in WASH-1400[7]. The design of FEED was executed after careful consideration of NCR experience, as well as various other data management programs. Key-word search was rejected because of: (1) the requirement to store evaluated data, event data and plant data, (2) slowness, and (3) the possible loss of information through the use of synonyms. Instead, FEED uses a data mask that includes descriptors of the "categories" of the free-text data that follows it. To retrieve information, a search mask containing the desired search descriptor in each category is compared to all of the data masks in the library. When agreement is found, the data is printed. If a category is not given a specific descriptor, i.e., if it is left blank, it is considered "defaulted" for the search and everything in that category is retrieved.

In addition to the data, FEED contains a library of three-letter mnemonics, each of which is paired with a ten-letter literal descriptor. There is a mnemonic (and a ten-letter literal descriptor) for each search category except for docket, date and data type. When new data is entered in the library, the mnemonics in the data mask are compared with those stored in the library. After matches in all categories have been obtained, the mnemonics are packed into two 60-bit computer words. Also contained in each binary data mask is a word count of the data in the entry. When data is being retrieved, the computer compares the binary search mask with the binary data masks. It skips the data following each mask by using the word count of that data contained in the data mask.

To illustrate, a search on Docket 50-259 would retrieve all information on the Brown's Ferry 1 Nuclear Power Plant while a search on 50-259 and 3/75 and PER would retrieve all personnel-caused failures at Brown's Ferry 1 during March 1975.

The first three items in Table 7-1 are self-explanatory. Plant type includes PWR, BWR, HTGR, LMFBR, (fuel) fabrication and reprocessing plants, as well as chemical and fossil plants. Failure cause includes such categories as design, construction, personnel, natural, etc. Plant status is self-explanatory.

TABLE 7-1. Data Search Categories in FEED

Category	Number of Parameters in Use
Docket Number	-
Month of Occurrence	-
Year of Occurrence	-
Data Type	4
Plant Type	8
Failure Cause	16
Plant Status	11
Subsystem Category	49
Component Class	62
Component Type	40

Subsystem category includes such items as the core, cooling, engineered safety, containment, and subcategories of these. For example, instead of searching the general category of engineered safety, a search may be limited to emergency core cooling or residual heat removal, etc. Component class and component type are paired together in the program so that a search may be conducted, e.g., on valves, motor operated. This results in different numbers of component type parameters in use for different component classes. The maximum number of component type parameters is use, as shown in Table 7-1, is 40 -- for valves. Using a mean value of 10 for the number of component types is use, it is found that there are about 10^7 combinations of search parameters.

Figure 7-1 shows an example of the output from FEED for Docket 50-220. Currently, there are 2,900 events with 12,000 masks in the FEED data file. In the case of multiple causes, loss of information is prevented by specifying multiple masks for the same event. For example, the failure cause field for a worn component discovered during a routine inspection would be specified both as "component wear" and "inspection".

The program is capable of reading event data from tape, cards, or both and searching the event data for any combination of the categories listed in Table 7-1. There is no editing capability currently available for the event data. It is anticipated that an editing package will be developed in the near future.

```
 220 -0 -0-0


THIS IS A SEARCH FROM THE FILE OF EVALUATED AND EVENT DATA (FEED)


-------------------------------SEARCH PARAMETERS-------------------------
DOCKET  EVENT DATA  PLANT   CAUSE   PLANT     SUBSYSTEM COMPONENT COMPONENT
NO.     DATE  TYPE  TYPE            STATUS    CATEGORY  CLASS     TYPE

50-220

        22003701BWROTROPNMSTVLVRLF                                          178
        NINE MILE POINT-1 ELECTR. REL. VALVE ACTUATIONS FOR PERIOD OCT.?69 THRU MAR.1970
          DATE    RV-111  RV-112  RV-113  RV-121  RV-122  RV-123
        OCT.1969   1CYC    1CYC    2CYC    1CYC    1CYC    2CYC  MANUAL AT STARTUP TESTS
          THRU       -     1CYC    1CYC    4CYC    2CYC    2CYC  MANUAL AT PERIOD. TESTS
        MAR.1970  (NO ACTUATIONS FROM APRIL 1970 THRU MARCH 1971)
        REF. EVENT 03/--/70 *  LTR 01/18/74 *  ORC 03/31/70    *


        22012731BWROTROPNMSTVLVRLF                                          179
        NINE MILE POINT-1 ELECTR. REL. VALVE ACTUATIONS FOR PERIOD APR.?71 THRU DEC.1973
          DATE    RV-111  RV-112  RV-113  RV-121  RV-122  RV-123
        TO/09/71   2CYC    1CYC    1CYC    1CYC    1CYC    1CYC  MANUAL AT PERIOD. TESTS
        TO/03/72   3CYC    1CYC    3CYC    4CYC    3CYC      -   AUTO   AT NORMAL OPER.
        TO/09/72   1CYC    4CYC    1CYC    1CYC    1CYC    1CYC  MANUAL AT PERIOD. TESTS
        TO/03/73   2CYC      -     1CYC    2CYC      -     1CYC  AUTO   AT NORMAL OPER.
        TO/12/73   3CYC    3CYC      -     3CYC    3CYC      -   AUTO   AT NORMAL OPER.
        TO/12/73   1CYC    1CYC    2CYC    1CYC    1CYC    1CYC  MANUAL AT PERIOD. TESTS
        REF. EVENT 12/--/73 *  LTR 01/18/74 *  ORC 12/31/73    *
```

Figure 7-1. Example FEED Output

SECTION 8

INVESTIGATION OF SAFETY ANALYSIS VERIFIABILITY

8.1 Introduction, Summary and Conclusions

Extensive analyses of reactor safety have been, and are being, performed with very little experience or experimental confirmation that these analyses predict reality. Herein are presented the results of a brief investigation into safety analysis verifiability.

The goal is to establish that the total system unavailability can be accurately predicted utilizing system reliability modeling techniques (such as fault tree analysis). These techniques can result in errors in the system unavailability estimate for several reasons. These include:

1. Errors in component data - The data which represents the probability that the system components fail is either incorrect and/or incomplete.

2. Errors in system definition - The schematics, diagrams, and operating procedures are incorrect or incomplete.

3. Modeling techniques are limited by evaluation tools - The tools available to evaluate the reliability model (usually a computer code) cannot evaluate a model of the complexity necessary to properly model the system.

4. Modeling is incorrect or simplifying assumptions are unjustified - During the modeling, the analyst has overlooked a failure or has left off a significant failure, assuming its contribution unimportant.

Because of the multiple error sources, a comparison of only the predicted probabilities and actual probabilities at the system level does not allow identification of the significant error sources. Thus, the evaluation of the reliability model must include qualitative as well as quantitative results. That is, the model must be analyzed to determine what combinations (or sets) of events lead to the system failure (termed "cut sets" in fault tree analysis) together with the probability of these sets occurring. For comparison, then, not only is the actual system failure recorded but the particular set of events which occurred leading to the system failure must be recorded. With this additional information, the error sources can be separated. For example, suppose testing results in the system being failed by components A and B with a probability of P(AB). First, the presence of the event AB in the evaluation of the model should be verified. If the model does not include this set, then the analyst has made a modeling error, the system definition was incorrect, or the evaluation technique did not detect this set. Examination of the analyst's model of the system and the system definition should reveal the cause of error. The other possible error is that the evaluation predicts a different probability for the set AB. This could be due to data error or incorrect modeling of the events, such as not including a dependency.

The high reliability of a safety system is achieved through redundancies such that multiple coincident failures are necessary to fail the system. It is this high reliability of the safety systems which makes experimental verification difficult. That is, it takes a "long time" to collect data on system failure. Thus, the major difficulty to be overcome is the choice of a complex system of high reliability, which can be tested and results obtained in a reasonable time. It should be noted that there are methods of accelerating testing, such as accelerating failure rates of parallel testing several systems (see Section 8.2 below) or perhaps a system could be chosen that is less reliable than a safety system in order to obtain test results in a reasonable time length. Another possible compromise would be to allow a complex system to be analyzed via fault tree analysis, and then simulated via Monte Carlo simulation, and the results compared. This partial test would only detect such things as modeling errors; it would not include data verification.

It is interesting to note that some comparative information is available in literature, but details of result differences were not obtained in these studies (results of this literature search are given in Section 8.3 below). In conclusion, verifying reliability modeling techniques can and should be accomplished by one of the following plans. The best results would be obtained in Plan 1; however, Plan 2 could be implemented instead of Plan 1, for partial verification, or together with Plan 1 for additional information.

Plan 1 - Full Verification

A system should be chosen which is maintained to a high degree of readiness, that responds to a demand whose occurrence in time is unpredictable, is well-documented and exists in sufficient numbers to allow accelerated testing by parallelism. A suggested system could be the availability of a fire engine to respond to an alarm. This type of system may: (1) exist locally, (2) exist in sufficient quantity to allow gathering of data, and (3) be maintained rigidly to written procedures. Such a test program would require cooperation from a fire department, but it could offer them information on their equipment availability.

Plan 2 - Partial Verification

If only partial verification of reliability prediction techniques is desired, a fault tree versus computer system simulation could be accomplished. As discussed previously, this type of test would not verify all aspects of the reliability modeling process.

8.2 Accelerated Testing*

Testing is any procedure or action that causes an object in a known environment to exhibit its properties. On the basis of repeatability, statistical inferences may be made with regard to the object's future properties. In a sense, the routine operation of reactor power plants is a test program. The difficulties with simply waiting to determine performance are: (a) a prior knowledge bounding the risk is needed because of the

*An extensive list of references on this subject can be found in two recent articles by W. Nelson[41,42].

ramifications of reactor accidents; (b) imprecise environmental definition; and (c) design evolution.

8.2.1 Parallel Testing

From a statistical veiwpoint, a test of a single component for a time nT is equivalent to a test of n identical components for a time T. This assumes that components being tested do not experience "wear out" with age. Thus, parallel testing accelerates statistical data acquisition in proportion to the number of items at test. The obvious constraint on this technique is the cost. It should be performed in a precisely determined environment matching that anticipated in normal operation or under accident conditions depending upon the required data.

A method of reducing the cost of parallel testing is to test smaller objects with known scaling relationships to the real items. Examples of this are the 1/30 and 1/12 scaled reactor vessel tests of sodium slug containment for the LMFBR program. Another example is turbine fragment penetration tests. The results of these tests directly impact reactor costs. The cost reduction due to scaled tests may permit parallel testing and accelerated data accumulation.

8.2.2 Environmental Acceleration

Through imposing adverse operating conditions on the test components, their lifetime may be shortened and data gathered more rapidly. In order to use this information, a physical or phenomenological understanding of the failure mechanism is required.

Arrhenius Model

For diffusion-like failure mechanism the Arrhenius model (Maxwell-Boltzmann distribution) is used. This is one of the few cases for which the accelerated test model has a firm physical foundation. Because of the general applicability of the Arrhenius model, special plotting paper is available on which the data plot into straight lines. (The Arrhenius model may also be considered to be log-normally distributed.)

The model is usually considered applicable to temperature acceleration but could also be applied for accelerated activation energy.

Stress Acceleration

Stress acceleration is treated as a power-law distribution which means a parametric phenomenological fit.

Voltage Acceleration

Voltage acceleration is modeled as a power-law and, with some physical basis, as a Weibull distribution.

8.3 Literature Review

A brief literature survey indicated a scarcity of information on experimental verification of reliability analyses, especially for safety-oriented systems which are designed in accordance with the single failure criterion.

8.3.1 Bounds of a Quantitative Assessment

Green and Bourne[43] and Green[44] compiled some comparisons between predicted and actually achieved reliability. They defined a ratio, r, of the value of a particular observed failure rate to the corresponding predicted rate. A ratio of unity means, of course, that the prediction is apparently exact; a ratio of less than unity means that this prediction was overestimated. In the past, a number of systems or elements of systems have been analyzed at the design or production stages and the data on their reliability performance subsequently collected during a reasonable sample period of practical usage. The above authors give a typical example of about 50 different system elements[43] examined in this way. In these references, the ratio r is plotted on log-normal probability paper. The closeness of this plot to a straight line indicates the degree of correspondence of the distribution of r to a log-normal distribution. From the plot, it can be seen that the median of r is 0.76, that the change of the ratio r being within a factor of 2 if the median value is 70%, and that the change of the ratio being within a factor of 4 is 96%.

This means that the results of a reliability analysis of a system performed with due care and attention can reasonably be expected to yield numerical values within a factor of 2 of the actual values and can be expected to be within a factor of 4 with quite a high degree of confidence.

The fact that r was found to be a random variable was expected and is believed to arise from the following two causes:

1. Variability in prediction due to:
   A. Method of analysis;
   B. Assumptions in the mathematical model;
   C. Errors in the component part data.

2. Variability in observation due to the method of recording system performance. Typically, for instance, errors arise in practice due to difficulties in detecting, classifying, timing and recording all changes and fault modes of an actual system.

There is virtually no information presented in reference 43 describing what systems or subsystems were included in the study. No information was given on how the systems were selected or how the data were obtained. It is fair to assume that the systems considered in this study did not possess the safety-related features dictated by the single failure criterion. The importance of the results, however, is in quantitatively defining the expected accuracy, or accuracy bounds, of comparisons between measured (or observed) and predicted reliability.

8.3.2 Example - Machine Systems

Another example of good agreement between predicted and observed reliability is shown in Reference 44.

The example compares results obtained on reliability of machines in die-casting factories. The predicted numbers were based on analysis of the two machine systems by breaking them down into detailed component parts and reliability parameters allocated to each part. These results obtained from two generically different machines, Type A and Type B, are compared to observations made on other machines in different factories; a good correlation

between predicted and measured results is shown. The overall predicted failure rate is about half of the overall recorded failure rate and this ratio is approximately true for most of the main subsystems. This is within the accuracy that would be expected from prediction techniques.

8.3.3 Example - Electronic Circuit

Another example of interest in the area of electronic circuits is presented by Breipohl and Corbett[45]. Their paper describes the results of predicting the reliability of an electronic circuit subjected to irradiation by neutron fluxes. The mean and the variance of the circuit output and the reliability are predicted based on the test data on components exposed to different levels of neutron dose. The reliability results are obtained by incorporating the test data in a computer model of the electronic circuit. These predictions are compared with the results of actual tests on the circuit. The result of this comparison is shown in Table 8-1, below.

TABLE 8-1. Probability of Failure of the Circuit

Dose (neutron/cm^2)	Calculated	Measured	Calculated from revised Measured Parameters
3×10^{14}	0.83	0.1	0.12
6×10^{14}	1.00	0.94	0.90

The discrepancy between the predicted and measured probability of circuit failure is quite substantial for the case of the smaller dose. The errors were found to be associated with an incorrect mean and standard deviation in the transistor data due to the limit of accuracy of the tester. In fact, the tester introduced a bias of 3%. Shifting the distribution by that amount yielded calculated reliability data much closer to the measured ones as is shown in the last column. This example elucidates the importance of obtaining data on the components or subsystems with accuracy commensurate to the problem at hand. Obviously, when dealing with failure rates of 10^{-6} and 10^{-8}, as in the case of power reactors, the required accuracy of the failure rate of the subsystems is not as stringent as in the example, but it is still of importance.

8.3.4 Example - Aerospace Systems

Few examples of comparisons of prediction versus experience in the aerospace industry are available. Table 8-2, below is such a comparison[47].

TABLE 8-2. Prediction Versus Experience for Aerospace Systems

System	Predicted Results	Observed Results
Lunar Orbiter	0.56	0.8
Apollo/Saturn S-1C (1st stage)	0.95	0.93
Booster	0.97	1.0
Liquid Hydrogen Insulation faults (Apollo/Saturn 2nd stage)	8 to 19	18
Minuteman command/ destruct (classified data)	Predicted data matched actual	

The prediction in the first case, the lunar orbiter, was made by adding up all failure rates of parts that had to function in order for the orbiter to perform. Thus, the results attest more to an impressive ability to estimate the reliability of key components in their operating environment than to the adequacy of the reliability methodology. Similar remarks probably apply to the other systems mentioned in Table 8-2. However, the booster program involved a more sophisticated reliability analysis and redundancies were taken into account. The good agreement between predicted and observed results in this case is remarkable.

8.3.5 Example - Reactor Related Systems

As a means of indicating the validity of the FTA approach used in WASH-1400[46], system unavailability data were obtained on two systems which were similar to those evaluated in the study. The comparison between the prediction and the observed data is shown in Table 8-3 below.

TABLE 8-3. System Unavailability (Q)

System	Q-Observed	Q-Upper	Calculated Q-Median	Q-Lower
High Pressure Coolant Injection (HPIS)	1×10^{-1}	1.4×10^{-1}	9.8×10^{-2}	6.8×10^{-2}
Containment Spray Injection (CSIS)	1×10^{-3}	7.8×10^{-3}	2.4×10^{-3}	1.0×10^{-3}

The calculated unavailability* values are in relatively good agreement with the observed unavailability values. The r index is about 1 in the first case and about 0.4 in the second case. These indices fall within the expected range for a log-normal distributed r as explained in Section 8.2.1. It should be noted that Q-observed was obtained as a ratio of one-half of the number of failures to the number of demands (tests) as reported in the AEC incident reports, apparently under the implicit assumption that, on the average, 50% of the system's failures occur on demand.

The high unavailability rates for the HPIS system shown in Table 8-3 indicate that the high pressure coolant injection system fails when any of the three pumps present in that system fail. The observed data apparently is obtained from the one pump which is being used in normal reactor operation. This is substantiated by the failure probability values in WASH-1400[48]. Thus, while the comparison between observation and prediction in this case is important and useful in verification of the validity of the methodology and the basic data used, it cannot be considered definitive since it does not reflect the complexity of a safety system which complies with the single failure criterion.

The comparison made on the containment spray is somewhat more significant from the point of view of a safety system. The CSIS consists of two

*The calculated unavailability did not use only component data involved in the specific systems observed. Rather generic data were used for calculations; e.g. data on pumps in chemical plants were used to develop pump failure data applied to the nuclear plant system.

redundant spray subsystems from the refueling water storage tank (RWST) to the containment. Failure of CSIS is considered to be failure to deliver spray fluid from the RWST to the containment atmosphere at a rate at least equivalent to the full delivery from one of the two containment spray pumps. Normal tests of the CSIS are confined to the system outside the containment and apparently involve the test of individual pumps and valves. Thus, the effect of full redundancy is not directly measured but inferred from the component measurements. This may diminish the significance of the above-mentioned comparison as a stringent test of the validity of the fault tree analysis methodology and of the data input.

The survey of the literature described in this section shows the scarcity of comparisons between observed and predicted reliability. The available information is nonetheless very useful. It shows that an index describing the ratio between observed and predicted reliabilities (at least some cases) complies empirically with a log-normal distribution. This fact may assist in defining the bounds of accuracy in future predictions of system reliabilities. Several examples of reasonably good agreement between predicted and observed reliability in various industrial areas, including reactor safety systems, were discussed. It should be noted, however, that the systems discussed were not of the type which are of high reliability. Hence, while previous studies increase the credibility of the various predictive reliability techniques, they do not provide the necessary comparison of measured vs predicted reliability of high reliability safety systems.

REFERENCES

1. R.C. Erdmann, et al, "Probabilistic Safety Analysis," prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report 217-2-4, July 1975.

2. R.C. Erdmann, "Quarterly Progress Report for the Period March 15 - June 15, 1975," submitted to EPRI from Science Applications, Inc., SAI/SR-117-PA.

3. R.C. Erdmann, "Quarterly Progress Report for the Period June 16 - September 15, 1975," submitted to EPRI from Science Applications, Inc., SAI/SR-122-PA.

4. R.C. Erdmann, "Quarterly Progress Report for the Period September 16 - December 15, 1975," submitted to EPRI from Science Applications, Inc., SAI/SR-137-PA.

5. A.A. Garcia and R.C. Erdmann, "Summary of the AEC Reactor Safety Study (WASH-1400)," prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report 217-2-1, April 1975.

6. F.L. Leverenz and R.C. Erdmann, "Critique of WASH-1400," prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report 217-2-3, June 1975.

7. Reactor Safety Study (WASH-1400), U.S. Atomic Energy Commission, Draft - August 1974, Final - October 1975 (NUREG 75/014).

8. J.E. Kelly, F.L. Leverenz, N.J. McCormick and R.C. Erdmann, "Sensitivity Assessments in Reactor Safety Analysis," prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report 217-2-6, February 1976.

9. F.L. Leverenz, J.E. Kelly, A.A. Garcia and R.C. Erdmann, "PWR Sensitivity to Alterations in the Interfacing-Systems LOCA," prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report NP-262, September 1976.

10. "Anticipated Transients without Scram for Water-Cooled Power Reactors", WASH-1270, U.S. Atomic Energy Commission, September 1973.

11. ATWS: A Reappraisal, Part I (Draft) "An Examination and Analysis of WASH-1270, Technical Report on ATWS for Water-Cooled Power Reactors," submitted to EPRI from Science Applications, Inc.

12. ATWS: A Reappraisal, Part II (Draft) "Evaluation of Societal Risks Due to Reactor Protection Failure," Volume 1 BWR Risk Analyses, submitted to EPRI from Science Applications, Inc.

13. ATWS: A Reappraisal, Part II (Draft) "Evaluation of Societal Risks Due to Reactor Protection Failure," Volume 2 BWR Fault Tree Evaluation, submitted to EPRI from Science Applications, Inc.

14. Reactor Safety Study (Draft), "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Summary Report," WASH-1400, U.S. Atomic Energy Commission, August 1974.

15. Reactor Safety Study (Draft), "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, U.S. Atomic Energy Commission, August 1974.

16. Reactor Safety Study (Draft), WASH-1400, Appendix I, "Accident Definition and Use of Event Trees," U.S. Atomic Energy Commission, August 1974.

17. Reactor Safety Study (Draft), WASH-1400, Appendix II (Vol. 1), "Fault Tree Methodology," U.S. Atomic Energy Commission, August 1974.

18. Reactor Safety Study (Draft), WASH-1400, Appendix II (Vol. 2), "PWR Fault Trees," U.S. Atomic Energy Commission, August 1974.

19. Reactor Safety Study (Draft), WASH-1400, Appendix II (Vol. 3), "BWR Fault Trees," U.S. Atomic Energy Commission, August 1974.

20. Reactor Safety Study (Draft), WASH-1400, Appendix III, "Failure Data," U.S. Atomic Energy Commission, August 1974.

21. Reactor Safety Study (Draft), WASH-1400, Appendix IV, "Common Mode Failures," U.S. Atomic Energy Commission, August 1974.

22. Reactor Safety Study (Draft), WASH-1400, Appendix V, "Quantitative Results of Accident Sequences," U.S. Atomic Energy Commission, August 1974.

23. Reactor Safety Study (Draft), WASH-1400, Appendix VI, "Calculations of Reactor Accident Consequences", U.S. Atomic Energy Commission, August 1974.

24. Reactor Safety Study (Draft), WASH-1400, Appendix VII, "Release of Radioactivity in Reactor Accidents", U.S. Atomic Energy Commission, August 1974.

25. Reactor Safety Study (Draft), WASH-1400, Appendix VIII, "Physical Processes in Reactor Meltdown Accidents", U.S. Atomic Energy Commission, August 1974.

26. Reactor Safety Study (Draft), WASH-1400, Appendix IX, "Safety Design Rationale for Nuclear Power Plants", U.S. Atomic Energy Commission, August 1974.

27. Reactor Safety Study (Draft), WASH-1400, Appendix X, "Design Adequacy", U.S. Atomic Energy Commission, August 1974.

28. Reactor Safety Study, WASH-1400 (NUREG 75/14), Appendix XI, "Analysis of Comments on the Draft WASH-1400 Report", U.S. Nuclear Regulatory Commission, October 1975.

29. John J. D'Azzo and Constantine H. Houpis, Feedback Control System Analysis and Synthesis, p. 469-470, McGraw-Hill, 1966.

30. E.T. Rumble, F.L. Leverenz and R.C. Erdmann, "Generalized Fault Tree Analysis for Reactor Safety", Electric Power Research Institute, EPRI 217-2-2, June 1975.

31. Standard Review Plan, NUREG-75/087, U.S. Nuclear Regulatory Commission, September 1975.

32. Reactor Safety Study, WASH-1400, (NUREG-75/014) Volume 5 PP V-43 through V-44, U.S. Atomic Energy Commission, October 1975.

33. F.L. Leverenz, H. Kirch, User's Guide for the WAM-BAM Computer Code, prepared for Electric Power Research Institute by Science Applications, Inc., EPRI Report 217-2-5, January 1976.

34. N.Y. Gately, D.W. Stoddard, R.L. Williams, "GO: A Computer Program for the Reliability Analysis of Complex Systems", KN-67-704(R) Kaman Science Corporation, April 1968.

35. W.E. Vesely and R. Narum, "PREP and KITT: Computer Codes for Automatic Evaluation of a Fault Tree", Idaho Nuclear Corporation, Report IN-1349, August 1970.

36. Reactor Safety Study, WASH-1400 (NUREG 75/014), Appendix II, "Fault Trees", U.S. Nuclear Regulatory Commission, October 1975.

37. J.B. Fussel, E.B. Henry and N.H. Marshall, "MOCUS-A Computer Program to Obtain Minimal Cut Sets from Fault Trees", Aeroject Nuclear Co., Report UC-32, August 1974.

38. W.J. Van Slyke and D.E. Griffing, "ALLCUTS, A Fast Comprehensive Fault Tree Analysis Code", Atlantic Richfield Hanford Co., Report ARH-ST-112.

39. Code of Federal Regulations (10CFR100), 10 Energy, Parts 0 to 199, Revised January 1, 1975.

40. W. Nelson, "Analysis of Accelerated Life Test Data-Lease Squares Methods for the Inverse Power Law Model", IEEE Trans. on Reliability, Vol. R-24, 2, June 1975 (pp. 103-107).

41. W. Nelson, "Graphical Analysis of Accelerated Life Test Data with a Mix of Failure Modes", IEEE Trans. on Reliability Vol. R-24, 4, October 1975 (pp. 230-237).

42. Clinch River Breeder Reactor, "Preliminary Safety Analysis", Appendix C, 1975.

43. A.E. Green and A.J. Bourne, "Reliability Technology", Wiley Interscience (1973).

44. A.E. Green, "The System Reliability Service and Its Generic Techniques", IEEE Transactions on Reliability, August 1974, Vol. R-23, NO 3 (pp. 131-136).

45. A.M. Breipohl and W.J. Corbett, "Results of a Computer Prediction of After-Radiation Reliability", IEEE Transactions of Reliability, August 1971, Vol. R-20, No. 3 (pp 154-158).

46. Reactor Safety Study (Draft), WASH-1400, Appendix II, Vol. 1, "Fault Tree Methodology", U.S. Atomic Energy Commission, August 1974, (pp 88-101).

47. Ibid., Appendix III, "Failure Data" (pp 205-208, pp 214-217, pp 113-118).

48. Ibid., Appendix II, Vol, 2, "PWR Fault Trees" (pp 307-309).