NUREG/CR-1659 (2 of 4)
SAND80-1897 (2 of 4) Revised
AN

Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant

Gregory J. Kolb, Steven W. Hatch,
Peter Cybulskis, Roger O. Wooton

Printed January 1981
Revised May 1981

Sandia National Laboratories

Prepared for

US NUCLEAR REGULATORY COMMISSION

NOTICE

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1659/2of4
SAND80-1897/2of4

AN

REACTOR SAFETY STUDY METHODOLOGY APPLICATIONS PROGRAM: OCONEE #3 PWR POWER PLANT

Gregory J. Kolb
Steven W. Hatch

Sandia National Laboratories
Albuquerque, New Mexico 87185

Peter Cybulskis
Roger O. Wooton

Battelle Columbus Laboratories
Columbus, Ohio 43201

Printed: January 1981
Revised: May 1981

Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
for the
U. S. Department of Energy

Prepared for
Division of Risk Analysis
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1047

PURPOSE OF REVISION

This document is a revision of the report originally published in January 1981. The revision primarily affects the list of accident sequences appearing in Table 6-1. Other minor editorial changes have also been included.

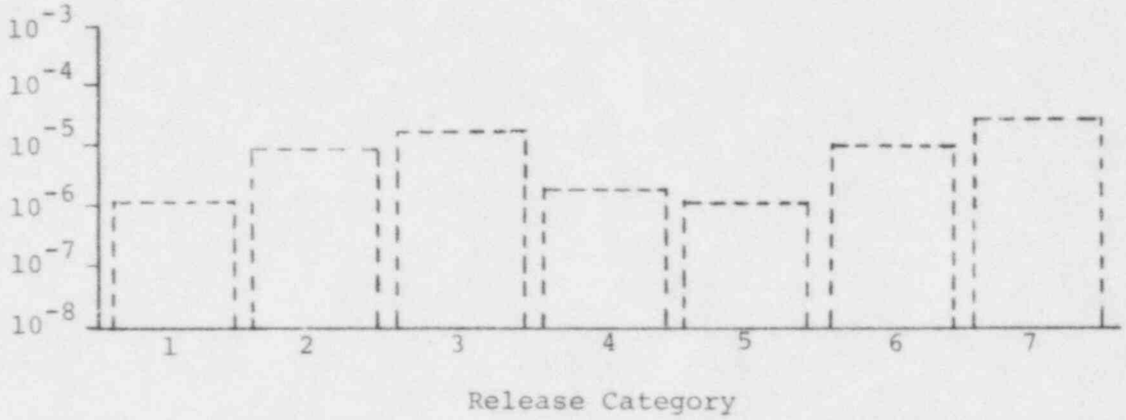
This document contains all the information included in the original report; therefore, it is recommended that the original report be destroyed.

EXECUTIVE SUMMARY

This volume represents the results of the analysis of Oconee Unit 3 nuclear power plant which was performed as part of the Reactor Safety Study Methodology Applications Program (RSSMAP). The RSSMAP was conducted to apply the methodology developed in the Reactor Safety Study (RSS) to an additional group of plants with the following objectives in mind: (1) identification of the risk dominating accident sequences for a broader group of reactor designs; (2) comparison of these accident sequences with those identified in the RSS; and (3) based on this comparison, identification of design differences which have a significant impact on risk.

Significant use of RSS insights and results was made for the Oconee analysis. Loss of coolant accidents (LOCAs) and transients were used as initiating events and the release categories and human error and component failure data bases were the same as those used in the RSS. The transient and LOCA event trees for Oconee differ somewhat from the RSS event trees. This is due to different systems and interactions among systems at Oconee. In addition, the RSSMAP transient and LOCA trees are interrelated in recognition that transient initiating events may ultimately lead to LOCA conditions. Unlike the RSS, detailed fault trees were not used to identify all possible failure modes; rather, a "survey and analysis" technique was used to identify the most likely failure modes of a system. The determination of which accident sequences result in core melt and the subsequent containment response and release was made by the MARCH and CORRAL codes which are significantly more developed codes than those available when the RSS was performed. No site specific consequence analysis was performed.

Results of the Oconee RSSMAP analysis can be summarized in the histogram below, which depicts the total accident sequence frequency in each of the seven PWR core melt categories used in the RSS.



Oconee Dominant Accident Sequence (Using RSS Smoothing Technique)

The most significant sequences contributing to both the core melt frequency and the risk were one of three types: (1) transient initiated sequences which involve loss of all feedwater, high pressure injection, and, in some cases, loss of containment systems, (2) small LOCAs with failure of emergency core cooling in the early or late recirculation phases, and (3) anticipated transients without SCRAM sequences.

The total frequency of core melt has been predicted to be similar for Oconee and Surry (i.e., within a factor of two). The dominant contributors to the Oconee core melt frequency are significantly different than those for Surry, however.

FOREWORD

This report is the second in a series of four reports which present the results of analyses performed in the Reactor Safety Study Methodology Applications Program (RSSMAP). This volume describes the analysis performed for the Oconee Unit 3; other volumes describe the analyses of Grand Gulf, Sequoyah Unit 1 and Calvert Cliffs Unit 2. The RSSMAP analyses were an attempt to use insights from the relatively detailed and elaborate Reactor Safety Study analysis to perform a meaningful plant risk analysis with minimum manpower and economic impacts. It was also desired that the study of plants with differing reactor and containment designs would broaden the class of nuclear power plants explicitly analyzed in terms of risk.

The reader should be cautioned to consider these results in their proper context. As was true of all the RSSMAP plants studied, the Oconee analysis was conducted primarily with information available in the Final Safety Analysis Report (FSAR), Technical Specifications and selected plant procedures. This approach does imply some limitations in the depth of the analysis since as-built systems often differ from those depicted in FSAR drawings. Also, FSAR analysis and technical specifications generally indicate more conservative criteria and guidelines than are actually required for system success. It should also be noted that some developments in risk assessment methodology have been employed in the Oconee analysis which were not used in the earlier Sequoyah analysis. Among the most important of these involve the development of the transient event trees and the treatment of dominant accident sequences to include complement events. As a final point, it is acknowledged that, subsequent to the completion of the draft Oconee analysis, some changes in plant hardware or procedures have been made or are being planned which may have an effect on the probabilities of dominant accident sequences. However, due to the development of major new efforts in plant reliability analysis by both the nuclear industry and the Nuclear Regulatory Commission, an attempt to analyze the effect of these recent changes was not undertaken in this study.

Comments on this report and the RSSMAP methodology are invited. Comments should be sent to:

Chief, Reactor Risk Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555

CONTENTS

CONTENTS (Cont'd) PAGE

CONTENTS (Concluded)

APPENDICES

ACKNOWLEDGEMENTS

A number of people have contributed to this program during its existence, in particular,

*Stuart V. Asselin
Wallis R. Cramond
Jack W. Hickman
Sandia National Laboratories

Mario A. Fedele
Anthony J. Giacobbe
Robert B. Klaiber
Evaluation Associates, Inc.

Mark Cunningham
James J. Curry
Gordon Edison
Merrill Taylor
U. S. Nuclear Regulatory Commission

Richard Denning
Battelle Columbus Laboratories

The authors would also like to thank Emily Preston and June Christy for their help in typing and assembling this report.

*Presently employed by Technology for Energy Corporation.

1.0 INTRODUCTION

As a part of determining the public risk due to accidents in light water reactors (LWR), the Reactor Safety Study (RSS) (Reference 2) developed a methodology for evaluating risks associated with potential accidents at nuclear power plants. A number of organizations and individuals have recommended that the methodology developed in the RSS be used on a wider basis to analyze commercial power reactor systems and to assist in making informed decisions when public risk is a consideration. Further, it has also been stated by the Nuclear Regulatory Commission (NRC)[1] that ways should be examined in which the RSS methodology can be used to improve the regulatory process. In light of this, the Probabilistic Analysis Staff (currently the Division of Risk Analysis) of the NRC initiated a program in October of 1975, entitled "The Reactor Safety Study Methodology Applications Program (RSSMAP)," to provide a broader foundation for applications of the RSS methodology and engineering insights into the regulatory safety review process.

The RSS addressed two reactors, the Surry and Peach Bottom plants. For those two reactors, the accident sequences that dominated risk were identified. As a further application of the RSS methodology, the RSSMAP was conducted with the following objectives: (1) identify the risk dominating accident sequences for a broader spectrum of reactor designs, (2) compare these accident sequences with those identified for the reactors studied in the

[1]See NRC Annual Report to the President, 1975.

RSS, and (3) based on this comparison, identify design differences between the plants which have a significant impact on risk.

The Reactor Safety Study Methodology Applications Program was divided into two principal tasks: systems analysis of engineered systems, and analysis of the accident processes. Sandia National Laboratories was asked to perform the systems analysis task. This task was performed with the aid of Evaluation Associates, Inc., of Bala Cynwyd, Pennsylvania as a subcontractor. Battelle Columbus Laboratories was asked to perform the analysis of accident processes.

The RSSMAP study includes three PWR power plant designs and one BWR plant design. These designs are significantly different from those studied in the RSS. Table 1-1 identifies the RSSMAP plants, the RSS plant used for comparison, and some key design features.

This volume documents the RSSMAP results for the Oconee #3 unit. It is a 886 MWe Babcock and Wilcox PWR with a dry containment and is located on Lake Keowee, South Carolina. Oconee, owned and operated by the Duke Power Company, obtained their construction permit and operating license on November 6, 1967, and July 19, 1974, respectively. Oconee #3 entered commercial operation on December 16, 1974. Separate volumes will describe the RSSMAP results for each of the other plants studied.

Table 1-1

MAJOR CHARACTERISTICS OF RSS AND RSSMAP STUDIED PLANT

RSSMAP PLANT	RSS PLANT USED FOR COMPARISON
Sequoyah #1 PWR · Reactor Vendor - Westinghouse · Architectural Engineer - Tennessee Valley Authority · Four Reactor Coolant Loops · 1148 MWe · Ice Condenser Containment · Now in low power testing	Surry PWR · Reactor Vendor - Westinghouse · Architectural Engineer - Stone and Webster Engineering Corp. · Three Reactor Coolant Loops · 775 MWe · Dry Subatmospheric Containment · Commercial Operation on 12/72
Oconee #3 PWR · Reactor Vendor - Babcock and Wilcox · Architectural Engineer - Duke Power Co. with Assistance from Bechtel Power Corp. · Two Hot Leg Reactor Coolant Loops Four Cold Leg Reactor Coolant Loops · 886 MWe · Dry Containment · Commercial Operation 12/74	SURRY PWR
Calvert Cliffs #2 PWR · Reactor Vendor - Combustion Engineering · Architectural Engineer - Bechtel Power Corp. · Two Hot Leg Reactor Coolant Loops Four Cold Leg Reactor Coolant Loops · 850 MWe · Dry Containment · Commercial Operation 4/74	SURRY PWR
Grand Gulf BWR · Reactor Vendor - General Electric Co. · Architectural Engineer - Bechtel Power Corp. · BWR/6 Design · 1250 MWe · Mark III Containment	Peach Bottom BWR · Reactor Vendor - General Electric Co. · Architectural Engineer - Bechtel Power Corp. · BWR/4 Design · 1065 MWe · Mark I Containment

2.0 METHODOLOGY

As stated in Chapter 1, the RSS Methodology Applications Program consists of two principal tasks: systems analysis and accident process analysis. This chapter will discuss the basic methodology utilized in performing these tasks, differences from the methodology presented in the RSS, and important assumptions and restrictions used in performing the analyses. Details of how the methodology was applied to the analysis of the Oconee #3 power plant can be found in Chapters 4 and 5.

2.1 Review of RSS Methodology

Before discussing the RSSMAP methodology, a brief review of the RSS methodology may be useful in identifying similarities and defining differences between the two methodologies. In the RSS, the methodology consisted essentially of three basic tasks. These included: (1) a systems analysis task, (2) an accident process analysis task, and (3) a consequence analysis task. The first two correspond to RSSMAP tasks. The third task analyzed the accident sequences in terms of consequences to public health and property damage. This third task was not included in this study.

The initial step in the RSS systems analysis task involved the construction of functional event trees. These trees delineated the functions which must be performed by plant systems to mitigate an accident initiated by various loss of coolant accidents (LOCAs) or transients. For LOCAs, these functions were reactor subcriticality, emergency core cooling, post accident radioactivity removal, containment heat removal, and containment integrity. For transients, the required functions were reactor subcriticality, heat transfer to the environment, reactor coolant system overpressure protection, and reactor vessel coolant volume control. Then system event trees were constructed by identifying the plant systems needed to perform the required post-accident functions. After completing this, the system accident sequences were delineated and a detailed fault tree analysis was conducted on all the systems represented on the event tree to determine the failure modes and failure probability of these systems. In some cases, detailed fault trees were not needed if actual plant failure probability data existed. The fault trees were quantified using a component and human failure data base compiled as part of the RSS. The system failure probability was expressed in terms of a median value with an associated error bound. The tolerance bound was due to uncertainties in the RSS data base.

The final step of the RSS systems analysis task was the quantification of the accident sequences depicted on the system event trees. Any dependencies which existed among the systems in the sequence, which were not explicitly covered by the event tree structure, were identified (i.e., a shared system component) and incorporated into the quantification. System accident sequences with the highest frequencies were then analyzed in terms of accident processes.

The accident process analysis was conducted to determine (1) which of the dominant system accident sequences resulted in core melt (2), the response of the containment following an accident, and (3) for those sequences predicted to result in containment failure, the amount and types of radioactivity released to the environment. Containment event trees displaying potential containment failure modes were created for each system accident sequence. Probabilities of these failure modes were then estimated. The complete accident sequences (defined as a system accident sequence with its appropriate containment failure mode) were then assigned to one of nine PWR or one of five BWR radioactive material release categories. The categories were ordered in terms of severity with Category 1 representing the most severe radioactive material release. The accident sequence frequencies in each category were then summed in order to assess the release category frequency (per reactor year). It was recognized that there was an uncertainty associated with the release category placement of each sequence. To account for this, the RSS smoothing technique was used: that is, a probability of 0.1 was assigned to an accident sequence being in an adjacent release category, and a probability of .01 was assigned to an accident sequence being two release categories from the one in which it was placed, etc. After applying this technique, the final release category frequency was assessed.

The final RSS task was to analyze the release categories in terms of consequences to public health and property damage. This was accomplished through the use of various models depicting items such as meteorology, population evacuation, and population dose. Through the use of these models, the consequences of each release category were determined. Multiplication of the frequency of the release category and its associated consequence resulted in a risk estimate of each category. Summing the risk of all the release categories resulted in an estimate of the total power plant risk.

2.2 RSSMAP Methodology

The RSSMAP methodology is based on that used in the RSS. To meet, in an efficient manner, the objectives of the program stated in the introduction, insights and results from the RSS were used when appropriate. However, certain departures from the RSS methodology did occur and are summarized below.

During the development of the RSSMAP event trees it was found that the RSS functional event trees were basically applicable to the RSSMAP plants. A redefinition of one of these functions was made, however, for purposes of clarification. Specifically, the RSS LOCA function, containment heat removal, was split in the RSSMAP into two functions, namely containment overpressure protection during the injection phase and containment overpressure protection during the recirculation phase. Each of these functions is needed to prevent a containment overpressure failure; however, using the RSSMAP presentation, the analyst can more easily distinguish containment overpressures which occur early in the accident from those that occur late. This distinction is useful because the time at which the containment fails is important to accident consequences.

In addition to the LOCA function redefinition, two additional transient functions, which were previously implied in the RSS results, were defined. From the list of PWR transient sequences in Table V 3-7 of the RSS, it can be seen that containment systems (e.g., containment spray systems, events C and F) appear as part of the sequence even though they don't explicitly appear on the transient event tree. These containment systems provide the functions of containment overpressure protection and post accident radioactivity removal. In the RSSMAP, these functions have been explicitly added to the list of transient functions.

The plant systems required to perform the LOCA and transient functions were sometimes different in the RSSMAP plants. As an example, during a LOCA the containment heat removal function at Surry is performed through heat exchangers located in the containment spray recirculation system. At Oconee, this function is performed with heat exchangers located in the low pressure recirculation system and/or by the reactor building air fan cooling system. Further, many dependencies between the RSSMAP event tree systems were found to be different from those found in the RSS, thus resulting in changes in the event tree structure.

During the formulation of the event tree, it was decided that a single LOCA tree, rather than the three RSS LOCA trees, was an adequate representation of the plant response to a LOCA of any given break size. As a result of these differences in plant design and analysis, the RSSMAP system event trees for Oconee differ significantly from the RSS trees.

One of the insights gained from the RSS was that system failure probabilities are dominated by only a few failure modes such as single, double and common mode hardware and human failures. Because of this insight, elaborate fault tree models to identify all possible system failure modes, as was done in the RSS, were not developed for the RSSMAP. Instead, a "survey and analysis" technique was used to determine system failure modes. This technique was, in essence, a systematic approach by which the analyst searched for system failure modes. The search was done manually and was usually stopped when all double or triple failure modes were identified. A Boolean equation was then constructed for each system which represented these failure modes. These equations were utilized in the accident sequence analysis described later. (For an example of the "survey and analysis" technique, see Appendix B.) It should be noted that the failure mode search was based largely on systems information gained from the plant FSAR, a single visit to the plant, and some follow up conversations with plant personnel. It is recognized that this limitation in the study does not provide assurance that all system failure modes have been identified.

The RSSMAP system unavailabilities were quantified using the RSS hardware and human error data base, except for those systems where actual plant failure probability data existed. Throughout the course of this work, point estimate unavailabilities were used in determining the system failure probabilities ratner than the median unavailability with its associated error bound as was used in the RSS. This departure from the RSS methodology was made because the additional effort of estimating error bounds was not judged necessary for risk comparisons or the identification of dominant accident contributors.

The final step of the RSSMAP systems analysis task was the performance of a system accident sequence analysis to determine those core melt sequences with the highest frequency. This was done by combining the Boolean equations describing the succeeded and failed systems for each accident sequence, performing a Boolean reduction of the equations to produce sequence cut sets (i.e., the system failures which produce an accident sequence), and quantifying these cut sets using the data base. The cut sets for each accident sequence were summed to arrive at a total sequence frequency. The accident sequence Boolean reduction and cut set quantification was performed with the aid of the SETS and SEP computer codes (reference 5). In the RSS, the accident sequence analysis was performed largely by hand calculations. In some cases, this may have required some assumptions concerning interactions between systems in a sequence to make the calculations practicable. Such assumptions were unnecessary in the RSSMAP due to the increased analytical capability afforded by SETS and SEP. (For more details concerning the systems analysis task, see Chapter 4.)

System accident sequences identified with the highest frequencies were then analyzed in terms of accident processes. The accident process analysis task for the RSSMAP was conducted in a more detailed manner than was done in the RSS. Use was made of a new computer code known as MARCH, and an updated version of the CORRAL code (references 6 and 7).

The MARCH code, developed at Battelle Columbus Laboratories, performs LOCA and transient initiated accident calculations from the time of the initiation of the accident through the stages of blowdown (LOCA only), core heat up, boiloff, core meltdown, pressure vessel bottom head melting and failure, debris-water interaction in the reactor cavity, and interaction of the molten debris with the concrete containment base pad. The mass and energy additions into the containment building during these stages are continuously evaluated and the pressure-temperature response of the containment with or without the engineered safety features is calculated. The MARCH simulation also accounts for metal water reactions, combustion of hydrogen, and heat losses to structures in the containment. By comparison, the accident process analysis conducted in the RSS was conducted largely with hand calculations, which required several simplifying assumptions (e.g., small LOCAs and transients were treated in a gross manner by comparing them to calculations done for large LOCAs).

The updated version of the CORRAL code uses the same basic analytical models as the RSS version, but has been made more versatile. The code can now model the transport of the radionuclides within the containment in more detail because of the increased capability of handling larger problems.

For each of the dominant system accident sequences, the codes were used in determining possible containment failure modes, estimating the probabilities of each failure mode, and placing each sequence into the seven RSS PWR core melt release categories. The non-melt categories 8 and 9 were found to have a negligible impact on risk in the RSS and were not included in the RSSMAP. (For more details concerning the accident process analysis task see Chapter 5.)

Upon completion of the accident process analysis, the complete accident sequences (defined as the combined system accident sequence and containment failure mode) were ranked and the dominant accident sequences identified. The final step in the RSSMAP was then to compare the expected risk of the Oconee plant with the RSS PWR. This was done indirectly by comparing the probability (per reactor year) of the seven PWR core melt release categories, i.e., the RSSMAP methodology did not include a task to directly analyze the consequences of each release category.

3.0 GENERAL PLANT DESCRIPTION AND DIFFERENCES FROM RSS PLANT

The likelihood of certain accident sequences and the factors which cause an accident sequence to dominate the risk associated with a plant are clearly dependent on the plant design. In this section, significant design differences between the Oconee and Surry units are summarized. Detailed system descriptions and reliability estimates are presented in Appendix B.

The Oconee reactor units each have two steam generators and four steam generator loops designed by Babcock and Wilcox; the Surry units have three steam generators and three loops designed by Westinghouse. Each Oconee reactor unit power is 866 MWe; the Surry units each develop 775 MWe. Both containments are the dry type and are of approximately the same volume. The Oconee containment construction is a prestressed, post tensioned, reinforced concrete cylinder and dome with a steel liner. The design pressure is 59 psig. The Surry containment is of reinforced concrete design with a steel liner and has a design pressure of 45 psig. The Oconee containment volume is more open than Surry's (i.e., less internal structure).

It should be noted that the Oconee design analyzed in this report assumes an AC dependent Auxiliary Feedwater System (AFWS) and a High Head Auxiliary Service Water System (HHASWS). The HHASWS is an add-on system which is intended to be put in service in 1981. Also, design changes are being planned which will remove the AC dependencies from the AFWS.

There are several important differences in the safety systems between the plants which perform the LOCA and transient engineered safety functions (ESF). These differences are the result of different systems present at the Oconee plant as well as many differences in piping and circuitry configurations, system success criteria, and test and maintenance intervals for systems which appear at both plants. Some of the more obvious dissimilarities can be seen in Figures 3-1 and 3-2 which depict Oconee and Surry ESF's with related system components in a simplified manner.

A word of caution should be made about comparing the system failure probabilities of both plants. The comparison given in the following descriptive summaries is based on an independent comparison of the systems. Interdependencies among the various systems at the plant are not considered at this point. Because of this fact, a statement such as "Oconee System A has a failure probability five times greater than Surry System A," has no safety significance unless the systems being compared are truly independent of other systems at the plant. For purposes of comparing safety then, the appropriate place of comparison is the accident sequences since it is at this point where all system interdependencies are considered. Accident sequences and system interdependencies are discussed in Chapters 4 and 6.

It should be noted that for some physically identical systems at Surry and Oconee, there exists differences in the success criteria. These differences generally occur from the different ECCS requirements and different technical specifications at each plant.

3.1 Oconee ESF Systems Which Do Not Have Comparable Surry ESF Systems

There are two Oconee ESF systems having no comparable Surry ESF system. A brief description of the purpose and dominant failure modes of these systems follows:

3.1.1 Reactor Building Cooling System (RBCS)

The Oconee RBCS acts in conjunction with the Containment Spray Injection System (CSIS) to depressurize the containment following a LOCA. The system consists of three independent electric motor driven fans and cooling units. Successful operation requires one of three fan trains according to Battelle Columbus Laboratories. The dominant failure mode is a common mode failure caused by a miscalibration of the actuation system bistables.

3.1.2 High Head Auxiliary Service Water System (HHASWS)

The function of this system is similar to the auxiliary feedwater system (AFWS) in that it serves to remove residual heat from the steam generators following plant trip. The HHASWS consists of a single electric pump which is capable of delivering emergency feedwater to all six steam generators located in the three Oconee units (two steam generators per unit). The system has its own AC and DC power supply which is independent of the emergency hydropower system. The system is currently only intended to be utilized following a station blackout (i.e., complete loss of offsite and onsite AC power). In order to start the system, normally closed manual valves must be opened locally by an operator. Failure to open these valves was assessed to be the dominant failure mode of the system.

3.2 Oconee ESF Systems Which Have Comparable Surry ESF Systems

Brief descriptions of the differences between similar Surry and Oconee systems are given below.

3.2.1 Emergency AC Power System (EPS)

The EPS for Oconee is essentially the same as Surry below the 4160 ESF buses. The sources that supply the 4160 ESF buses are considerably different. Surry has three 2.75 MW diesel generators for two units with one being shared while Oconee can utilize either of two 87.5 MW hydro generators to supply emergency power. Oconee also has backup from one of two combustion turbine generators which are available for long term operation. Another major difference is that there is a direct connection between the diesel generators and ESF buses in Surry, whereas several circuit breakers and transformers make the connection in Oconee. Also, emergency loads at Oconee are applied to the hydro generators in sequence to minimize the impact of motor starting currents. At Surry emergency loads are applied simultaneously, which increases the trip probability of the diesel generators. This common mode is more probable at Surry than at Oconee. The unavailability of the Oconee EPS was estimated based on actual plant test data and expected hydro maintenance outages. Comparing this unavailability with Surry yields more than an order of magnitude decrease in the Oconee EPS unavailability.

3.2.2 DC Power System (DCPS)

The DCPS at both plants include a 125-volt DC power subsystem for instrumentation, on-site switching, and executive protection and control as well as separate 125-volt DC power subsystem for emergency on-site power generation control. The Oconee plant also includes an additional separate safety related 125-volt DC power subsystem for high voltage power switching between the alternate off-site network supply sources and the emergency on-site AC hydro power generation source. All of these 125-volt DC power subsystems are similarly powered by batteries and battery chargers.

Oconee's design does not require load shedding for the 125-volt instrumentation and control subsystem; Surry's design requires load shedding of the main turbine generator bearing and seal oil pumps after the turbine has coasted to a stop. If a loss of all AC power should occur, the Oconee instrumentation and control subsystem is designed to supply emergency loads for one hour while Surry's system is designed for two.

Based on the technique used for estimating DC system unavailability in the RSS, the Oconee and Surry DCPS have a similar unavailability estimate. However, a recent Sandia DC power system study (reference 3) identified a DC common mode failure not previously identified in the RSS. This failure is attributed to the miscalibration of the battery charger charging rate which causes the batteries to degrade and fail upon demand following a loss of offsite power. This common mode was assessed to be applicable to the Oconee 125V DC subsystem which controls the emergency AC power system. The unavailability estimate for this subsystem is two orders of magnitude higher than would have been estimated using the RSS method.

3.2.3 Reactor Protection System (RPS)

The RPS for both Surry and Oconee are actuated by interrupting power to the control rod assemblies (CRA) but the method for doing so is significantly different. The Surry RPS accomplishes reactor trip by deenergizing combinations of 1 out of 2 primary circuit breakers via the logic channel. The Oconee RPS accomplishes the trip by deenergizing combinations of two primary and two secondary circuit breakers and two groups of contactors.

Based on the technique used in estimating RPS unavailability in the RSS and research made available during the course of the RSSMAP, the two systems have a similar unavailability estimate.

3.2.4 Containment Leakage (CL)

Certain differences exist between the Oconee and Surry containment isolation designs. The Oconee design isolates the reactor building by closing various penetrations upon receipt of a high containment pressure signal. The Surry plant does not have a particular system for containment isolation, but isolation design is achieved by applying common criteria to penetrations in all interfacing fluid systems and by using ESF signals to activate appropriate valves. The Oconee design also includes the penetration room ventilation system (not present in Surry) which routes any leakage from several of the penetrations through HEPA filters before being discharged to the environment. The most significant design difference between the Oconee and Surry units is that the Oconee containment is at atmospheric pressure while the Surry contaiment is a subatmospheric design. The CL probability for Oconee has been assessed at approximately an order of magnitude higher than for Surry, primarily due to the latter design difference.

3.2.5 Core Flooding System (CFS)

The Oconee CFS and Surry cold leg injection accumulator system (CLAS) perform the same function, but there are some major design differences. The Surry design employs three identical trains for delivery into the cold legs of the RCS and Oconee has two identical trains which deliver directly to the reactor vessel. If a LOCA occurs in the cold leg, then the Surry system is impaired and must dump both of its remaining accumulators to successfully reflood the core. The Surry system in this case would have the same success criteria as Oconee, which must also deliver both of its accumulators.

At Oconee the CFS is required for only the largest LOCA, whereas the stated LOCA success criteria for Surry requires the accumulators for the large and intermediate size LOCA. If an isolation valve in the Surry system is inadvertently left closed, it will be opened automatically by the safety injection signal. In Oconee this provision does not exist; instead, valve position is monitored and alarmed.

An additional important difference is the technical specification requirement for CFS availability. At Surry, one core flood tank is allowed to be out of service for 4 hours before the reactor is to be shut down. At Oconee both core flood tanks must always be available. This difference adds a significant test and maintenance contribution to the Surry CLAS unavailability which does not exist at Oconee and results in a somewhat higher system unavailability for Surry.

3.2.6 Low Pressure Injection System (LPIS)

Both Oconee and Surry employ dual, redundant trains to deliver borated water to the RCS following a LOCA. The Surry system delivers water to the RCS cold legs while the Oconee LPIS delivers water directly to the reactor vessel. The pump trains at both plants share a common suction header which has one or more valves in it. The discharge header at Surry is also common to both trains and contains a valve. The Oconee discharge headers are separate. The Surry LPIS therefore has more single failures than Oconee's LPIS. This latter point causes the unavailability for the Surry system to be slightly higher than Oconee's.

3.2.7 Low Pressure Recirculation System (LPRS)

The Oconee and Surry LPRS are similar in that they employ dual redundant trains to deliver water to the RCS from the sump following a LOCA. One difference is that the Oconee LPRS includes containment heat removal heat exchangers in each pump train while Surry's heat exchangers are part of the containment spray recirculation system. Both systems use the same pumps as in their LPIS and both require operator action to realign the pump suction from the BWST or RWST to the containment sump at the start of the recirculation phase. The Surry system also requires operator action after 24 hours to realign LPRS flow from RCS cold legs to the hot legs. This later realignment does not apply to the Oconee system. Failure to perform any of the above realignments constitutes a common mode failure of the system due to human error. The Surry LPRS therefore has a higher contribution to system unavailability due to common mode failure than does the Oconee LPRS. Due to this and other contributors, the Surry LPRS has an estimated factor of three greater unavailability than the Oconee LPRS.

3.2.8 High Pressure Injection System (HPIS)

The Oconee HPIS is similar to the Surry HPIS in that each have three high pressure pumps which take suction from a 350000 gallon borated water supply. Both systems have a single header which connects this borated water supply to the high pressure pumps. The three high pressure pumps discharge paths are interconnected in Surry, whereas at Oconee, one pump train is isolated from the others by two normally closed manual valves and used as a backup for either train.

A major difference between the two systems is that the Surry system has a boron injection tank (BIT) and a borated water supply, whereas Oconee has only the borated water supply. Addition of the BIT includes additional failure modes not found at Oconee.

Another major difference is the type of pumps used. The Oconee HPIS pumps deliver adequate flow at elevated RCS operating pressures to cool the core if heat removal via the steam generators fails. The Surry pumps, however, do not deliver adequate flow at elevated RCS pressures to cool the core. This makes the requirement for heat removal via the steam generators more critical at the Surry reactor.

In response to a LOCA, the unavailability of the Surry HPIS is a factor of six higher than the Oconee HPIS due to more single failures in the pump suction header and the BIT failure modes.

3.2.9 High Pressure Recirculation System (HPRS)

The HPRS at both Oconee and Surry are similar in that each has three high pressure pumps which take their suction from two independent flow paths at the discharge of the LPRS pumps. Both systems require the successful operation of their respective LPRS and require operator action to valve in the HPRS pump suction to the LPRS pump discharge. Failure of the LPRS or of the appropriate operator action are the main contributors to HPRS unavailability at both plants.

At the Surry plant, HPRS flow must be realigned from the cold legs to the hot legs within 24 hours. The failure to realign flow is an additional important contributor to the Surry system availability which does not apply to the Oconee HPRS. The unavailability, however, of the Oconee system was estimated to be similar to the Surry HPRS.

3.2.10 Engineered Safeguards Protective System (ESPS)

The Oconee ESPS and the equivalent Surry consequence limiting control system (CLCS) and safety injection control system (SICS) employ comparable degrees of redundancy in processing sensor data and initiating engineered safeguards actuation when required. Both designs actuate similar types of systems and utilize dual logic trains which derive their signals from a sensor group common to both trains. At both plants, the HPIS and LPIS, in addition to their normal trip signals, receive backup signals from a high reactor building pressure trip. There are several differences between the systems, however.

One difference between the two designs is that the Oconee design monitors RCS pressure only, whereas the Surry SICS monitors RCS pressurizer pressure and level. Another difference is that the Oconee ESPS employs 3 pressure sensors for generating a HI reactor building pressure signal and 6 pressure switches, arranged in 2 groups of 3 switches, for generating a HI-HI signal. The Surry CLCS employs 4 pressure sensors for generating both the HI and HI-HI signals. The Oconee design employs 2-out-of-3 trip logic while the Surry design employs 3-out-of-4 trip logic. The Surry CLCS provides for automatically initiating, through delay circuits, the CSRS with manual initiating as backup. The Oconee CSRS is initiated when the operator manually realigns the LPIS for the recirculation mode.

Based on a qualitative comparison between the two designs, it was concluded that the unavailability of the Oconee ESPS is similar to that estimated for the Surry SICS and CLCS.

3.2.11 Containment Spray Injection System (CSIS)

Both systems are similar in that each has redundant CSIS trains to deliver water to the containment spray nozzles. They are also susceptable to similar common mode failures. Common mode failure of either system may be caused by mispositioning of valves after a pump test and miscalibration of the sensor group which actuates the system. There are, however, some differences.

At Surry each train has an independent header connecting the water tank and the pump suction. At Oconee, however, each train shares a common header. Because of this, the Oconee CSIS has an additional single failure that is not applicable to Surry. However, the CSIS unavailabilities for Surry and Oconee were found to be similar.

3.2.12 Containment Spray Recirculation System (CSRS)

The CSRS systems for Oconee and Surry are considerably different in both design and mode of operation. One important difference is that the Surry CSRS is independent of its CSIS, whereas the Oconee CSRS uses much the same equipment as its CSIS. The success criteria for Surry is two of four pumps. The success criteria for Oconee is one of two pumps.

The Surry CSRS is automatically activated, whereas Oconee is manually activated when the operator realigns the pump suction from the BWST to the containment sump. The Oconee system also requires the operator to throttle the pump flow rate to provide an adequate net positive suction head so that pump cavitation failure will not occur. If these operator actions are not performed, common mode failure of the Oconee CSRS will result. These important common mode failure mechanisms do not apply to the Surry system and account for more than an order of magnitude greater unavailability for the Oconee CSRS.

3.2.13 Power Conversion System (PCS)

One of the main functions of the PCS at both Oconee and Surry is to provide feedwater to the steam generators during normal operation. Following a reactor trip both systems are also capable of delivering feedwater at a lesser rate to provide the function of decay heat removal.

One method of successful decay heat removal at Oconee can be accomplished by delivering steam generator feedwater with one of two high pressure steam driven feedwater pumps. If these pumps are lost, an alternate method requires the steam generator pressure to be reduced by the operator and feedwater delivery provided by a combination of one of three low pressure electrically driven hotwell pumps and one of three low pressure electrically driven condensate booster pumps. In both modes of operation the heat sink is either the condenser or the secondary steam system safety valves. At Surry successful PCS decay heat removal can be accomplished by one of three low pressure electrically driven condensate pumps delivering to one of two high pressure electrically driven feedwater pumps. The heat sink at Surry is also the condenser or secondary safety valves.

The power conversion systems are expected to have similar failure probabilities in response to reactor shutdowns not associated with loss of feedwater. For these transients success requires the continued operation of the feedwater system. However, in response to a loss of feedwater transient caused by a hardware problem or a loss of offsite power (LOP), successful feedwater operation requires the recovery of the system.

PCS recovery following a LOP requires that offsite power be restored and several operator actions be performed. Discussions with Oconee plant personnel indicate that it is reasonable to assume that the PCS would not be restored in most cases following a LOP within the short term (approximately 30 minutes). The probability of not recovering the PCS following a LOP was therefore assumed to be 1.0.

PCS recovery following a hardware problem requires assessment and correction of the problem. Discussions with plant personnel and examination of recent plant data suggests that at least 90% of all feedwater problems at Oconee were corrected within 30 minutes or did not involve total loss of the PCS. The Oconee data examined reflects situations where there were problems with the PCS and the Emergency Feedwater System (EFWS) was available. The true situation, as modeled into the sequences, is one where there is a total loss of feedwater. In such a case, discussions with plant personnel indicate that primary emphasis would be placed on restoring the EFWS but that a somewhat parallel effort to restore the PCS would also be conducted. PCS nonrecovery after a hardware failure was roughly estimated to be 10^{-1} for Oconee based on a 90% recovery rate.

(The RSS assumed a PCS nonrecovery probability following a LOP of .2. This value corresponds to the expected nonrecovery probability of offsite power. A value of 10^{-2} was used for PCS nonrecovery following a hardware problem at Surry (compared to the 10^{-1} value described above) and was derived from industry data. It is suspected that the 10^{-2} nonrecovery probability is based on data for cases where the emergency feedwater system is successfully operating. The true situation is one where all feedwater is lost. For this reason, and due to the fact that plant specific data existed, a different PCS nonrecovery probability was used for Oconee.

3.2.14 Emergency Feedwater System (EFWS)

The Oconee EFWS and Surry AFWS are similar in that each system consists of two electric and one turbine driven pump train. Though many piping differences exist between systems, successful system operation requires the flow equivalent of one pump to one steam generator at both plants.

Given a loss of offsite power the Oconee system requires operator action to engage important EFWS components to the emergency power buses. If this is not accomplished, system flow control and operation of the turbine driven pump will be lost (due to loss of pump cooling) in a short time. Similar operator actions were not identified for the Surry AFWS.

Given a loss of all AC power (both normal and emergency) the Oconee EFWS will fail in a short time due to loss of turbine pump cooling. The Surry turbine pump was not identified to have this cooling dependency and could therefore operate given a loss of all AC power.

The HHASWS at Oconee has no comparable Surry system. This system can provide backup to any EFWS demand and is especially important following a total loss of all AC power. Since the HHASWS has its own power system, this system is not affected and can successfully provide post shutdown cooling.

3.2.15 Low Pressure Service Water System (LPSWS)

The CHRS system at Surry and the LPSWS at Oconee both rely on river water to cool the containment sump recirculating water and other portions of the operating plant. Major differences appear in the means by which this water is routed to the CHRS/LPSWS and the interface of the heat exchangers with the ESF systems. At Surry, service water is pumped from the James River into the 25-million-gallon intake channel. This water gravity feeds the four heat exchangers in the CSRS, then on to the discharge channel back into the river. At Oconee, water is obtained from the Little River arm at Lake Keowee and is delivered via a siphon effect created and maintained by the LPSWS vacuum pumps to the reactor building cooling system (RBCS) heat exchangers and the LPIS coolers. Other pumps are employed to overcome friction losses. Upon loss of offsite power, the siphon effect is maintained by steam ejectors. The unavailability of the Oconee LPSWS was assessed to be similar to the Surry CHRS.

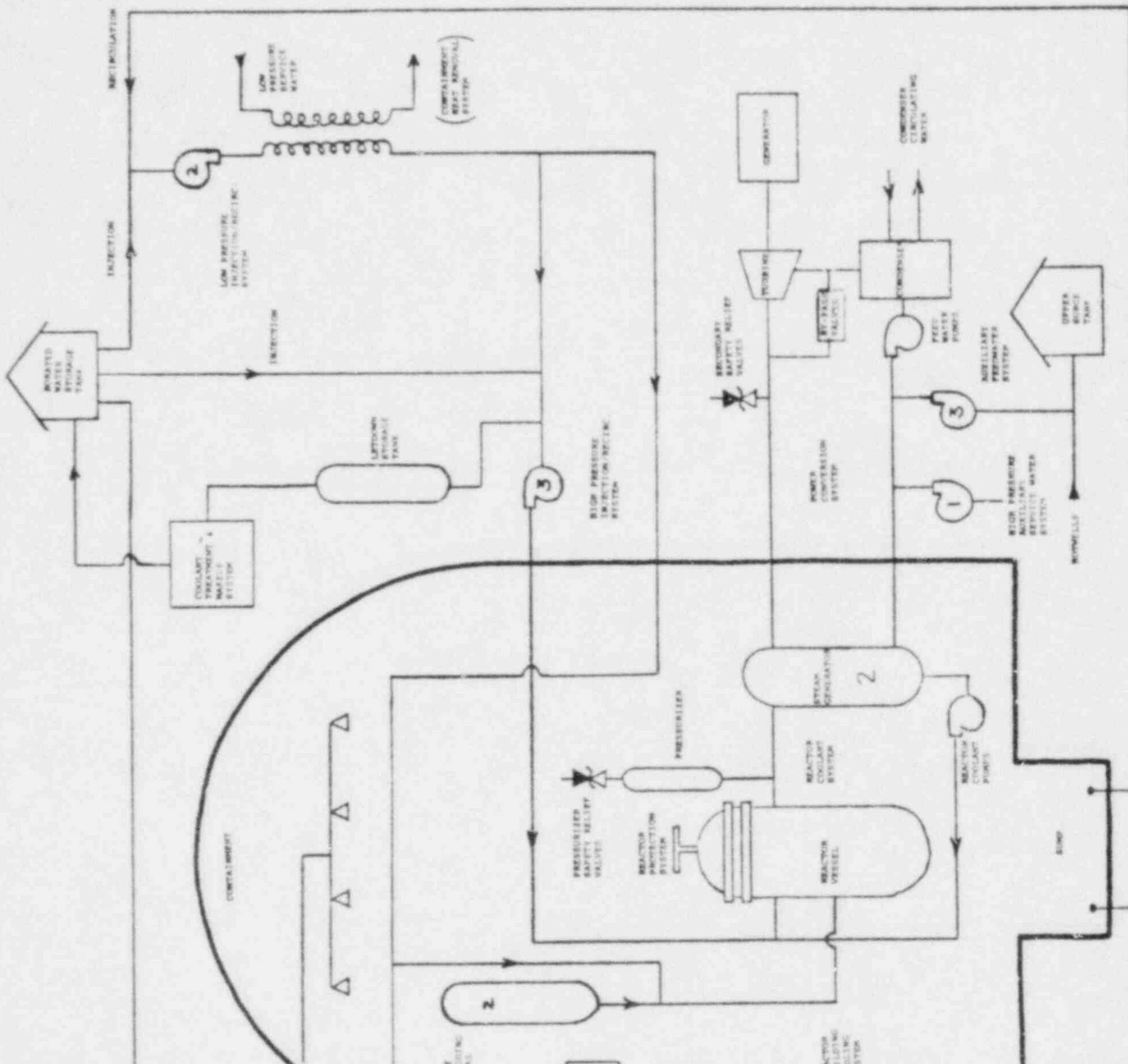


Figure 3-1 Simplified Oconee ESF Diagram

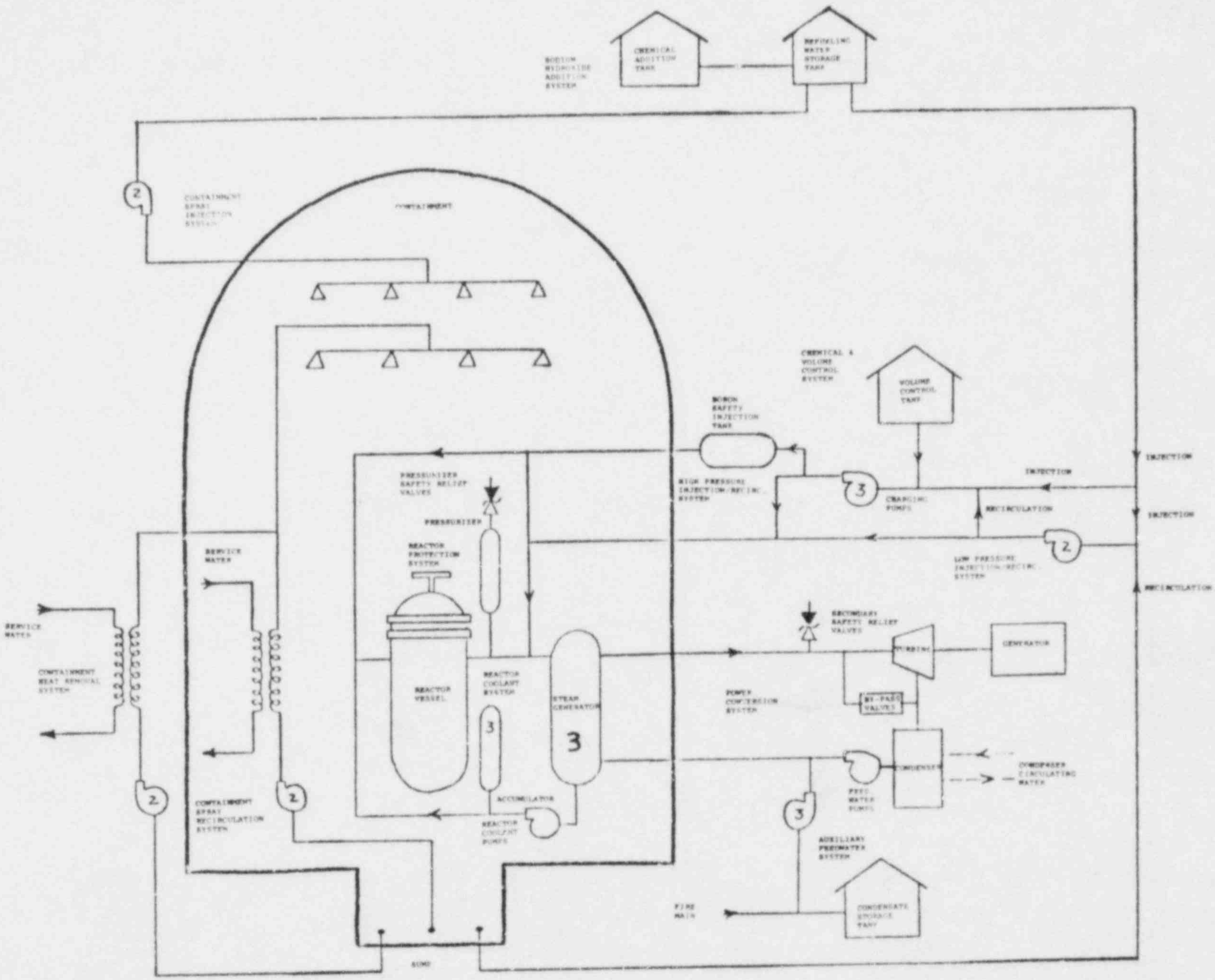


Figure 3-2 Simplified Surry ESF Diagram

4.0 SYSTEMS ANALYSIS TASK

This chapter summarizes the work done as part of the RSSMAP Oconee #3 systems analysis task. The work was done by Sandia National Laboratories with the aid of Evaluation Associates Inc. The objective of this task was to identify the dominant system accident sequences which are the major contributors to risk for the Oconee plant. These sequences were identified through the use of event tree and safety system availability models. The system availability models are, in essence, a Boolean equation representation of a simplified fault tree. The event tree and system availability models utilized are discussed in Sections 4.1 and 4.2, respectively. The dominant system accident sequences, generated through the use of these models, are presented in Section 4.3 along with an illustrative example showing how a typical accident sequence calculation was performed.

4.1 Event Trees

Event trees are the structures from which accident sequences are derived. Two event tree types, used in succession, produce the complete accident sequences. The System Event Trees, the subject of this section, interrelate the initiating event and the engineered safety feature failure events and result in system accident sequences such as "ACD." The Containment Event Trees, done as part of the accident process analysis, relate the possible responses of the containment to the physical situations associated with each system accident sequence. The resulting containment failure modes, designated by terms such as α, β, δ are added to the system accident sequences to form the complete accident sequences such as "ACD-δ." Details of the Containment Event Trees can be found in Chapter 5.

4.1.1 Initiating Events

The type of initiating events considered were the same as in the RSS, i.e., LOCAs and transients. The RSS considered three LOCA size ranges. These were designated "S_2" ($1/2" < D \leq 2"$), "S_1" ($2" < D \leq 6"$), and "A" ($D > 6"$). Three sizes were chosen since the number of ECCS and other systems required to mitigate a LOCA was different for each LOCA range. The RSS also considered three types of transients. These were all designated "T" and included reactor shutdowns initiated by

1) a loss of offsite power,

2) a loss of the main feedwater system caused by other than a loss of offsite power, and

3) other causes in which the main feedwater system is initially available.

These transient initiators were assessed to adequately represent a spectrum of generic PWR transients (RSS, Table I 4-9) in terms of their effects on the mitigating systems.

Based on the study of the Oconee FSAR it was determined that four LOCA sizes should be chosen based on different ECCS subsystem requirements (See the Oconee FSAR page 14-57). These are designated "S_3" (D $\leq$ 4"), "S_2" (4" < D $\leq$ 10"), "S_1" (10" < D $\leq$ 13.5), and A (D>13.5"). The estimated frequency of these LOCAs is given in Table 4-1. Since the RSS pipe rupture data is for a generic plant, it was utilized in arriving at these estimates. (As noted from this table some double counting of RSS LOCA sizes was required due to overlap of LOCA size ranges between the RSS and Oconee.)

The same three transients used in the RSS and their estimated frequency were also used to represent transients at Oconee. The loss of offsite power transient is designated T_1 and has a frequency of 0.2/year. The loss of main feedwater transient is designated T_2 and has a frequency of 3/year. Other transients with main feedwater initially available are designated T_3 and have a frequency of 4/year.

4.1.2 LOCA Event Tree

The Oconee LOCA event tree is presented in Figure 4-1. A detailed discussion of this event tree is presented in Appendix A1. This section will highlight the discussion given there.

A single LOCA event tree was judged to be an adequate representation for the entire spectrum of break sizes. Except for the removal of the reactor protection system event K for A and S_1 LOCA initiators, the rest of the tree headings and structure are identical for all size breaks.

The systems depicted on the tree perform seven plant functions. The combinations of plant systems which are required to successfully perform these functions for a variety of LOCA sizes are displayed in Table 4-2. These functions were chosen since they are either required to successfully mitigate a LOCA or they can affect the consequences of a core melt if mitigation of the LOCA is unsuccessful. The definitions of success for the event tree headings are given in Table 4-3.

Dependencies incorporated into the LOCA event tree structure are the following:

1) If containment spray injection fails (event C) then containment spray recirculation fails (event F), since the systems share most of the same equipment.

2) If the reactor building cooling system fails during the time interval corresponding to the ECCS injection phase (event Y), then it fails during the recirculation phase (event Z) since the equipment and the success criteria are exactly the same during both phases.

3) If the emergency coolant injection system fails (event D), then emergency coolant recirculation (event H) is superfluous, since failure to provide sufficient injection cooling will result in a core melt regardless of what happens during the recirculation phase. This is consistent with the RSS treatment.

4) Containment overpressure protection during recirculation (COR) can succeed by either of two methods: Operation of one reactor building cooling system (RBCS) fan train or operation of one containment spray system train in conjunction with the LPRS heat exchanger. Operation of the LPRS heat exchanger is represented by event G. Therefore, if the RBCS succeeds during the recirculation phase (event $\bar{Z}$), no success/failure choice is given for event G, since COR has succeeded. Also, for sequences where either the containment spray system (events C or F) or emergency core cooling systems (events D or H) fail, no success/failure choice is given for event G.

It can be noted on the LOCA tree that no event tree structure was developed following failure of the reactor protection system, event K. This was done for purposes of simplification since the event tree structure following failure of event K would be identical to the structure following the success of event K.

4.1.3 Transient Event Tree

The Oconee transient event tree is presented in Figure 4-2. A detailed discussion of this event tree is presented in Appendix A2. This section will highlight the discussion given there.

A single transient event tree was judged to be an adequate model of the plant response following the three transient initiating events considered.

The systems depicted on the tree perform six plant functions. The combination of plant systems which are required to perform these functions for all three transients is shown in Table 4-4. These functions were chosen since they are either required to successfully mitigate a transient or they can affect the consequences of a core melt if mitigation of the transient is unsuccessful. The definitions of success for the event tree headings are given in Table 4-5.

Transient sequences with failure of event Q can be treated as a small-small LOCA since the systems responding to these LOCAs are identical to those required for an S_3 LOCA. These "transient induced LOCAs" are therefore transferred to the LOCA event tree upon failure of event Q.

Dependencies incorporated into the transient event tree structure are the following:

1) If the power conversion system remains in uninterrupted operation ($\overline{M}$) then the operation of the emergency feedwater system or high pressure injection system are not required since these systems perform the same function (only one of these systems is required for any given sequence). Exceptions are sequences with failure of the reactor protection system and power conversion system which require the operation of the emergency feedwater <u>and</u> high pressure injection systems.

2) If the reactor protection system and power conversion systems succeed, then the RCS relief valves are not demanded since the RCS pressure would not reach the relief valve setpoint.

3) For those sequences in which the reactor protection system or emergency feedwater systems fail, the RCS relief valves will definitely be demanded.

4) For those sequences involving failures of the reactor protection system, power conversion system, and emergency feedwater system, the RCS relief valves will stay open through core meltdown.

5) If the RCS relief valves fail to open, the valves cannot, logically, fail to reclose. Also, the operation of the high pressure injection system does not matter since core melt is assumed. This conservative assumption is justified because the very small probability of event P_2 (failure of S/RVs to open when demanded) is expected to cause all accident sequences containing that event to be relatively small contributors to risk. (Exception: Core melt is not assumed if event P_2 occurs in the sequence where the reactor protection system and emergency feedwater systems succeed, the power conversion system fails and the RCS relief valves are required (events $\overline{K}$ M $\overline{L}$ $\overline{P}_1$) because the excess RCS pressure is not expected to be very great).

6) If the RCS relief valves fail to reclose the sequence results in a LOCA, and the sequence (and analysis) is continued in a LOCA event tree. This is justified by the fact that the rate of leakage of RCS inventory is sufficient to fit the definition of a LOCA.

7) The operation of the reactor building cooling system and containment spray systems are considered only in those sequences which result in core melt since these systems perform functions which reduce the consequences of core melt accidents, and they would not serve any purpose in other transient situations. (Exception: Containment Pressure Reduction (event O) is considered in sequences 6 and 7. For these sequences, which require a "bleed and feed" operation, core melt is prevented by removing decay heat through the S/RVs and replacing the coolant with the high pressure injection system. However, this will cause a buildup of steam in the containment, which will necessitate containment pressure reduction to prevent a containment over-pressure failure and subsequent core melt).

An explanation is in order concerning the "note 1" on the transient tree. If too much cooling is provided to the secondary side of the steam generators by the power conversion system or emergency feedwater systems, a rapid RCS cooldown transient would ensue. Following RCS depressurization, due to the shrink of the RCS coolant, the high pressure injection system (HPIS) would be demanded. Operation of the HPIS would overfill the RCS and cause water to be ejected through the RCS relief valves. If these valves do not reclose, a LOCA would ensue, which would require operation of the LOCA systems discussed in the previous section.

4.1.4 Interfacing Systems LOCA Event Tree

The Oconee interfacing system LOCA event tree is presented in Figure 4-3. A detailed discussion of the Oconee interfacing system LOCA is presented in Appendix A3. This section will highlight the discussion given there.

The event tree shown in Figure 4-3 is identical to the Surry (RSS) LPIS check valve rupture event tree. The initiating event of the tree, event V, assumes failure of a series of two check valves in one of the low pressure injection system lines and the opening of the normally closed isolation motor operated valve (MOV), which is also in series with the check valves, for quarterly MOV testing. This would allow high pressure coolant water to enter the low pressure piping outside containment and pipe rupture to occur. The containment engineered safety features would be relatively ineffective for this accident, and the low pressure injection system would also fail due to the LOCA. As a result, core melt would occur. Since the containment engineered safety features are relatively ineffective, the variations in consequences are so small among the sequences, which all include the initiating event, only the initiating event V was evaluated as an accident sequence.

The frequency of occurrence for this accident is considerably higher for the Oconee design (7.2×10^{-5} vs. 4×10^{-6}/R-yr) than for Surry due primarily to the presence of the normally closed MOV.[1] Because of this, the failure mode caused by both check valves failing to reseat after a cold shutdown low pressure injection system flow test is included in the probability assessment. This failure mode was not applicable to the RSS PWR since the comparable MOV was in the normally open position allowing such a failure to be detected by the operator during plant startup before an unsafe condition could develop.

4.1.5 Comparison of Oconee & Surry Event Trees

The Surry LOCA and Transient event trees are displayed in Figures 4-4 through 4-7. A detailed discussion of the event tree differences are presented in Appendices A1 and A2. Some of the more important differences are listed below.

LOCA

1) Response to a LOCA was depicted by one event tree at Oconee and three event trees at Surry.
2) Due to plant design differences, events Y and Z appear only on the Oconee tree and events I and L appear only on the Surry trees.

---

[1]Duke Power has recently introduced changes which significantly reduce the frequency of this sequence (i.e., less than or equal to the frequency of the RSS event V).

3) For purposes of simplification, the Oconee equivalent to the Surry events B and E were removed from Oconee LOCA tree.

4) The event tree structure differs somewhat between the plants due to some different interdependencies between the systems represented on the tree.

Transient

1) The Oconee transient event tree explicitly includes systems related to containment response (events O and O'). The Surry transient tree did not include these systems. Success/failure of these systems were implied, however, in the Surry accident sequence results.

2) For purposes of simplification, the Oconee equivalent to the Surry events U and W were removed from the Oconee transient event tree. These events/systems were required to bring the Surry plant from hot to cold shutdown and were included in the Surry analysis for completeness.

3) The Oconee event U represents the "feed and bleed" core cooling mode of the high pressure injection system. The Surry event U represents the operation of the chemical and volume control system to bring

the plant from hot to cold shutdown. The RSS assessed that a "feed and bleed" core cooling method could not be achieved at Surry.

4) The Surry transient event tree treated transient induced LOCA sequences directly on the transient event tree and assumed they were core melts. On the Oconee tree, these sequences are transferred to the LOCA tree and treated in a similar manner as other LOCAs.

5) The event tree structure differs somewhat between the plants due to some different interdependencies between the systems represented on the tree.

6) The P_1 event, which represents a probabilistic demand of the RCS relief valves, appears only on the Oconee transient tree. The Surry event tree assumed that the relief valves either were or were not demanded with 100% certainty.

4.2 Safety System Reliability Models

Each system represented on the event trees, except for those where plant and/or industry data existed, was reviewed and analyzed in order to determine system failure modes. An insight gained from the RSS was that system unavailabilities are usually dominated by single, double and common mode hardware and human failures. Because of this insight, elaborate fault tree models to identify all possible system failure modes were not used. Instead, a "survey and analysis" technique was used to determine system failure modes. This technique is in essence a systematic approach by which an analyst searches for system failure modes.

The first step in conducting a typical survey and analysis was to review all available information pertaining to the Oconee system. Sources of information available for this study were the FSAR system description and drawings, the technical specifications and discussions with plant personnel.

The next step was to review a similar system analyzed in the RSS. The purpose of this review was to gain insight concerning typical types of important system failure modes (e.g., singles, doubles, human error, test, maintenance, and common mode faults). Based on the Oconee system information and RSS insight, the analyst manually conducted a failure mode search. Identification of single and common mode failures were made first followed by doubles, test, and maintenance. Any interactions that the system being analyzed had with other systems on the event tree, such as a shared component or actuation system, were noted.

The failure modes were then quantified using the RSS hardware and human error data base. In some instances, due to a lack of detailed subsystem information, subsystem unavailabilities were taken directly from the similar system analyzed in the RSS. This was done primarily in obtaining estimates of control circuit unavailabilities for pumps and valves.

During the course of the analysis it was generally found that most systems which appear on the event trees share a number of components and support systems. Because of this fact, it was necessary to construct a Boolean equation describing the system failure modes so that these interdependencies could be properly treated during the accident sequence calculations. Some systems, however, were assessed to be independent or nearly independent of all other event tree systems. A Boolean equation describing failure modes for independent systems was not necessary since the system unavailability could be simply multiplied into the accident sequence calculation.

A "survey and analysis" for each of 15 Oconee safety systems can be found in Appendices B1 through B15. Most of these systems appear as events on the event trees. Some of these are support systems (e.g., emergency AC and DC power system, engineered safeguards protective system) which are common to several event tree systems. Each appendix includes a derivation of the Boolean equation(s) describing system failure and an unavailability estimate assuming independence from all other Oconee systems. In many instances more than one Boolean equation was derived for a particular system because some system failure modes were different depending on the initiating event.

Tables 4-6 and 4-7 can be used as a key to the contents of Appendix B. Across the top of each table is a list of the systems which appear on the LOCA and transient event trees, respectively. Listed in the first column are the event tree initiating events studied. The four LOCA's A, S_1, S_2, S_3 and three transients, T_1, T_2, T_3, have been discussed previously. The LOCA initiators, T_xQ, are transient induced LOCA's. The transient initiator $T_1(B_3)$ represents a loss of all AC power. (T_1 is a loss of offsite power and (B_3) is a failure of the emergency power system. See Appendix B1 for more details). The entries in the tables are either an unavailability estimate, the letter "X", an equation number, or blank. The numerical entries in the Table are unavailability estimates for the system under consideration. The systems which have unavailabilities listed were considered to be independent of all other event tree systems. The columns in the table also have alphabetic entries. The letter "X" denotes that a single Boolean equation describes system failure for all initiators, i.e., the system failure is independent with respect to the initiator. The equation numbers reference specific Boolean equations in the appendices which were used in the calculation of a particular sequence. The letters "a" and "b" in parenthesis after some of the equation references indicate which form of the equation was used. Different initiators sometime require different equation forms, and are described in the appendices. A blank entry means that the system is not used in response to the initiator. For example, HPIS failure is modeled by HPIS Boolean equation B8-1, form "a", for all LOCAs except $T_1(B_3)$. For $T_1(B_3)Q$ LOCAs, the unavailability is assessed to be unity. HPIS failure is modeled by equation B8-1, form "b", for all transients except $T_1(B_3)$. For $T_1(B_3)$ transients, HPIS failure is modeled by equation B8-1. These three HPIS equations can be identified in Appendix B8.

4.3 Accident Sequence Analysis

The final step of the Oconee systems analysis task was the performance of a system accident sequence analysis to determine those core melt sequences with the highest frequency. This was done by combining the Boolean equations describing the succeeded and failed systems for each accident sequence, performing a Boolean reduction to produce sequence cut sets (i.e., the minimum combination of system failures which produce an accident sequence), and quantifying these cut sets using the data base. The cut sets for each accident sequence were summed to arrive at a total sequence frequency. The accident sequence Boolean reduction and cut set quantification was performed by the SETS and SEP computer codes respectively. System accident sequences with a frequency $>10^{-8}$/R-yr were identified. These sequences were then given to Battelle Columbus Laboratories and were analyzed in terms of accident processes (see Chapter 5).

An example which illustrates the procedure utilized in performing the system accident sequence analysis follows in Section 4.3.1. Those sequences with a frequency $>10^{-8}$/R-yr are presented in Section 4.3.2.

4.3.1 Generating and Quantifying Accident Sequence Cut Sets - An Example

The sequence chosen to illustrate the procedure is the transient induced LOCA T_2MLQ-FH. It is a transient initiated by a loss of main feedwater (T_2M) followed by failure to restore the main feedwater system and failure of the emergency feedwater system (L), a failure of the RCS relief valves to reclose (Q) and failure of the containment spray recirculation and emergency coolant recirculation systems (F and H respectively). It is a combination of transient sequence 12 and LOCA sequence 7. The dash in the accident sequence T_2MLQ-FH indicates a transient induced LOCA. The events to the left of the dash (T_2MLQ) are events from the transient event tree. Those on the right (FH) are the sequence events that continue on the LOCA event tree.

The sequence label T_2MLQ-FH is a convenient identifier since it represents all the systems which failed in the sequence. This convenient identifier, however, should not be confused with the Boolean representation of the same sequence. Besides the systems which failed in this sequence, several systems succeeded. These are the reactor protection system ($\overline{K}$), opening of the RCS relief valves ($\overline{P}_2$), the containment spray injection system ($\overline{C}$), the reactor building cooling system ($\overline{Y}$ and $\overline{Z}$), and the emergency coolant injection system ($\overline{D}$). The Boolean representation of the sequence depicts both the succeeded and failed systems and would be $T_2\ \overline{K}\ M\ L\ \overline{P}_2\ Q$ - $\overline{C}\ \overline{Y}\ \overline{D}\ F\ \overline{Z}\ H$. Quantification of this accident sequence requires the use of the Boolean sequence representation.

A number of the systems/events in the sequence are independent from all other systems/events. These are $\overline{K}$, T_2M, $\overline{P}_2$, and Q. Since they are independent their unavailabilities/ availabilities can be simply multiplied together. The unavailabilities/availabilities of these systems can be determined from Table 4-7 as:

$$P(T_2M) = 3$$

$$P(\overline{K}) = 1 - (2.6 \times 10^{-5}) \approx 1$$

$$P(\overline{P}_2) = 1 - (2 \times 10^{-5}) \approx 1$$

$$P(Q) = 5 \times 10^{-2}$$

Multiplying these together yields 0.15.

The rest of the system/events in the sequence are dependent due to sharing of various components and subsystems. In order to properly treat these dependencies in the accident sequence calculation a Boolean equation must be written for each of the remaining system/events. These Boolean equations were derived in Appendix B and Tables 4-6 and 4-7 can be used as a key to determine the necessary equations to perform the sequence calculation. These equations are:

1) <u>EFWS/PCS Non Recovery Equation B13-1</u>

$$L = [CONST1 + LPSW] \cdot PCSNR$$

2) <u>CSIS Equation B11-1(b)</u>

$$\overline{C} = \overline{A + RBHIHICM + CSISCM + (F + C + CH7) \cdot (G + B + CH8)}$$

3) <u>RBCS Equation B15-1(a)</u>

$$\overline{Y} = \overline{(H1 + CH5) \cdot (J1 + CH5 \cdot CH6) \cdot (K1 + CH6) + LPSW + RBHICM}$$

4) <u>HPIS Equation B8-1(a)</u>

$$\overline{D} = \overline{(A1 + CH1 + D1 \cdot E1 + C1) \cdot (B1 + CH2) + A + RCSRBCM + RCSLOCM \cdot RBHICM + LPSW}$$

5) <u>CSRS Equation B12-1</u>

$$F = (F + C + CH7 + F' + W) \cdot (G + B + CH8 + G' + X) + WXCM + CSRSCM$$

6) <u>HPRS Equation B9-1</u>

$$H = HPRSCM + LPRS + LPISCM$$

where

$$LPRS = (B + J + CH4 + E + E' + X) \cdot (C + K + CH3 + D + D' + W) + WXCM$$

No equation was derived for $\overline{Z}$ because it is assumed that $\overline{Y}$ implies $\overline{Z}$. The terms of these equations are defined in Appendix B. In general, each term represents a group of system components. These groups or modules were constructed in order to reduce the number of terms in the Boolean equations. This greatly simplifies the accident sequence calculation, i.e., reduces the computer time required to perform the Boolean reduction. A module was created when it was assessed that a group of components, such as a pump train or control circuit actuation train, were independent from all other plant components or modules.

The six Boolean equations are then "anded" together and Boolean reduced. This reduction was performed by the SETS computer code. Reduction involves the elimination of redundant terms by applying the Boolean identities $P \cdot \overline{P} = \emptyset$, $P + PQ = P$, and $P \cdot P = P$. Applying these identities eliminated a large number of the redundant terms. However, due to the addition of complement events in the Boolean equation, several redundant terms still remain. These redundant terms were eliminated by removing all complemented events from the remaining terms and reapplying the second Boolean identity given above. For example, after applying the Boolean identities the first time, two terms in the reduced Boolean equation may be of the form $AB\overline{C} + AB\overline{D}$. Since we are interested in the minimum number of component/module failures, or minimal cut sets, which cause an accident sequence to occur, the events $\overline{C}$ and $\overline{D}$, which represent component/module success, are not important in the final results. These two terms can be replaced with the term AB. Reducing the second time yielded terms which represent the sequence minimal cut sets.

After obtaining the sequence minimal cut sets, the next step was to quantify them. This was done by substituting the module point estimate unavailabilities found in Appendix B into the cut sets and performing the arithmetic. The arithmetic was performed by the SEP computer code. Those cut sets with the highest frequency were then identified. These cut sets are the dominant contributors to the sequence frequency. The total sequence frequency was calculated by summing all the sequence cut sets frequencies. A list of the dominant cut sets and estimates of the sequence frequency can be found in Table 4-8.

4.3.2 Identification of the Dominant System Accident Sequences

Using the procedure described in the previous section, each potential core melt event tree sequence was quantified. Those sequences with a frequency $\geq 10^{-8}$/R-yr are listed in Tables 4-9, 4-10, and 4-11. These sequences were given to Battelle Columbus Laboratories and analyzed in terms of accident processes. Work at Battelle resulted in assigning an appropriate containment failure mode probability for those sequences which were found to lead to core melt and the placement of the sequences in their proper PWR release category. (Battelle's work is described in detail in Chapter 5.)

Based on the estimated sequence frequency and release category placement, those accident sequences which are expected to dominate the risk at Oconee were identified. These sequences and the most important system failures which cause the sequence to occur (i.e., sequence cut sets) are discussed in detail in Chapter 6.

Table 4-1. RSS and Estimated Oconee LOCA Frequencies

RSS LOCA	RSS LOCA FREQUENCY	OCONEE LOCA	ESTIMATED LOCA FREQUENCY
$S_2(1/2" < D \leq 2")$	1×10^{-3}/yr	$S_3(\ D \leq 4")$	$S_{2_{RSS}} + S_{1_{RSS}} = 1 \times 10^{-3} + 3 \times 10^{-4} = 1.3 \times 10^{-3}$/yr
$S_1(2" < D \leq 6")$	3×10^{-4}/yr	$S_2(4" < D \leq 10")$	$S_{1_{RSS}} + A_{RSS} = 3 \times 10^{-4} + 1 \times 10^{-4} = 4 \times 10^{-4}$/yr
$A(\ D > 6")$	1×10^{-4}/yr	$S_1(10" < D \leq 13.5")$	$A_{RSS} = 1 \times 10^{-4} = 1 \times 10^{-4}$/yr
		$A(\ D > 13.5")$	$A_{RSS} = 1 \times 10^{-4} = 1 \times 10^{-4}$/yr

Table 4-2. Alternate Equipment Success Combinations for Functions Incorporated into the Oconee LOCA Event Tree

LOCA Size	Reactor Subcriticality	Injection Phase: Containment Overpressure Protection Due to Steam Evolution	Injection Phase: Post Accident Radioactivity Removal	Injection Phase: Emergency Core Cooling[1]	Recirculation Phase: Containment Overpressure Protection Due to Steam Evolution	Recirculation Phase: Post Accident Radioactivity Removal	Recirculation Phase: Emergency Core Cooling
<4" ($\leq$.087 ft^2) S_3LOCA	>5 Control Rod Groups Inserted Into Core by the Reactor Protection System (RPS)	1/2 Containment Spray Injection (CSIS) OR 1/3 Reactor Bldg. Fan Coolers (RBCS	1/2 CSIS	1/3 High Pressure Injection (HPIS)[3]	1/2 Containment Spray Recirc. (CSRS) with the LPRS heat exchanger OR 1/3 RBCS	1/2 CSRS	1/3 High Pressure Recirc. (HPRS)[2] with Associated Low Pressure Recirc. (LPRS)
4"-10" (.087-.55 ft^2) S_2 LOCA				1/3 HPIS AND 1/2 Low Pressure Injection (LPIS)			1/2 LPRS
10"-13.5"D (.55-1.0 ft^2) S_1LOCA				1/3 HPIS AND 2/2 LPIS			
(>1.0 ft^2) D > 13.5" 'A' LOCA				1/3 HPIS and 1/2 LPIS and 2/2 CFT			

[1]The ECCS success criteria utilized in this study was taken from the FSAR. Duke Power has recently proposed an alternate criteria. The Duke criteria is: 1/3 HPIS for < 4" breaks, 1/3 HPIS and 1/2 LPIS and 2/2 CFT for 4"-10" breaks, 1/2 LPIS and 2/2 CFT for 10" breaks. Utilization of this criteria would not change significantly the results of this study.

[2]It is assumed that the HPRS pumps can operate at greater than 200°F (the pump design temp is 200°F). In some sequences, water temperatures of greater than 200°F may occur (i.e., success of ECR with the LPRS heat exchangers unavailable).

[3]See Table 4-3 for variation depending on success or failure of event K.

Table 4-3 Event Definition for LOCA Event Tree

LOCA - A breach of the pressure boundary of the reactor coolant system (RCS) which causes an uncontrollable loss of water inventory. There are four LOCA categories.

A Large LOCA - a breach of the RCS with a flow area greater than 1 ft^2 ($A > 13.5"$ diameter).

S_1 Medium LOCA - a breach of the RCS with a flow area greater than .55 ft^2 and less than or equal to 1 ft^2 ($13.5" \geq S_1 > 10"$ diameter).

S_2 Small LOCA - a breach of the RCS with a flow area greater than .087 ft^2 and less than or equal to .55 ft^2 ($10" \geq S_2 > 4"$ diameter).

S_3 Small-Small LOCA - a breach of the RCS with a flow area less than or equal to .087 ft^2 ($4" \geq S_3$ diameter).

K Reactor Protection System (RPS) - Failure of automatic reactor scram system (Note: This event applies only to S_2 and S_3 LOCAs. For other LOCAs reactor subcriticality is assumed due to the effects of blowdown.)

C Containment Spray Injection System (CSIS) - Failure to provide flow from at least 1 of 2 reactor building spray pumps, taking suction from the BWST, through its respective spray header into the containment atmosphere.

Table 4-3 Event Definition for LOCA Event Tree (Con't)

Y Reactor Building Cooling System (RBCS) (Injection Phase) - Failure to remove steam (heat) from the containment atmoshphere by at least 1 out of 3 reactor building cooling fans.

D Emergency Coolant Injection System (ECIS) - Failure to provide sufficient water to the core to prevent melt during the injection phase.

- ECIS for Large (A) LOCA - failure to provide flow to the RCS from at least 1 of 3 high pressure trains, 1 out of 2 low pressure trains (taking suction from the BWST), and 2 out of 2 core flooding tanks.

- ECIS for Medium (S_1) LOCA - failure to provide flow to the RCS from at least 1 of 3 high pressure trains and 2 of 2 low pressure trains (taking suction from the BWST).

- ECIS for Small (S_2) LOCA -

  (a) For sequences containing event $\overline{K}$ - failure to provide flow to the RCS from at least 1 out of 3 high pressure pumps and 1 out of 2 low pressure trains (taking suction from the BWST).

  (b) For sequences containing event K - failure to provide flow to the RCS from 2 out of 3 high pressure pumps and 1 out of 2 low pressure trains

Table 4-3 Event Definition for LOCA Event Tree (Con't)

(taking suction from the BWST) and to provide flow to the secondary side of the steam generators from 1 out of 3 emergency feedwater trains.

- ECIS for Small-Small (S_3) LOCA -

  (a) For Sequences containing event $\overline{K}$ - failure to provide flow to the RCS from at least 1 out of 3 high pressure trains (taking suction from the BWST).

  (b) For Sequences containing event K - failure to provide flow to the RCS from 2 out of 3 high pressure pumps (taking suction from the BWST) and to provide flow to the secondary side of the steam generators from 1 out of 3 emergency feedwater trains.

F Containment Spray Recirculation System (CSRS) - Failure to provide flow from at least 1 out of 2 reactor building spray pumps, taking suction from the reactor building sump, through its respective spray header into the containment atmosphere.

Z Reactor Building Cooling System (RBCS) (Recirculation Phase) -

Table 4-3 Event Definition for LOCA Event Tree (Con't)

Failure of at least 1 out of 3 reactor building cooling fans to continue to remove steam (heat) from the containment atmosphere.

H Emergency Coolant Recirculation System (ECRS) - Failure to provide sufficient water to the core to prevent core melt in the recirculation phase of a LOCA.

- ECRS for Large, Medium and Small LOCA - failure to provide flow to the RCS from at least 1 out of 2 low pressure trains (taking suction from the reactor building sump).

- ECRS for Small-Small LOCA - failure to provide flow to the RCS from at least 1 out of 3 high pressure trains with its associated low pressure train (taking suction from the reactor building sump).

G LPRS Heat Exchange (LPRSX) - Failure to provide sufficient cooling of containment sump water by at least one of two LPRS heat exchangers. This requires that both LPRS trains or their associated low pressure service water trains are inoperable.

Table 4-4. Alternate Equipment Success Combinations for Functions Incorporated into Oconee Transient Event Tree

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

Table 4-5. Event Definitions for Transient Event Tree

T_1, T_2, T_3 Transient - Any abnormal condition in the plant which requires that the plant be shut down, but does not directly breach RCS integrity.

- T_1 - Shutdown initiated by a loss of offsite power.
- T_2 - Shutdown initiated by a loss of main feedwater caused by other than a loss of offsite power.
- T_3 - Shutdowns with main feedwater initially available.

K Reactor Protection System (RPS) - Failure to insert $\geq$ 6 control rod groups into the core.

M Uninterrupted Power Conversion System (PCS) - Failure of the PCS to remain in uninterrupted operation following a transient. Since the PCS will be interrupted by a T_1 and T_2, event M will always follow these initiators.

L Emergency Feedwater System (EFWS), Recovery of the PCS, or High Head Auxiliary Service Water System (HHASWS) - Failure to provide steam generator cooling by the use of at least one of the following methods:

a) Recovery of the PCS

b) Flow from the EFWS turbine drive pump to at least one steam generator or from one EFWS motor driven pump to its associated steam generator

Table 4-5. Event Definitions for Transient Event Tree (Con't)

c) Flow from the HHASWS pump to at least one steam generator.[1]

P_1 RCS Safety/Relief Valve Demand (SR/Demand) - Failure to require the RCS pressure relief function (i.e. - RCS pressure does not exceed relief setpoint).

P_2 Safety/Relief Valves Open (SR/VO) - Failure of sufficient S/RVs to open and relieve excess primary system pressure.

Q Safety/Relief Valves Close (SR/VR) - Failure of any S/RVs which opened to reseat.

U High Pressure Injection System (HPIS) - Failure to establish flow from BWST to the RCS using at least one high pressure injection pump (for the purpose of a core cooling via a "bleed and feed" operation).

O Reactor Building Cooling System (RBCS) Failure to prevent containment overpressure due to steam evolution by the use of at least one RCBS Fan.

O' Containment Spray Injection System (CSIS) - Failure to prevent containment overpressure due to steam evolution or remove radioactive effluents from the containment atmosphere by the use of at least one CSIS subsystem.

[1]The HHASWS would only be utilized following a station blackout (i.e., loss of offsite and onsite AC power). Credit is therefore not given for this system for T_2 and T_3 transients.

Table 4-6. Information on Oconee Systems Involved in LOCA Event Tree

				ECIS				ECRS		
LOCA Initiators \ System	RPS K (App B3)	CSIS C (App B11)	RBCS Y (App B15)	CFS D (App B5)	LPIS D (App B6)	HPIS D (App B8)	CSRS F (App B12)	LPRS H (App B7)	HPRS H (App B9)	CHRS (LPSWS) G (App B14)
A		Eq B11-1(a)	Eq B15-1(a)	X	Eq B6-1	Eq B8-1(a)	X	X		X
S_1		Eq B11-1(a)	Eq B15-1(a)		Eq B6-2	Eq B8-1(a)	X	X		X
S_2	2.6×10^{-5}	Eq B11-1(a)	Eq B15-1(a)		Eq B6-1	Eq B8-1(a)	X	X		X
S_3	2.6×10^{-5}	Eq B11-1(a)	Eq B15-1(a)			Eq B8-1(a)	X	X	X	X
T_1Q, T_2Q, T_3Q		Eq B11-1(a)	Eq B15-1(a)			Eq B8-1(a)	X	X	X	X
$T_1(B_3)$ Q		Eq B11-1	Eq B15-1			1.0	X			

NOTE:

1. The letter "X" denotes that a single Boolean equation was used to describe the system. Refer to the appropriate appendix.

Table 4-7. Information on Oconee Systems Involved in Transient Event Tree

System / Transient Initiators	RPS(4) K (App B3)	Uninterrupted PCS(1)(5) M	EFSW/PCS Recovery(5) HHASWS L (App B13)	SR/(2) DEMAND P_1 (DATA)	SR/VO(3) P_2	SR/VR(2) Q (DATA)	HPIS U (App B8)	RBCS O (App B15)	CSIS O' (App B11)
T_1	ϵ	1	Eq B13-3	$\sim 10^{-2}$	2×10^{-5}	5×10^{-2}	Eq B8-1(b)	Eq B15-1(a)	Eq B11-1(a)
T_2	2.6×10^{-5}	1	Eq B13-1	$\sim 10^{-2}$	2×10^{-5}	5×10^{-2}	Eq B8-1(b)	Eq B15-1(a)	Eq B11-1(a)
T_3	2.6×10^{-5}	10^{-2}	Eq B13-2	$\sim 10^{-2}$	2×10^{-5}	5×10^{-2}	Eq B8-1(b)	Eq B15-1(a)	Eq B11-1(a)
$T_1(B_3)$	ϵ	1	Eq B13-4	$\sim 10^{-2}$	2×10^{-5}	5×10^{-2}	Eq B8-1	Eq B15-1	Eq B11-1

Notes

1. The uninterrupted PCS failure probability estimate of 10^{-2} was extracted from the RSS.

2. The SR/DEMAND and SR/VR data is based on PWR operating experience reported in NUREG-0611,0560,0565,636. The SR/VR data gives credit to the operator to close the PORV block value. However, due to post TMI changes to the pressurizer PORV actuation set point,it can be reasonably assured that a PORV demand will also demand pressurizer safety valves. Since the safety valves do not have block valves, the operator cannot isolate a safety valve if it should fail to reclose.

3. The SR/VO unavailability was obtained from relief value data given in Table III 2-1 of the RSS and assuming that both Oconee pressurizer code safety/relief valves must open.

4. The RPS unavailability is epsilon for T_1 initiators because the only RPS failure mode results from stuck rods since rod holding power is removed by the initiator. Research presented in NUREG-0460 indicates a much greater number of stuck rods than the number assumed in the RSS is necessary to prevent a successful reactor shutdown.

5. The long-term (~2 days) unavailability for PCS recovery, EFWS, and/or HHASWS was assumed to be epsilon. This assumption affects the frequency assessed for the TMLOO' sequence only.

Table 4-8. Dominant Cut Sets for Sequence T_2MLQ-FH

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot Q \cdot CONST1 \cdot PCSNR \cdot WXCM$	1.1×10^{-8}	T_2M - loss of power conversion system; $F(T_2M) = 3/R\text{-yr}$ Q - failure of one pressurizer safety/relief valve to close; $P(Q) = 0.05$ CONST1 - failure of emergency feedwater system due to primarily hardware failure of the turbine pump train and both of the electric pump trains; $P(CONST1) = 2.4 \times 10^{-4}$ PCSNR - failure to restore the power conversion system; $P(PCSNR) = 0.1$ WXCM - failure of the operator to open the sump valves at the start of recirculation which are common to both the spray and core cooling system; $P(WXCM) = 3 \times 10^{-3}$
$T_2 \cdot M \cdot Q \cdot CONST1 \cdot PCSNR \cdot B \cdot W$	1×10^{-10}	T_2,M,Q,CONST1,PCSNR (discussed above) B·W - failure of the low pressure/containment spray injection Train B tank suction valves and low pressure/containment spray recirculation Train A sump suction valves; $P(B \cdot W) = 2.7 \times 10^{-5}$
$T_2 \cdot M \cdot Q \cdot CONST1 \cdot PCSNR \cdot C \cdot X$	1×10^{-10}	T_2,M,Q,CONST1,PCSNR (discussed above)

Table 4-8. Dominant Cut Sets for Sequence T_2MLQ-FH (Con't)

Cut Set	Cut Set Frequency	Description
		C·X - failure of the low pressure/containment spray injection Train A tank suction valves and low pressure/containment spray recirculation Train B sump suction valves; $P(C \cdot X) = 2.7 \times 10^{-5}$
$T_2 \cdot M \cdot Q \cdot CONST1 \cdot PCSNR \cdot W \cdot X$	2.6×10^{-11}	T_2,M,Q,CONST1, PCSNR (discussed above)
		W·X - failure of both low pressure/containment spray recirculation sump suction valves; $P(W \cdot X) = 7.2 \times 10^{-5}$

$$F(T_2MLQ\text{-}FH) = \sum(\text{Cut Sets}) = 1.2 \times 10^{-8}$$

Table 4-9. LOCA Sequences with Frequencies $\geq 10^{-8}$/R-yr

A		S_1		S_2		S_3	
AD	3.6×10^{-7}	S_1D	6.7×10^{-6}	S_2FH	1.3×10^{-6}	S_3H	1.0×10^{-5}
AFH	3.2×10^{-7}	S_1FH	3.0×10^{-7}	S_2D	2.0×10^{-6}	S_3FH	4.2×10^{-6}
AH	8.0×10^{-8}	S_1CD	1.2×10^{-7}	S_2H	3.0×10^{-7}	S_3D	1.4×10^{-6}
ACD	4.3×10^{-8}	S_1DF	7.0×10^{-8}	S_2CD	1.7×10^{-7}	S_3CD	5.2×10^{-7}
		S_1YD	1.3×10^{-8}	S_2YD	1.2×10^{-8}	S_3CY	6.6×10^{-8}
		S_1H	1.0×10^{-8}	S_2DF	1.0×10^{-8}	S_3CH	6.0×10^{-8}
						S_3YD	3.4×10^{-8}
						S_3YH	1.5×10^{-8}

V 7.4×10^{-5}

Table 4-10. Transient Induced LOCA Sequences with Frequencies ≥ 10^{-8}/R-yr

T_1		T_2		T_3	
T_1MQ-H	7.4×10^{-7}	T_2MQ-H	1.1×10^{-5}	T_3MQ-H	1.5×10^{-7}
$T_1(B_3)$MLQ-D	5.0×10^{-7}	T_2MQ-FH	5.0×10^{-6}	T_3MQ-FH	6.2×10^{-8}
T_1MQ-FH	3.2×10^{-7}	T_2MQ-D	1.5×10^{-6}	T_3MLQ-YD	4.8×10^{-8}
T_1MLQ-YD	2.4×10^{-7}	T_2MQ-CD	6.0×10^{-7}	T_3MQ-D	2.0×10^{-8}
T_1MQ-D	1.0×10^{-7}	T_2MLQ-YD	3.6×10^{-7}		
$T_1(B_3)$MQ-D	5.0×10^{-8}	T_2MQ-CH	6.3×10^{-8}		
T_1MLQ-H	5.8×10^{-8}	T_2MQ-YD	3.9×10^{-8}		
T_1MQ-CD	4.0×10^{-8}	T_2MLQ-H	2.6×10^{-8}		
T_1MLQ-FH	2.0×10^{-8}	T_2MQ-YH	1.5×10^{-8}		
		T_2MLQ-FH	1.1×10^{-8}		

Table 4-11. Transient Sequences with Frequencies $\geq 10^{-8}$/R-yr

T_1		T_2		T_3	
T_1MLUO	5.4×10^{-6}	T_2KMU	7.8×10^{-6}	T_3MLUO	1.1×10^{-6}
$T_1(B_3)$MLU	2.2×10^{-6}	T_2MLUO	8.1×10^{-6}	T_3MLU	1.5×10^{-7}
T_1MLU	2.0×10^{-6}	T_2MLU	1.2×10^{-6}		
T_1MLUO'	5.8×10^{-8}	T_2MLUO'	3.3×10^{-8}		
$T_1(B_3)$MLUOO'	3.0×10^{-8}	T_2MLUOO'	2.4×10^{-8}		
T_1MLUOO'	1.6×10^{-8}				
$T_1(B_3)$MLUO'	1.0×10^{-8}				

Table 4-12. Footnote to LOCA and Transient Event Trees

Recent preliminary experiments performed at Sandia National Laboratories which simulate the core melt process suggest that the RBCS and CSRS may be significantly degraded or fail when operating in a post core melt environment. The Oconee event trees do not reflect this potential system/core melt interaction.

The experiments indicate that during the core meltdown process, large quantities of aerosols are generated which plate out very well on cooled surfaces. The experiments also indicate that the plate out material has very poor heat transfer characteristics (i.e., very low thermal conductivity). Therefore, following a core meltdown, plate out of the aerosols on the RBCS cooling coils may degrade their heat removal capability to the point of uselessness.

The experiments also indicate that during the core meltdown process, millions of solidified metal droplets of various sizes would be ejected when the molten core interacts with the concrete in the cavity below the reactor vessel. Following a core meltdown, it is reasonable to assume that the water in the reactor building sump would be contaminated with these metal chips. Discussions with pump experts at Babcock and Wilcox have also revealed that the containment spray pumps may sieze if the sump water contains small metal chips.

In the Oconee analysis, it was assumed that the RBCS and CSRS would be available post core melt, barring other hardware or actuation failures.

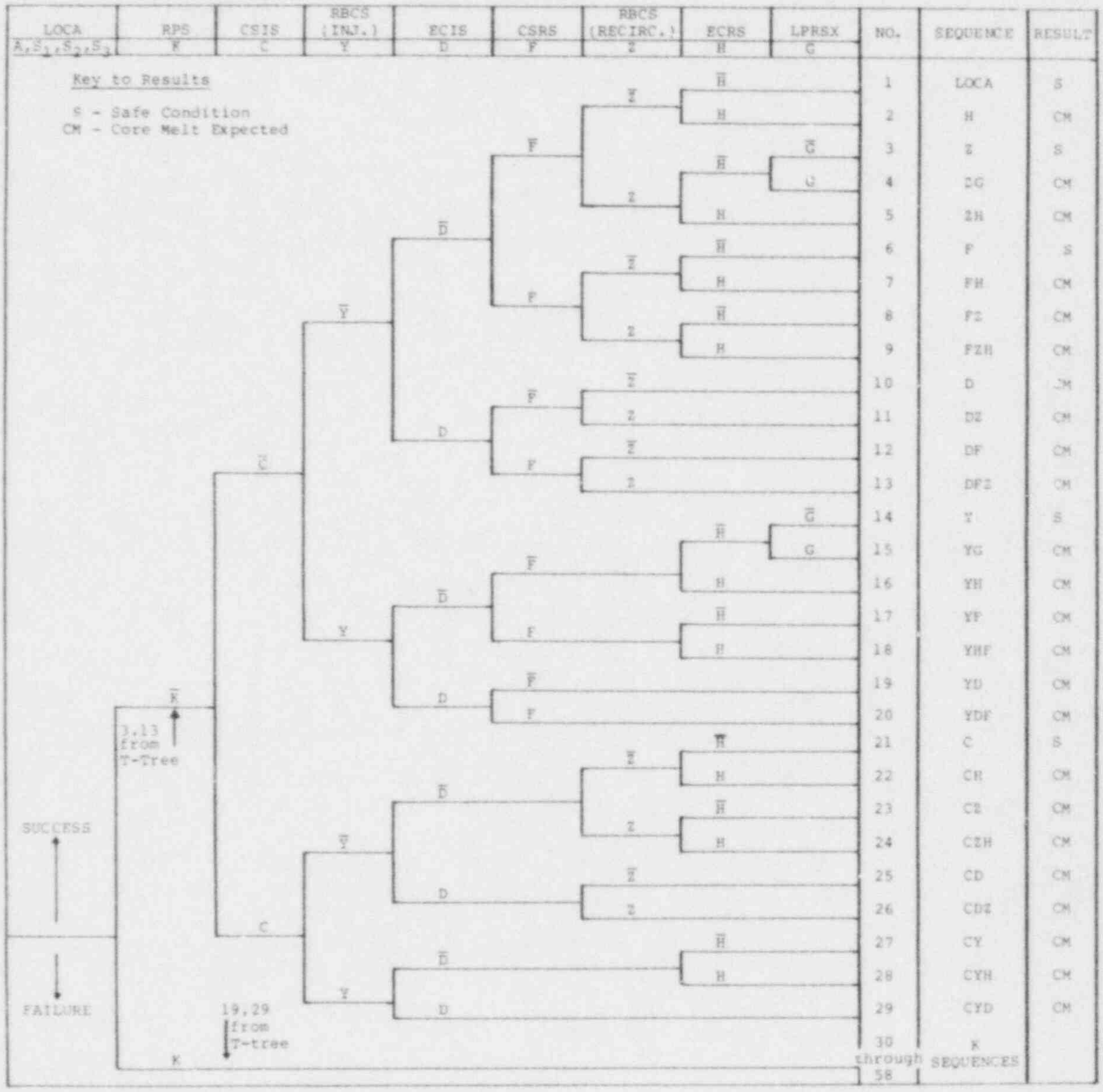


Figure 4-1 Oconee LOCA Event Tree[1]

[1]See discussion given in Table 4-12.

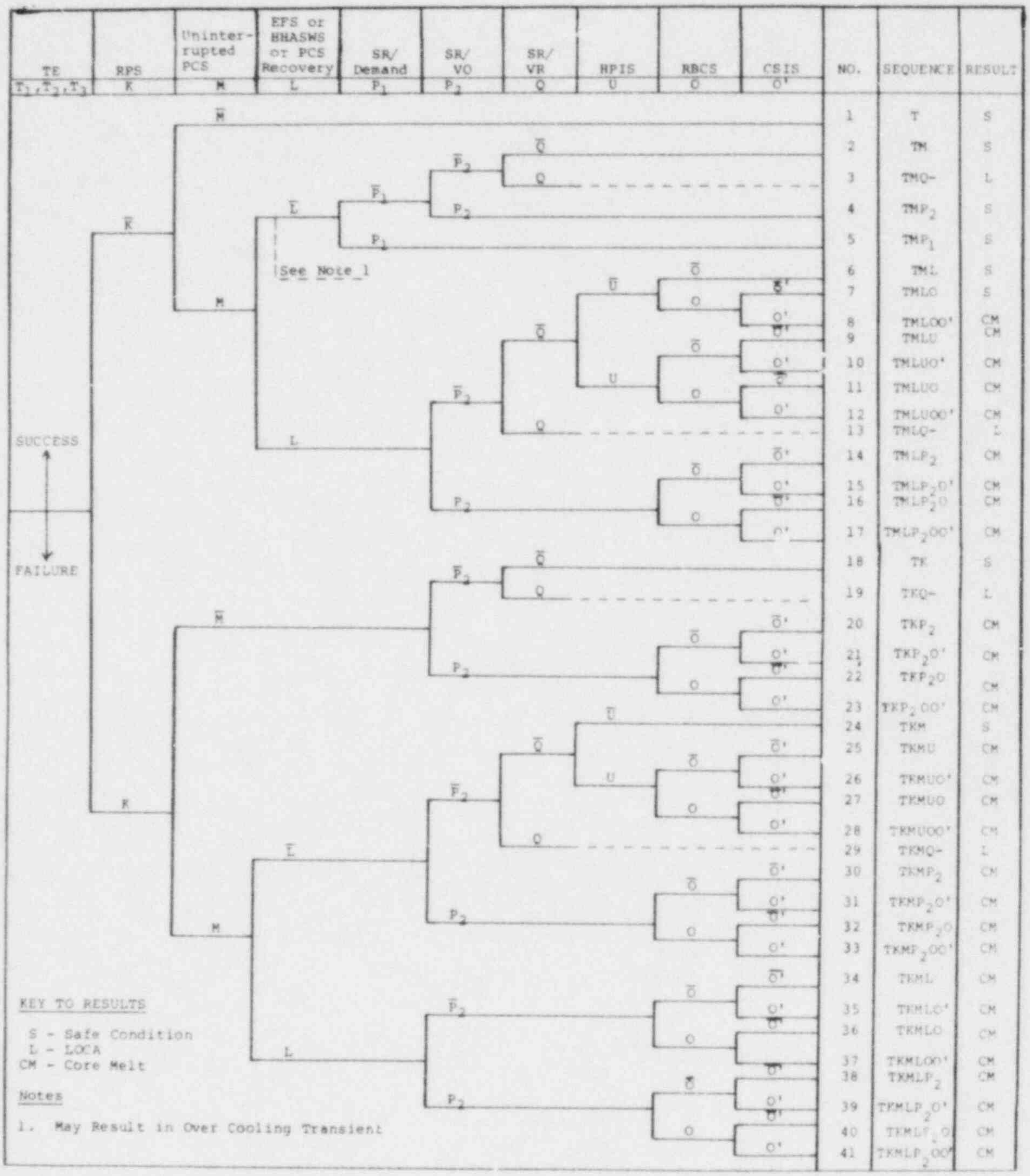


Figure 4-2 Oconee Transient Event Tree[1]

[1]See discussion given in Table 4-12.

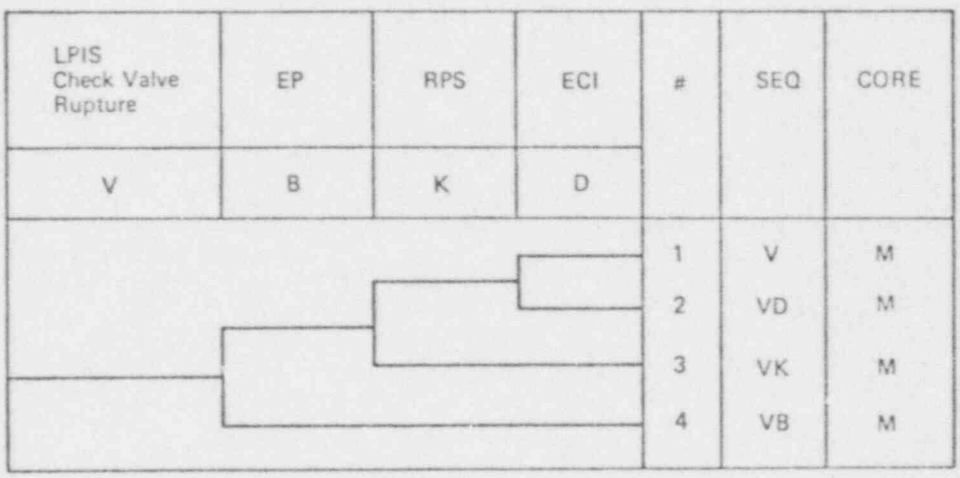


Figure 4-3 LPIS Check Valve Rupture Event Tree

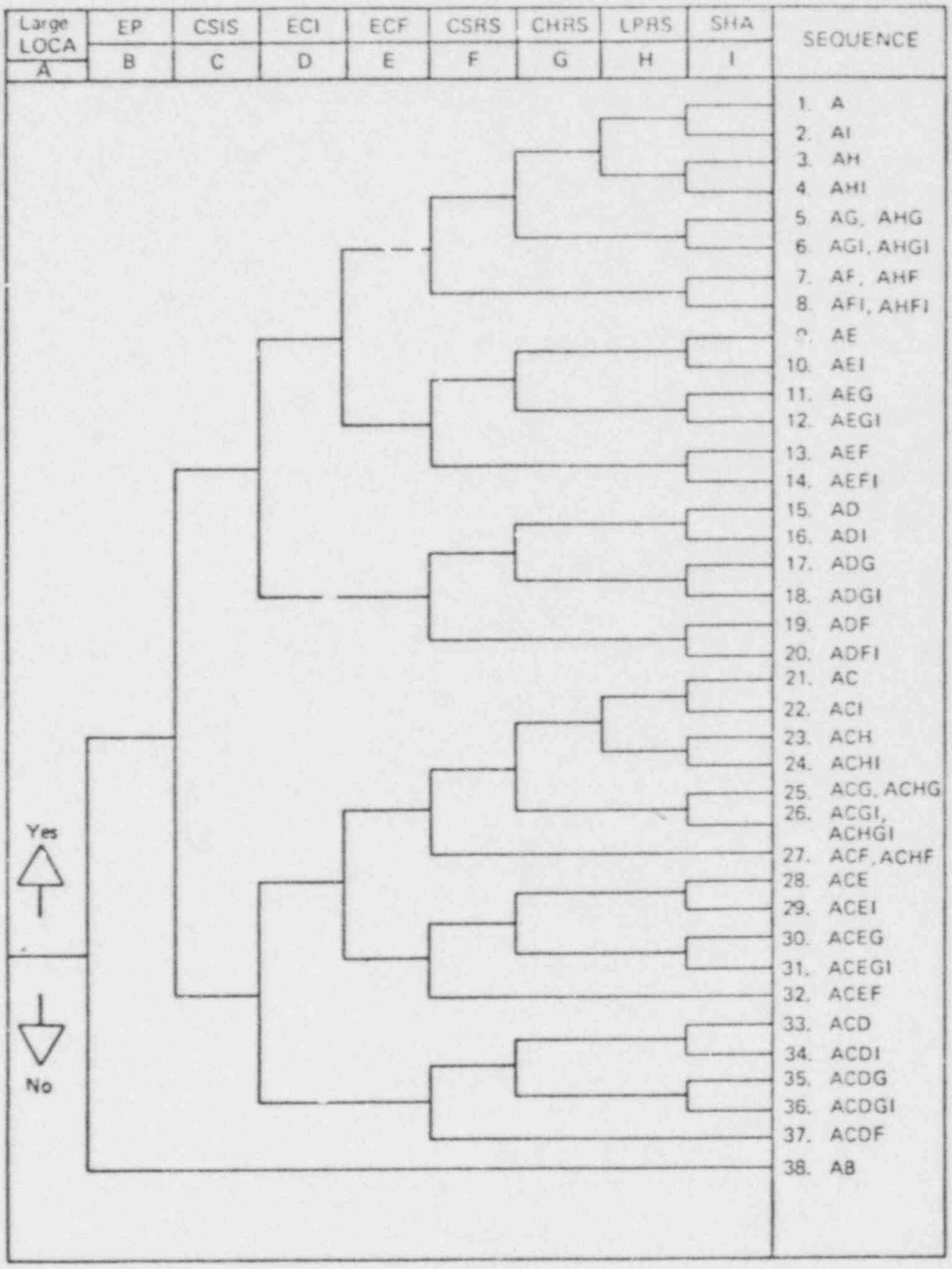


Figure 4-4 Surry Large LOCA (A) Event Tree

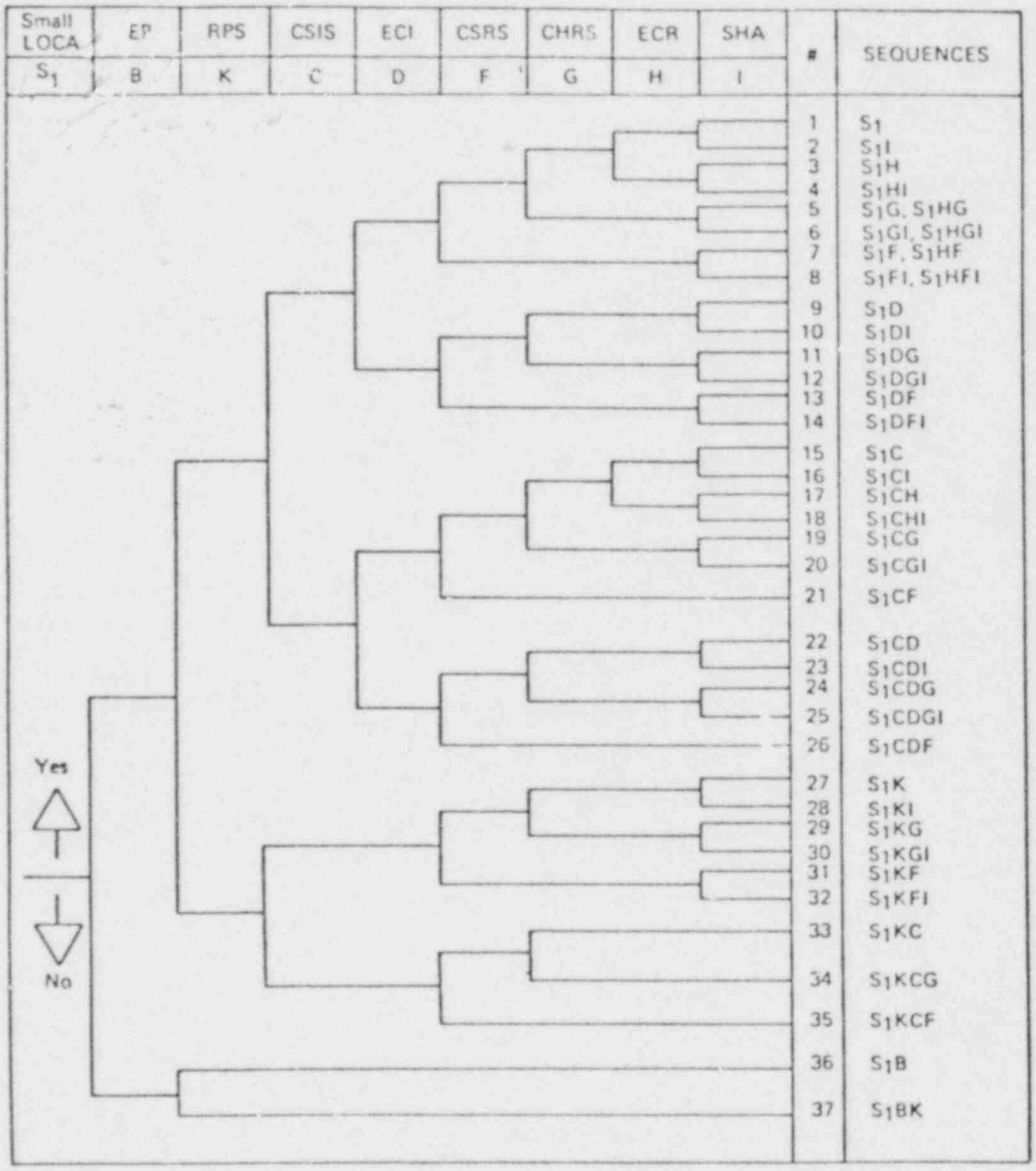


Figure 4-5 Surry Small LOCA (S_1) Event Tree

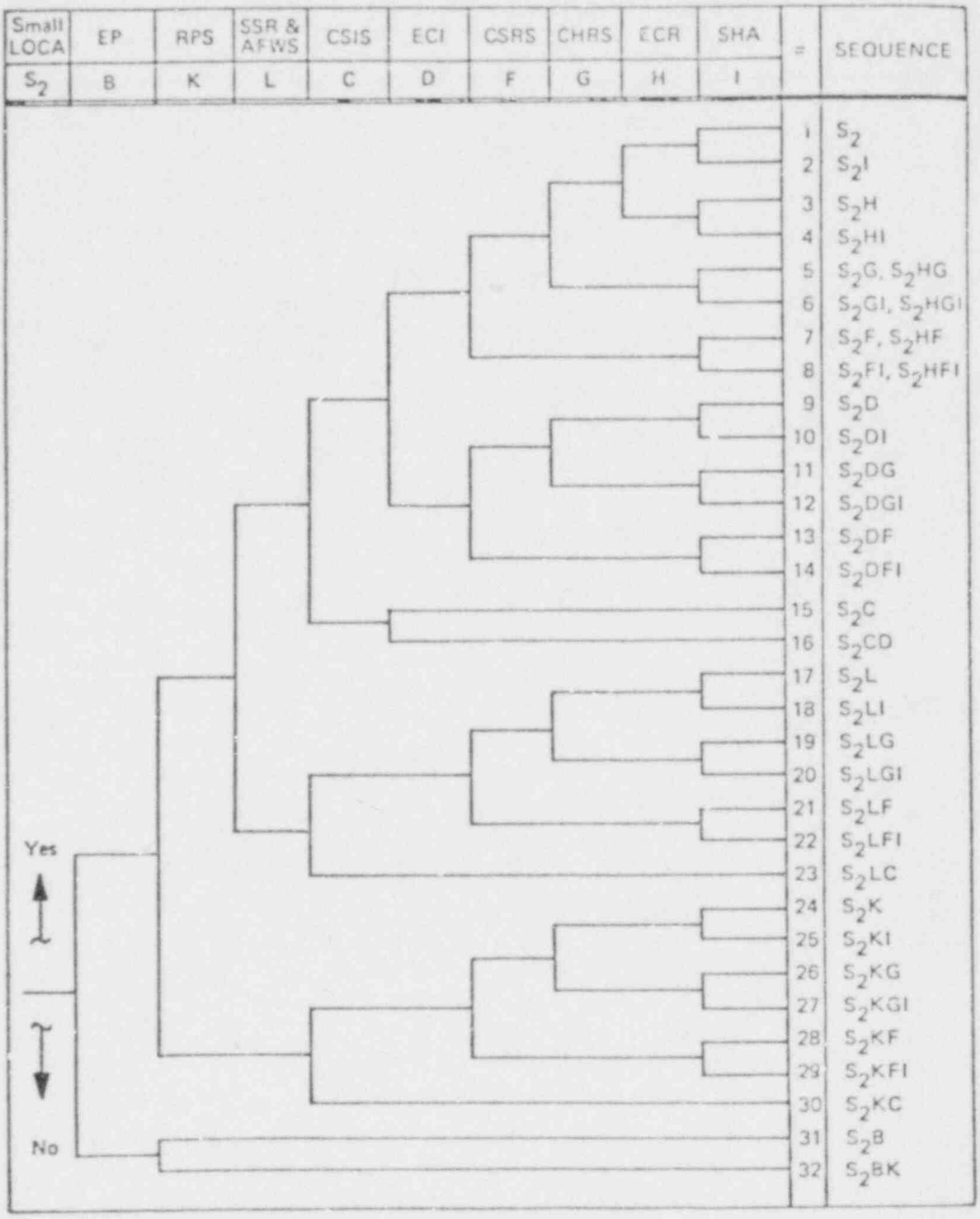


Figure 4-6 Surry Small LOCA (S_2) Event Tree

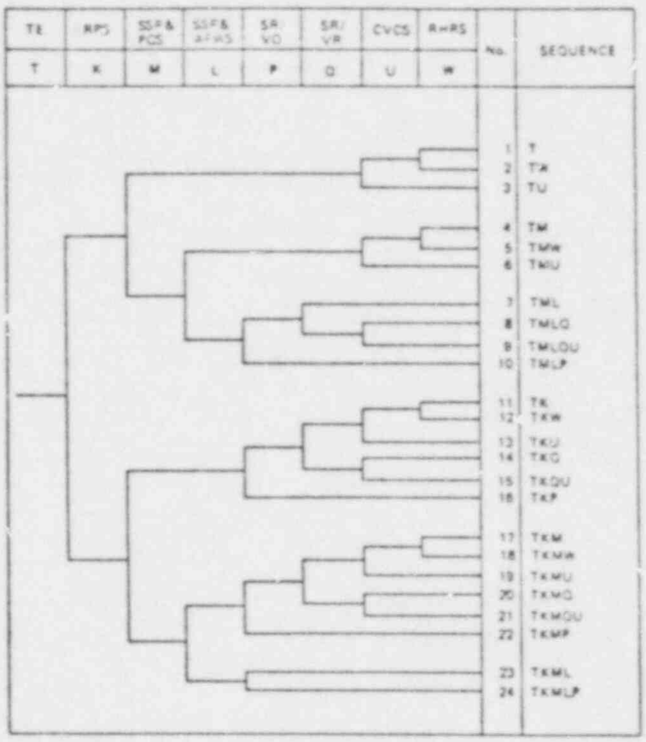


Figure 4-7 RSS Transient Event Tree, PWR

5.0 ACCIDENT PROCESS ANALYSIS TASK

This chapter summarizes the results of the accident processes and source term evaluation for hypothesized core meltdown accidents in the Oconee PWR.

5.1 Scope

The accident processes task is aimed at quantitatively describing the physical phenomena that are expected to occur during hypothetical reactor meltdown accidents and at determining the nature and quantities of fission products that would be expected to be released from containment during the various accident sequences. The principal physical processes and accident parameters of concern are:

a) The time scale of the accident, particularly the times for the start and completion of core melting.

b) The time required for the molten core to fail the reactor vessel bottom head.

c) Possible energetic interactions when the core debris fall to the floor of the reactor cavity, including the likelihood of containment failure due to such interactions.

d) Long-term pressure-time history within the reactor containment, including the likelihood and time of containment failure due to overpressure.

e) The probability and consequences of hydrogen burning or detonation within the containment building.

f) The interaction of the core debris with the concrete foundation.

g) The magnitude and timing of fission product release from the fuel to the containment atmosphere.

h) The transport and removal of the various fission product species in the containment building atmosphere.

i) Time-dependent leak rate from the containment building, including the airborne fission products.

The analyses were conducted with the MARCH and CORRAL computer codes. MARCH performs a consistent analysis of the thermal hydraulics associated with the successive stages of core meltdown and containment response. It represents a significant improvement over the methods of meltdown analysis used in the RSS. CORRAL describes fission product transport and deposition within the containment and determines the leakage to the environment. Much of the input required by CORRAL is provided by MARCH. The current version of CORRAL is a modification and generalization of the CORRAL code developed during the Reactor Safety Study. The general features of these codes are described in References (2, 6, 7).

5.2 Containment Processes and Accident Sequence Selection

5.2.1 Containment Event Tree

The containment event tree utilized for the Oconee evaluation was identical to that developed in the Reactor Safety Study. This is shown in Figure 5-1, with the notation given in Table 5-1.

5.2.2 Containment Failure Pressure

The Oconee containment structure consists of a post-tensioned reinforced concrete cylinder and dome connected to and supported by a massive reinforced concrete foundation slab. The interior surface of the structure is lined with a 1/4-inch thick welded steel plate to assure a high degree of leak tightness. In the post-tensioned concept, the internal pressure load is balanced by the application of an opposing external pressure type load on the structure. Sufficient post-tensioning is used on the cylinder and dome to more than balance the internal pressure so that a margin exists beyond that required to resist the design basis accident pressure. Bonded reinforced steel is also provided to distribute strains due to shrinkage and temperature changes. Additional bonded reinforcing steel is included around penetrations and discontinuities to resist local moments and shears. The basic design criterion is that the integrity of the liner be maintained under all anticipated load conditions and the structure shall have an elastic, low-strain response under all design loadings.

Some of the principal design parameters for the containment building are as follows:

Inside Diameter	116 ft
Inside Height	208.5 ft
Vertical Wall Thickness	3.75 ft
Dome Thickness	3.25 ft
Foundation Slab Thickness	8.5 ft
Liner Thickness	0.25 inch
Free Volume	1910000 ft^3
Design Pressure	59 psig
Test Pressure	68 psig
Design Leak Rate	0.1 ^{v}/o per day

In the absence of detailed information on the sizing and placement of reinforcing in the structure and given the limited scope of the study, it was not possible to perform a detailed nonlinear analysis of the structure to define an expected failure level. On the basis of available information on the details of the structure and limited analyses, it was estimated that the concrete would be loaded in tension and the post-tensioning tendons in the hoop direction would reach their yield strength at an internal pressure of about two times the design level. The ultimate strength of the hoop tendons would be approached at about three times design pressure. Based on these observations, the nominal failure level for the purposes of this study was selected to be two times the design pressure, or 133 psia internal pressure.

As utilized here, the failure pressure is not a single discrete value, but a continuous variable with a cumulative probability distribution. This approach recognizes that the probability of structural failure is small at loads slightly above design, but increases with increasing loading. By definition, the probability of failure at the nominal failure pressure is 0.5; it approaches unity as the stresses due to the loading approach the ultimate strength of the materials. Under this approach, a failure pressure of 133 $\pm$ 20 psia has been selected for the purpose of this study.

5.2.3 Oconee PWR Accident Sequences Considered

Accident event trees have been developed by the Systems Analysis Team for several LOCAs (A, S_1, S_2, S_3) as well as transients (T_1, T_2, T_3). Based on the preliminary evaluation of the event trees and the potential consequences of the various sequences, a number of accident sequences were identified as being potentially important with regard to overall accident risk. This set of accident sequences identified in Table 5-4 was examined in more detail; the results of these analyses formed the basis for the conclusions of this study. A number of these potentially important sequences were explicitly evaluated by means of MARCH and CORRAL calculations, others were evaluated on the basis of similarity with sequences previously evaluated, still others were considered on the basis of insights developed as a result of related analyses on other reactor designs.

5.3 Analyses of Accident Processes

The MARCH (Meltdown Accident Response CHaracteristics) code provides the analysis of the various thermal-hydraulic processes during reactor meltdown accidents. MARCH contains a number of interrelated and coupled subroutines, each of which treats a particular process or phase of the accident. The principal subroutines are noted below. PRIMP evaluates the primary coolant system response including pressure history, coolant leakage, effect of secondary system heat transfer, and emergency core cooling system operation, if appropriate. These features are essential for the analysis of small break and transient accident sequences. BOIL is the only element of MARCH that was available at the time of the Reactor Safety Study. The initial versions of BOIL described the boiloff of water from the reactor vessel and the meltdown of the core up to the point of core support failure; they assumed a large LOCA as the initiating event. The current version of BOIL provides continuous transitions for core collapse, grid plate failure, and the dropping of the core debris into the lower head of the reactor vessel; a number of user selected options are provided for these transitions. HEAD evaluates failure of the reactor vessel head considering meltthrough as well as the effects of pressure stress; the latter can have a significant effect in small break and transient sequences. The HOTDROP subroutine describes the interaction of the core debris with water in the reactor cavity following vessel meltthrough, including such effects as debris fragmentation, heat transfer, and chemical reactions. The interaction of the core debris with concrete is described by the INTER code, Reference (8); the latter was written at Sandia National Laboratories and has been adapted and integrated by BCL into MARCH. The FPLOSS routine describes the release of the radionuclides from the fuel and follows the heat source associated with each group of fission products. The MACE routine describes the containment temperature and pressure history taking into account nuclear and chemical heat generation, heat losses to structures, effects of containment safeguards, intercompartment flows, leakage to the outside, etc. MACE is continuously coupled to the other subroutines in MARCH. It may be noted that the MACE subroutine in MARCH provides the essential containment thermal-hydraulic input required in CORRAL, the fission product transport code to be discussed later.

5.3.1 Results

The results of the MARCH analyses of the key accident sequences are summarized in Table 5-2. As can be seen, not all the accident sequence-containment failure mode combinations were evaluated. However, a sufficient number of cases were evaluated in detail to develop an overall insight on expected phenomena in the sequences of interest. Some general observations on the MARCH results are given below. A description of other Oconee sequences is given in Appendix C.

The accidents initiated by pipe ruptures were broken up in the Systems Analysis Task into four categories according to the size of the initiating primary system break. A classification of this type was required because the probability of occurrence varies with the size of the break and also because the specific engineered safety features required to mitigate the LOCA are a function of the size of the break. In terms of the accident response as predicted by MARCH, the LOCAs initiated by greater than 2-inch diameter breaks are substantially similar to the large break (A) cases. While the depressurization and blowdown rates for the S_1 and S_2 cases are different from the A cases, they were sufficiently rapid for these sets of cases so as to lead to very similar times for safety system actuation, core melting, containment failure, etc. Thus, from the accident processes viewpoint, the A, S_1, and S_2 sequences were treated as equivalent. For LOCAs initiated by breaks of $\leq$ 2-inch diameter, on the other hand, the predicted accident behavior was somewhat different. In the evaluation of the accident processes, the S_3 sequences were characterized by 2-inch breaks. In these, the primary system depressurization is quite slow, with core melting in most cases taking place while the primary system was still at elevated pressure. The latter situation has several implications, including: reducing the probability of the occurrence of reactor vessel steam explosions, shortening the incremental time required for reactor vessel failure (meltthrough) due to the addition of significant pressure stress, and delaying the discharge of accumulator water until after substantial core melting or even after reactor vessel failure. The transient (T) sequences were typified by extended primary system depressurization times and, thus, were generally similar in most respects to the S_3 sequences discussed above.

5.3.2 Containment Failure Modes

The containment event tree used for the present analysis is the same as that developed in the Reactor Safety Study for the PWR. Some further observations based on the MARCH analyses of a number of accident sequences will be given here.

The consideration of the possibility of containment rupture due to steam explosions in the reactor vessel (α) is largely based on the analyses that were conducted for the Reactor Safety Study, with some modification to take into account subsequent experimental work. Based on fuel-coolant interaction work at Argonne National Laboratory (ANL) and Sandia, the occurrence of steam explosions in the presence of a high ambient pressure is believed to be very unlikely. As was noted above, high primary system pressures during the core melting phase have been predicted for many of the small breaks (S_3) and transient (T) sequences. In these situations, the probability of α, the containment failure due to a steam explosion in the reactor vessel, is taken as 0.0001. In the absence of high pressure, the α probability is the same as that used in the Reactor Safety Study, namely 0.01. The differences in design between Oconee and the Reactor Safety Study PWR are not expected to have any appreciable influence on the effects of a steam explosion if it does take place.

Containment leakage (β) results from the failure to isolate, in the event of an accident, containment penetrations that are normally open. None of the sequences involving containment isolation failure were found to be among the dominant ones in the Reactor Safety Study and the same situation is expected to prevail for the Oconee design. This is a result of the combination of low probability of these sequences together with relatively modest consequences associated with them. As a result of these considerations, no containment isolation failure sequences were evaluated.

The potential for containment rupture due to hydrogen burning (γ) depends on a number of factors, namely, composition of the atmosphere, availability of an ignition source, and incremental pressure rise associated with the burning.

MARCH analyses indicate that for the Oconee core melt sequences initiated by large and intermediate LOCAs, with containment safeguards operating, conditions favorable to hydrogen burning will be achieved prior to the end of a core melting and are maintained for the duration of the sequence. In corresponding sequences with no containment safeguards, the high partial pressure of steam that typically results may preclude hydrogen burning. In very small break (S_3) and transient (T) sequences, the hydrogen is not released to the containment as it is generated, but may be retained partially in the primary system until reactor vessel failure. The potential flammability of the atmosphere subsequently may again depend on the status of the containment safeguards. Combinations and intermediate situations can also be observed in specific cases, e.g., flammable atmosphere for limited periods of time.

The question of the availability of an ignition source for hydrogen burning can have several aspects. The hydrogen generated during the core melting process will generally be at a very high temperature. If the path from the core to the containment atmosphere is short, e.g., for a hot leg break, the hydrogen may be above the spontaneous ignition temperature upon release to the containment and no other ignition source will be required to produce burning. If, on the other hand, the hydrogen passes through a substantial length of piping before reaching the containment, it may be cooled to the point where an external ignition source would be required to produce burning. In several studies of large scale melt-concrete interactions, hydrogen burning is apparently always observed. Thus, the time of reactor vessel meltthrough and dropping of the core debris on concrete may be the most likely point in the accident sequence for the ignition of hydrogen. Thus, for purposes of determining containment failure mode probabilities, ignition of hydrogen at the time of vessel meltthrough has been assumed if the composition of the atmosphere is determined to be in the flammable region. Some points of qualification regarding the application of these experimental observations to the present analyses should be noted. The experiments were conducted in a normal atmosphere with an essentially unlimited supply of oxygen (air); this is clearly not the case in a closed containment where the quantity of air is limited and where the partial pressure of steam may be considerable.

Also, in many of the accident sequences of interest, the dropping of the core debris is accompanied by large quantities of water; whether this water could cool the evolved hydrogen sufficiently to avert ignition is unknown.

5.4 Fission Product Release Evaluation

The fission product release model used in the present analyses is the same as that used in the Reactor Safety Study. The model consists of four fission product release terms for each of seven classes of fission product species; additionally, a fraction of iodine, one of these species, can be specified as being converted to organic iodide. The release terms and classes of fission products are noted in the discussion below; the basis for and details of this model are given in Appendix VII of WASH-1400.

5.4.1 CORRAL Code

The CORRAL (Containment of Radionuclides Released After LOCA) code models fission product transport and disposition in containment systems of water cooled reactors. CORRAL II, the version used here, Reference (7), is a revised and generalized version of the program written for the Reactor Safety Study, Reference (2). The containment is represented by up to fifteen individual compartments connected to each other in any combination of series or parallel arrangements. Radionuclide release into the containment by any of four release mechanisms for each of eight groups of fission products can be specified. The four release mechanisms are: gap (cladding rupture) release, fuel melting, fission product vaporization, and steam explosion (oxidation) release. The eight groups of radionuclides considered are: noble gases, molecular iodine, organic iodine, cesium-rubidium, tellurium, barium-strontium, ruthenium, and lanthanum. Radionuclides can be removed from the atmosphere by particle settling, deposition, spray removal, pool scrubbing, filters, etc. Input requirements for CORRAL include: descriptions of the containment system, engineered safeguards parameters, timing of accident events, thermodynamic conditions as a function of time, intercompartment flows, leakage rates, and fission product release component fractions. The code uses this input to continuously compute changing properties and fission product removal rates as a function of time. These values are used in incremental solutions to the coupled set of differential equations to obtain the time dependent fission product concentrations and accumulations in each compartment of the containment. The principal output consists of cumulative fractional releases from containment with time for each of the fission product groups.

5.4.2 Results

The results of the CORRAL calculations are summarized in Table 5-3. The results of the specific CORRAL cases presented here were used to estimate the release fractions for other similar sequences that were not evaluated in detail. This is similar to the approach used in the Reactor Safety Study.

5.5 Summary and Discussion of Results

The combined results of the MARCH and CORRAL analyses of the Oconee (B&W) PWR key accident sequences are summarized in Table 5.4.

Given here for each of the previously identified sequences are applicable containment failure modes and the estimated release category for each accident sequence-failure mode combination. Also shown are the estimated probabilities of the various containment failure modes for each sequence. The release categories assumed here are the same as those defined in the Reactor Safety Study. It may be noted, however, that in many cases the specific fission product release calculated in the present study did not correspond very closely to the previously defined release categories. This suggests a need to reevaluate the definition of the Reactor Safety Study release categories and consider the establishment of alternate, perhaps more generally applicable categories.

5.5.1 Assignment to Release Categories

From Table 5.4 it is seen that all the steam explosion cases for Oconee are estimated to fall into Release Category 1, even those in which the sprays are initially operating. In the Reactor Safety Study the latter were predicted to be in Release Category 3. The assignment to Category 1 in the present study was due to the high ruthenium releases calculated. Examination of the details of the analyses indicates that the higher release fractions currently calculated for steam explosion cases with sprays initially operating are a direct result of larger puff releases associated with the steam explosion itself. The MARCH analyses take into account the vapor generated by the steam explosion and include this in the puff release. For steam explosions at low containment pressures, this results in larger fractional releases than were previously predicted. The results for steam explosion with no containment sprays are consistent with previous results except for the lower release of iodine. The reasons for this have been discussed previously.

Sequences involving loss of containment isolation (β) were found to lead to Category 4 or Category 5 releases, without and with containment safety features, respectively.

Containment failure due to hydrogen burning (γ) occurring near the time of vessel failure was found to lead to Category 2 and 3 releases. The Category 2 releases are associated with sequences in which the containment sprays do not operate during core melting. The Category 3 releases are associated with sequences in which the containment sprays are operational during core melting, but in which rapid hydrogen burning is still predicted to have some probability of containment failure. Even if operating, the sprays are assumed to be ineffective for fission product removal following containment failure.

Some further considerations with regard to the treatment of the hydrogen burning cases are as follows. As noted previously, the most likely time of hydrogen ignition was judged to be at the time the core debris drops to the floor of the reactor cavity. At this time, the hydrogen concentrations are generally well into the flammability range, and the assumption of burning leads to the prediction of a significant probability of containment failure even though the containment sprays and/or coolers are operating. If it were assumed that the hydrogen burned as it was generated, or as soon as a flammable composition was achieved, the effective rate of energy input into the containment would be lower, and the time of containment failure would be later than under the present assumptions, if it were predicted at all. This could, in turn, shift the hydrogen burning cases to lower release categories for the cases with sprays operating. The latter set of assumptions would require the availability of an ignition source other than the melt-concrete interaction.

Containment overpressurization (δ) in the absence of containment safety features was found to result in Category 2 releases. In some instances involving limited containment safety feature operation, containment overpressure failure was delayed substantially in time; such sequences were found to lead to Release Category 6.

Containment meltthrough (ϵ) was estimated to result in Release Category 6 or 7. The former is associated with sequences in which the containment sprays are not available; the latter with sequences in which the sprays operate.

5.5.2 Quantification of Containment Failure Modes

The quantification of the steam explosion probabilities was discussed previously. Basically the reference steam explosion probabilities are unchanged from the results of the Reactor Safety Study. For core melting at high ambient (primary system) pressure, the probabilities of steam explosions are reduced on the basis of the results of studies at ANL and Sandia.

The probability of containment isolation failure (β) was estimated in the systems analysis task to be approximately 7×10^{-3}. It was expected that sequences involving containment isolation failure would not significantly contribute to the overall risk. This expectation was supported by the results of this study.

The probability of containment failure due to hydrogen burning (γ) was evaluated in light of the previously discussed containment failure pressure. For many sequences involving complete failure of the containment safety features, the partial pressure of steam in the containment atmosphere is high enough to preclude hydrogen burning. In a number of other sequences the containment pressure at the time of assumed burning, i.e., the time of vessel head failure, was found to be elevated even with the operation of containment safety features; in these, the pressure resulting from rapid hydrogen burning was found to be about equal to the nominal failure pressure. A failure probability of 0.5 was determined for these sequences. In another class of sequences, e.g., LOCAs with containment safety features operating, the assumption of rapid hydrogen burning at the time of head failure was found to lead to pressures somewhat below the nominal failure level, but substantially above design levels. These have been assigned a failure probability of 0.2. As was previously noted, the prediction of the possibility of containment failure due to hydrogen burning in the presence of containment safety features is closely related to the assumptions of accumulation of the hydrogen up to the time of and ignition at the time of head failure. Changes in these assumptions could alter the above probabilities.

The probability of containment overpressure failure (δ) is again evaluated by comparing the predicted containment pressure with the failure pressure. In sequences where all the safety functions except ultimate heat removal are successful, containment overpressurization will be inevitable; hence the failure probability of 1. In a number of sequences, e.g., transients with loss of electric power, the peak containment pressures are limited by the amount of water that is in contact with the core debris. In these sequences, the peak pressures are generally close to the nominal failure level; these are typified by failure levels of 0.5.

Containment failure by base mat meltthrough (ε) was assumed to take place in the absence of any other failure modes. This is consistent with the treatment in the Reactor Safety Study. There are continuing questions, however, as to the inevitability of containment meltthrough. It may be possible that in many cases, the attack of the base mat can be arrested. This is a matter of continuing study in the core melt research effort.

5.5.3 <u>Interface With Systems Analysis Task</u>

The results shown in Table 5-4 when combined with the frequencies of the individual accident sequences as determined in the systems analysis task, yield the dominant accident sequences for the B&W PWR. This is discussed in the following chapter.

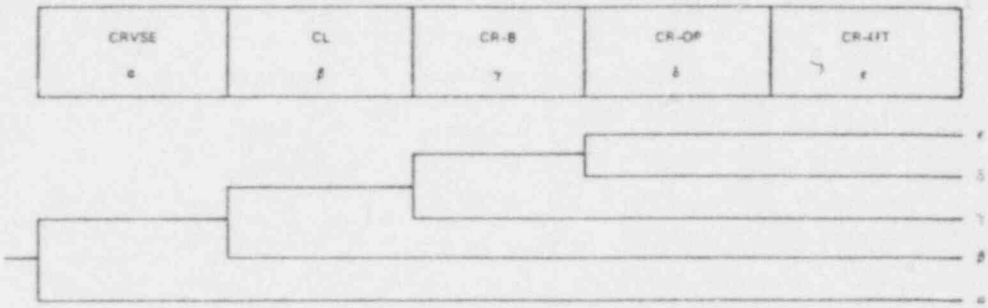


Figure 5-1 PWR Containment Event Tree

Table 5-1. Containment Event Tree Notation

Symbol	Letter	Meaning
CRVSE	α	Containment rupture due to a reactor vessel steam explosion
CL	β	Containment leakage
CR-B	γ	Containment rupture due to hydrogen burning
CR-OP	δ	Containment rupture by over-pressurization
CR-MT	ε	Containment failure by base mat meltthrough

Table 5-2. Summary of MARCH Results for Event Times*

Sequence	ECC Start	ECC Stop	Building Cooler Start	Building Cooler Stop	Containment Spray Start	Containment Spray Stop	Containment Failure Time	Containment Failure Pressure, psia	Core Uncovery	Core Melt Start	Core Melt End	Vessel Failure	Start Concrete Melt	Comments
TMLQD-γ	---	0	5	79	15	79	79	132[1]	37	59	79	79	79	H_2 burn at head failure
TMLQD-ϵ	---	0	5	---	15	---	13 hr	35[2]	37	59	79	79	79	CS recirculation at 194 min.
TMLU-γ	---	0	40	202	93	202	202	131[1]	119	140	196	202	267	H_2 burn at head failure
TMLU-ϵ	---	0	40	---	93	---	15 hr	35[2]	119	140	196	202	267	CS recirculation at 267 min.
$T_1(B_3)$MLUOO'-δ	---	0	---	0	---	0	206	113[3]	120	142	195	201	266	Debris fragmentation in reactor cavity
$T_1(B_3)$MLUOO'-ϵ	---	0	---	0	---	0	15 hr	115[2]	120	142	195	201	266	
TMLOO'-δ	10	---	---	0	---	0	4225	133	4663	4725	4884	4890	4892	Non-melt if steam generator is restored prior to containment failure
V	---	0	---	0	---	0	1	15[4]	62	84	117	132	133	LOCA in auxiliary building
AYF-δ	1	57	---	0	1	57	1100	133	1171	1224	1267	1313	1313	Coolers and CSR fail
AG-δ	1	1514	---	0	1	1514	1514	133	1570	1630	1692	1734	1734	No containment heat removal

* All time is in minutes unless otherwise stated.

(1) Pressure from complete, adiabatic hydrogen burn at head failure

(2) Base pad meltthrough 12 hrs after head failure

(3) Containment failure at pressure peak for rapid vaporization of reactor cavity water

(4) Failure of auxiliary building

Table 5-3. Summary of CORRAL Results, Final Releases

Case	Fission Product Group							Comments
	Xe	I	Cs	Te	Ba	Ru	La	
$T_1(B_3$`MLUOO'-δ	1.0	0.54	0.74	0.64	0.082	0.054	0.0085	Debris fragments(1)
TMLU-γ'	1.0	0.035	0.17	0.58	0.0091	0.035	0.0069	With scrubbing(2)
TMLU-γ	1.0	0.45	0.74	0.70	0.081	0.056	0.0090	No scrubbing(3)
V	1.0	0.48	0.79	0.44	0.092	0.045	0.0063	
AYF-δ	1.0	0.23	0.67	0.46	0.076	0.042	0.0063	
AG-δ	1.0	0.16	0.76	0.71	0.083	0.058	0.0094	
Total source	1.0	1.0	1.0	1.0	0.11	0.08	0.013	Total source and releases for PWR categories 2 and 3 from WASH-1400
PWR2	0.9	0.7	0.5	0.3	0.06	0.02	0.004	
PWR3	0.8	0.2	0.2	0.3	0.02	0.03	0.003	

(1) Containment fails from rapid boiloff of water, in reactor cavity.

(2) Containment fails from hydrogen burn at head failure. Cases show effect of containment spray scrubbing.

(3) Containment fails from hydrogen burn at head failure. Cases show effect of no containment spray scrubbing.

Table 5-4. Oconee (B&W) PWR Key Accident Sequences

Sequence	RELEASE CATEGORY 1	2	3	4	5	6	7
AD	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
AFH	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
AH	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
ACD	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
S_1D	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
S_1FH	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
S_1CD	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
S_1DF	$\alpha=.01$		$\gamma=0.2$	$\beta=.0073$		$\varepsilon=0.8$	
S_1YD	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$	$\delta=0.8$	
S_1H	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
S_2FH	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
S_2D	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
S_2H	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$
S_2CD	$\alpha=.01$	$\gamma=0.2$		$\beta=.0073$		$\varepsilon=0.8$	
S_2YD	$\alpha=.01$		$\gamma=0.2$		$\beta=.0073$	$\delta=0.8$	
S_2DF	$\alpha=.01$		$\gamma=0.2$	$\beta=.0073$		$\varepsilon=0.8$	
S_3H	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
S_3FH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
S_3D	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$

Table 5-4. Oconee (B&W) PWR Key Accident Sequences (cont'd)

Sequence	RELEASE CATEGORY						
	1	2	3	4	5	6	7
S_3CH	α=.0001	γ=0.5		β=.0073		ε=0.5	
S_3CY	α=.01	δ=1		β=.0073			
S_3YD	α=.0001		γ=0.5		β=.0073	δ=0.5	
S_3YH	α=.0001		γ=0.5		β=.0073	δ=0.5	
S_3CD	α=.0001	γ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MLQD$	α=.0001		γ=0.5		β=.0073		ε=0.5
$T_1(B_3)MQD$	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLQH	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLQFH	α=.0001	γ=0.5		β=.0073		ε-0.5	
$T_1(B_3)MLQCYD$	α=.0001	δ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MOCYD$	α=.0001	δ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MLQCD$	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_1MLQD	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLQYD	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MQH	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MQFH	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_1MLQCD	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_1MLQCH	α=.0001	γ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MQCD$	α=.0001	γ=0.5		β=.0073		ε=0.5	

Table 5-4. Oconee (B&W) PWR Key Accident Sequences (cont'd)

Sequence	RELEASE CATEGORY						
	1	2	3	4	5	6	7
$T_1(B_3)MLQDF$	$\alpha=.0001$		$\gamma=0.5$	$\beta=.0073$		$\varepsilon=0.5$	
T_1MQD	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
T_1MQCD	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_1MQCH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MLQYD	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$	$\delta=0.5$	
T_2MQH	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
T_2MLQH	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
T_2MLQFH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MQD	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
T_2MLQD	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$
T_2MLQCD	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MQCD	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MQCH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MLQCH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
$T_2MLQCYD$	$\alpha=.0001$	$\delta=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MQCY	$\alpha=.01$	$\delta=1$		$\beta=.0073$			
T_2MQYD	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$	$\delta=0.5$	
T_2MQFH	$\alpha=.0001$	$\gamma=0.5$		$\beta=.0073$		$\varepsilon=0.5$	
T_2MQYH	$\alpha=.0001$		$\gamma=0.5$		$\beta=.0073$	$\delta=0.5$	

Table 5-4. Oconee (B&W) PWR Key Accident Sequences (cont'd)

Sequence	RELEASE CATEGORY 1	2	3	4	5	6	7
T_2MQDF	α=.0001		γ=0.5	β=.0073		ε=0.5	
T_3MQH	α=.0001		γ=0.5		β=.0073		ε=0.5
T_3MQFH	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_3MLQH	α=.0001		γ=0.5		β=.0073		ε=0.5
T_3MLQYD	α=.0001		γ=0.5		β=.0073		ε=0.5
T_3MQD	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLU	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLUO'	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_1MLUOO'	α=.0001	δ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MLU$	α=.0001		γ=0.5		β=.0073		ε=0.5
$T_1(B_3)MLUOO'$	α=.0001	δ=0.5		β=.0073		ε=0.5	
$T_1(B_3)MLUO'$	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_1MLUO	α=.0001		γ=0.5		β=.0073		ε=0.5
$T_1(B_3)MLUO$	α=.0001		γ=0.5		β=.0073		ε=0.5
T_1MLP_2	α=.0001		γ=0.5		β=.0073		ε=0.5
T_2MLU	α=.0001		γ=0.5		β=.0073		ε=0.5
T_2MLUO'	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_2MLUOO'	α=.0001	δ=0.5		β=.0073		ε=0.5	
T_2MLUO	α=.0001		γ=0.5		β=.0073		ε=0.5
T_2KMU	α=.0001		γ=0.5		β=.0073		ε=0.5

Table 5-4. Oconee (B&W) PWR Key Accident Sequences (cont'd)

	RELEASE CATEGORY						
Sequence	1	2	3	4	5	6	7
T_2MLP_2	α=.01		γ=0.2		β=.0073		ε=0.8
T_3MLU	α=.0001		γ=0.5		β=.0073		ε=0.5
T_3MLUO'	α=.0001	γ=0.5		β=.0073		ε=0.5	
T_3MLUO	α=.0001		γ=0.5		β=.0073		ε=0.5

6.0 RESULTS

Two of the main objectives of this study were to determine which accident sequences are the most significant contributors to the risk associated with the operation of the Oconee plant and to compare the overall risk for this plant with the comparable RSS PWR. The most significant Oconee accident sequences, or "dominant accident sequences," are discussed in detail in Section 6.1. These sequences were derived by considering both the results of the systems analysis task and accident process analysis task presented in Chapters 4 and 5 respectively. The overall risk of the Oconee PWR was indirectly compared with the Surry PWR. This was done by comparing the frequency assessed for the seven PWR core melt release categories. The comparison is presented in Section 6.2. The appropriate conclusions and study limitations are given in Section 6.3.

6.1 Oconee Dominant Accident Sequences

The dominant accident sequences identified for the Oconee plant are given in Figure 6-1. A key to the figure nomenclature is given in Table 6-1.

The solid lines on the histogram represent the release category frequencies. These were found by summing, for each release category, the point estimate frequencies of the dominant accident sequences and less important sequences not presented in the associated matrix of accident sequences vs. release categories. It should be noted that the dominant accident sequences presented in Figure 6-1 represent greater than 90 percent of the total release category frequency for categories 1, 3, 5, and 7, and greater than 80% of categories 2, 4, and 6. The dashed lines represents the release category frequencies after application of the RSS curve smoothing technique; that is, a probability of 0.1 was assigned to an accident sequence being in the adjacent release category, and a probability of 0.01 was assigned to an accident sequence being two release categories from the one in which it was placed, etc. The curve smoothing technique reflects the uncertainty associated with the categorization of each accident sequence. As can be noted from the figure, the effect of curve smoothing dominates the frequency estimates for release categories 1, 4, and 5.

The dominant accident sequences will now be discussed in the order they are displayed in Figure 6-1. Only the most dominant cut sets for each accident sequence are listed. Also, some containment failure modes were not discussed for certain sequences. This was done when sequences were not dominant in a particular category. The systems and cut set terms used to describe the accident sequences are discussed in Appendix B.

Sequence $T_2MLU\ \gamma,\ \beta,\ \varepsilon$:

This sequence is initiated by a loss of the power conversion system (T_2M) followed by failure to restore the power conversion system and failure of the emergency feedwater system (L), and the failure of the high pressure injection system (U). Containment failure is predicted to be one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ε).

This sequence depicts a loss of the systems which provide the normal (T_2M) and emergency (L) means of delivering feedwater to the steam generators. Because of this, secondary decay heat removal via the steam generators would be lost in a short time due to the boil off of their inventory. In order to establish decay heat removal, the operator must open the pressurizer pilot-operated relief valve, actuate the high pressure injection system, and establish a "feed and bleed" core cooling operation. If the operator fails to perform these actions (U), the PCS inventory would boil off through the safety/relief valves leading to uncovering the core and eventual core melt. Babcock and Wilcox predicts the onset of core damage would occur within approximately 40 minutes.[1]

The frequency of this sequence is estimated as:

$$T_2MLU = 1.2 \times 10^{-6}$$

The dominant contributors, or cut sets, to this frequency are listed and described below:

Cut Set	Cut Set Frequency	Description
T_2·M·CONST1·PCSNR·HPMAN	1.1×10^{-6}	T_2M - loss of power conversion system; $F(T_2M) = 3/R\text{-yr}$
		CONST1 - failure of emergency feedwater system due to primarily hardware failure of the turbine pump train and both of the electric pump trains; $P(CONST1) = 2.4 \times 10^{-4}$

---

[1]It should be noted that the time to core damage, predicted by B&W and Battelle Columbus Laboratories, differs. Battelle predicts 73 minutes (see Appendix C, Section 3.0). Since the B&W computer codes model primary system response more accurately than the MARCH code, the 40-minute estimate was used for the assessment of recovery probabilities.

Cut Set	Cut Set Frequency	Description
		PCSNR - failure to restore the power conversion system; P(PCSNR) = .1
		HPMAN - operator fails to start the high pressure injection system; P(HPMAN) = 1.5×10^{-2}

The containment failure mode probabilities and release category placement were assessed as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\epsilon) = 0.5$; category 7

Multiplying the sequence frequency by the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_1MLU γ, β, ϵ:

This sequence is initiated by a loss of offsite power (T_1M), followed by the failure to restore the power conversion system (offsite power must be restored) and, failure of the emergency feedwater system (L), and the failure of the high pressure injection system (U). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is similar to the T_2MLU transient discussed above. However, since the initiating event is a loss of offsite power (T_1), the unavailability of the emergency feedwater system is increased about a factor of three. This is because the turbine pump train will most likely fail, since a critical valve which must open to allow cooling water to the pump is load shed following a T_1. In order to open this valve, it must be loaded on an emergency bus by the operator. However, since there is no valve position indication or cooling water flow indication, success of the turbine pump was deemed to be highly unlikely.

The frequency of this sequence is estimated as:

$$T_1MLU = 2.0 \times 10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$T_1 \cdot M_1 \cdot$CONST2$\cdot$ HPMAN	2.0×10^{-6}	T_1M - loss of offsite power; $F(T_1M)$ = 0.2/R-yr CONST2 - failure of the emergency feedwater system due to failure of both electric pump trains; P(CONST2) = 6.5×10^{-4} HPMAN - operator fails to start the high pressure injection system; P(HPMAN) = 1.5×10^{-2}

The containment failure mode probabilities and release category placements were assessed to be:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\varepsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probaiblities results in the values presented in Figure 6-1.

Sequence V:

This sequence represents failure of the Low Pressure Injection System check valves when the normally closed isolation MOV is opened for quarterly tests.

The primary coolant system operates at high pressures and consists of piping designed to withstand these pressures. There are systems which connect to the primary coolant system which may possess low pressure piping passing outside of containment, thus offering the potential for a loss of coolant accident outside the containment and concurrent damage to systems needed to cope with this accident. These are discussed in some detail in Appendix A3.

One such system identified is the low pressure injection system. This sequence assumes failure of a series of two check valves in one of the low pressure injection system lines and the opening of the normally-closed isolation MOV, which is also in series with the check valves, for quarterly MOV testing. This would allow high pressure coolant water to enter the low pressure piping outside containment and pipe rupture to occur. The containment engineered safety features would be ineffective for this accident, and the low pressure injection system would also fail due to the LOCA. As a result, core melt would occur.

Since failure of these valves would lead to a LOCA outside containment, the status of the containment is a relatively moot question. The consequences of this sequence correspond to those of release category PWR 2 according to the accident process analysis task. The probability of this sequence is the probability of failure of the two series check valves and the opening of the isolation MOV for quarterly tests. It should be noted that no provision exists to monitor the status of the check valves before the MOV is opened. Event V is discussed in Appendix A3 and has a frequency of:

$$V = 7.4 \times 10^{-5}.$$

The probability of occurrence for this accident is dominated by the failure mode caused by both check valves failing to reseat after a cold shutdown flow test of the low pressure injection system. This failure mode comprises 94% of the sequence V probability.[1]

Sequence $T_1(B_3)MLU\ \gamma,\ \beta,\ \epsilon$:

This sequence is initiated by a loss of offsite power (T_1M), followed by the failure of the emergency AC hydroelectric generators (B_3), followed by the failure to restore the power conversion system (offsite power must be restored) and failure of the emergency feedwater and high head auxiliary feedwater systems (L), and the failure of the high pressure injection system (U). Containment failure is predicted by overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is also similar to the T_2MLU transient discussed previously. In this case, however, a loss of both the normal and emergency AC power sources (i.e., station blackout) is assumed to occur ($T_1(B_3)$). Since the turbine driven emergency feedwater system pumps require cooling from the AC dependent low pressure service

[1] It has been recently learned that the normally closed isolation MOV is no longer opened when the plant is at power. This is an interim solution to reduce the sequence V frequency. The plant will eventually install a pressure gauge downstream of the MOV which will be checked prior to opening the MOV when at power. It is expected that these design changes will cause the Event V frequency to decrease to approximately that of the Surry plant, if not lower. Therefore, in Figure 6-1, the value used for Event V was the Surry value, namely, 4.0×10^{-6}.

water system, it will fail in a short time. The operator still has the option, however, of initiating steam generator cooling via the high head auxiliary service water system since it has its own power system. In order to utilize the high pressure injection system in the "feed and bleed" core cooling mode, either onsite or offsite AC power must be restored.

The frequency of this sequence is estimated as

$$T_1(B_3)MLU = 2.2 \times 10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$T_1 \cdot (B_3) \cdot M \cdot HHMAN \cdot LOPNRE$	2×10^{-6}	T_1M - loss of offsite power; $F(T_1M) = 0.2/R\text{-yr}$
		(B_3) - failure of both emergency AC hydroelectric generators; $P((B_3)) = 5 \times 10^{-4}$
		HHMAN - operator fails to manually start the high head auxiliarly service water system; $P(HHMAN) = 0.1$
		LOPNRE - offsite or onsite AC power is not restored within approximately 40 minutes. This power is required to operate the high pressure injection system; $P(LOPNRE) = 0.2$
$T_1 \cdot (B_3) \cdot M \cdot HHMAN \cdot HPMAN$	1.5×10^{-7}	T_1, (B_3), M, HHMAN (defined above)
		HPMAN - operator fails to start the high pressure injection system given that AC power is restored; $P(HPMAN) = .015$

The containment failure mode probabilities and release category placement were assessed to be:

$P(\gamma) = 0.5$	;	category 3
$P(\beta) = 0.0073$	;	category 5
$P(\varepsilon) = 0.5$	;	category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_2MQ-H γ, β, ε:

This sequence is initiated by a loss of the power conversion system (T_2M) followed by failure of one pressurizer safety/relief valve to reclose (Q), and failure of the emergency coolant recirculation system (H). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ε).

This sequence is a transient induced LOCA (T_2MQ) in which the emergency core cooling system fails during the recirculation phase (H).

It is assumed in this sequence that the emergency feedwater system is successful or the PCS is restored, but their initiation is delayed. This delay would cause the RCS pressure to rise causing a demand of the pressurizer safety/relief valves. Failure of one of these valves to reclose would constitute a small-small LOCA. This sequence assumes that the LOCA systems perform successfully during the injection phase (i.e., water source is borated water storage tank) but the emergency coolant recirculation system (ECRS) fails during the recirculation phase (i.e., water source is containment sump). For a small-small LOCA, the ECRS is composed of the high pressure recirculation system taking suction from the discharge of the low pressure recirculation system. This alignment is performed by the operator in the control room.

The frequency of this sequence is estimated as:

$$T_2MQ\text{-}H = 1.1 \times 10^{-5}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot HPRSCM$	4.5×10^{-6}	T_2M - loss of power conversion system; $F(T_2M) = 3/R\text{-yr}$
		$\overline{P}_1$ - pressurizer safety/relief valves demanded open; $P(\overline{P}_1) = 0.01$
		Q - failure of any pressurizer safety/relief valve to reclose; $P(Q) = 0.05$
		HPRSCM - failure of operator to align suction of high pressure recirculation system to the discharge of low pressure recirculation system; $P(HRPSCM) = 3 \times 10^{-3}$
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot LPISCM$	4.5×10^{-6}	T_2, M, $\overline{P}_1$, Q (discussed above)
		LPISCM - failure of low pressure recirculation system due to test valves left in wrong position; $P(LPISCM) = 3 \times 10^{-3}$
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot D \cdot E$	7.4×10^{-7}	T_2, M, $\overline{P}_1$, Q (discussed above)
		D·E - failure of both low pressure pump trains A and B $P(E \cdot D) = 4.9 \times 10^{-4}$ (double maintenance removed)

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot E \cdot W$	3.2×10^{-7}	T_2, M, $\overline{P}_1$, Q (discussed above) E·W - failure of low pressure train B and sump suction valves for low pressure train A; $P(E \cdot W) = 2.1 \times 10^{-4}$ (double maintenance removed)
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot D \cdot X$	3.2×10^{-7}	T_2, M, $\overline{P}_1$, Q (discussed above) D·X - failure of low pressure train A and sump suction valves for low pressure train B; $P(D \cdot X) = 2.1 \times 10^{-4}$ (double maintenance removed)

The containment failure mode probabilities and release category placement were as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\varepsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence S_3H γ, β, ε:

This sequence is initiated by a rupture in the RCS piping in the range $0<D\leq4"$ (S_3) followed by failure of the emergency coolant recirculation system (H). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ε).

This sequence is similar to the T_2MQ-H sequence discussed earlier. However in this case, the small-small LOCA is caused by a random rupture in the RCS piping rather than by a stuck open pressurizer safety/relief valve. The systems responding to both types of LOCAs are identical and the dominant failure contributors of the emergency coolant recirculation system are also identical.

The frequency of this sequence is estimated as:

$$S_3H = 1.0 \times 10^{-5}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$S_3 \cdot HPRSCM$	3.9×10^{-6}	S_3 - rupture of RCS piping, $0 < D \leq 4"$ $F(S_3) = 1.3 \times 10^{-3}$/Ryr HPRSCM - (described previously)
$S_3 \cdot LPISCM$	3.9×10^{-6}	S_3, LPISCM - (described previously)
$S_3 \cdot D \cdot E$	6.4×10^{-7}	S_3, $D \cdot E$ - (described previously)
$S_3 \cdot E \cdot W$	2.7×10^{-7}	S_3, $E \cdot W$ - (described previously)
$S_3 \cdot D \cdot X$	2.7×10^{-7}	S_3, $D \cdot X$ - (described previously)

The containment failure mode probabilities and release category placement were as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\varepsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence S_1D α, γ, β, ε:

This sequence is initiated by a rupture in the RCS piping in the range $10" < D \leq 13.5"$ (S_1), followed by failure of the emergency coolant injection system (D). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence assumes an intermediate size LOCA occurs followed by failure of the emergency core cooling system during the injection phase. Containment systems would operate as designed to control containment pressure and to remove radioactivity from the atmosphere, but failure of the core cooling system would lead to boil off of the water covering the core resulting in core melt.

The equipment required for core cooling for this size break is given in the FSAR as one of three high pressure injection system pump trains and two of the low pressure injection system pump trains.[1] The requirement of both low pressure trains implies that any single failure in the low pressure injection system will fail the emergency coolant injection system. Single failures, therefore, dominate the accident sequence cut sets.

The frequency of this sequence is estimated as:

$$S_1D = 6.7 \times 10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$S_1 \cdot D$	2.3×10^{-6}	S_1 - rupture of RCS piping, $10" < D \leq 13.5"$; $F(S_1) = 1 \times 10^{-4}$/Ryr
		D - failure of pump Train A discharge valves; $P(D) = 2.3 \times 10^{-2}$.

[1] Based on recent discussions with Duke Power, the FSAR criteria used for this break size range was found to be conservative. The more realistic criteria requires 2/2 CFT and one low pressure pump. Utilizing this criteria would significantly reduce the frequency of this sequence.

Cut Set	Cut Set Frequency	Description
$S_1 \cdot E$	2.3×10^{-6}	E - failure of pump Train B discharge valves; $P(E) = 2.3 \times 10^{-2}$
$S_1 \cdot CH3$	5×10^{-7}	CH3 - failure of pump Train A actuation channel; $P(CH3) = 5 \times 10^{-3}$
$S_1 \cdot CH4$	5×10^{-7}	CH4 - failure of pump Train B actuation channel; $P(CH4) = 5 \times 10^{-3}$
$S_1 \cdot C$	3.3×10^{-7}	C - failure of pump Train A suction valves; $P(C) = 3.3 \times 10^{-3}$
$S_1 \cdot B$	3.3×10^{-7}	B - failure of pump Train B suction valves; $P(B) = 3.3 \times 10^{-3}$
$S_1 \cdot LPISCM$	3×10^{-7}	LPISCM - failure to reclose low pressure pump train test valves; $P(LPISCM) = 3 \times 10^{-3}$

The containment failure mode probabilities and release category placement were as follows:

$P(\alpha) = 0.01$; category 1

$P(\gamma) = 0.2$; category 3

$P(\beta) = 0.0073$; category 5

$P(\epsilon) = 0.8$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_2MQ-FH γ, β, ϵ:

This sequence is initiated by a loss of the power conversion system (T_2M), failure of one pressurizer safety/relief valve to reclose (Q), failure of the containment spray recirculation system (F), and failure of the emergency coolant recirculation system (H). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is a transient induced LOCA (T_2MQ). As described earlier in the T_2MQ-H sequence, the LOCA is created due to a failure of a pressurizer relief valve to reclose after being demanded. The demand of the valve is assumed to occur due to a delay in the initation of the emergency feedwater and/or restoration of the power conversion system. In this sequence, the LOCA systems perform successfully during the injection phase, but the emergency core cooling system and containment spray system fail during the recirculation phase.

The frequency of this sequence is estimated as:

$$T_2MQ\text{-}FH = 5.0 \times 10^{-6}$$

The main contributor to this occurrence is due to a failure of the operator to correctly follow emergency procedures which instruct him to open both sump MOV's which are common to both the core cooling and spray systems when the borated water storage tank reaches 94% empty. This cut set, along with other contributors, are listed below:

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot WXCM$	4.5×10^{-6}	T_2M - loss of power conversion system; $F(T_2M) = 3/R\text{-yr}$
		$\overline{P}_1$ - pressurizer safety/relief valves demanded open $P(\overline{P}_1)$ 0.01
		Q - failure of any safety/relief valves to reclose; $P(Q) = 0.05$

Cut Set	Cut Set Frequency	Description
		WXCM - failure of the operator to open the sump valves at the start of recirculation which are common to both the spray and core cooling system; $P(WXCM) = 3 \times 10^{-3}$
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot B \cdot W$	4.1×10^{-8}	T_2, M, $\overline{P}_1$, Q (discussed above) $B \cdot W$ - failure of the low pressure/containment spray injection Train B tank suction valves and low pressure/containment spray recirculation Train A sump suction valves; $P(B \cdot W) = 2.7 \times 10^{-5}$ (double maintenance removed)
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot C \cdot X$	4.1×10^{-8}	T_2, M, $\overline{P}_1$, Q (discussed above) $C \cdot X$ - failure of the low pressure/containment spray injection Train A tank suction valves and low pressure/containment spray recirculation Train B sump suction valves; $P(C \cdot X) = 2.7 \times 10^{-5}$ (double maintenance removed)
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot W \cdot X$	1.3×10^{-7}	T_2, M, $\overline{P}_1$, Q (discussed above) $W \cdot X$ - failure of both low pressure/containment spray recirculation sump suction valves; $P(W \cdot X) = 8.8 \times 10^{-5}$ (double maintenance removed).

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$; category 2

$P(\beta) = 0.0073$; category 4

$P(\varepsilon) = 0.5$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence $S_3FH\ \gamma,\ \beta,\ \varepsilon$:

This sequence is initiated by a rupture in the RCS piping in the range $0<D\leq4"$ (S_3), followed by failure of the containment spray recirculation system (F), and emergency coolant recirculation system (H). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ε).

This sequence is initiated by a random rupture of the RCS piping. In this sequence, the LOCA systems perform successfully during injection phase, but the emergency core cooling system and containment spray system fail during the recirculation phase.

The frequency of this sequence is estimated as:

$$S_3FH = 4.2 \times 10^{-6}$$

The main contributor to this occurrence is due to a failure of the operator to correctly follow emergency procedures which instruct him to open both sump MOV's which are common to both the core cooling and spray systems when the borated water storage tank reaches 94% empty. This cut set, along with other contributors, are listed below:

Cut Set	Cut Set Frequency	Description
S_3·WXCM	3.9×10^{-6}	S_3 - rupture of RCS piping, $0 < D \leq 4"$. $F(S_3) = 1.3 \times 10^{-3}$/R yr. WXCM - failure of the operator to open the sump valves at the start of recirculation which are common to both the spray and core cooling systems; $P(WXCM) = 3 \times 10^{-3}$
S_3·W·X	1.1×10^{-7}	S_3 (discussed above).

Cut Set	Cut Set Frequency	Description
		W·X - failure of both low pressure/ containment spray recirculation sump suction valves; $P(W \cdot X) = 8.8 \times 10^{-5}$ (double maintenance removed).
$S_3 \cdot B \cdot W$	3.5×10^{-8}	S_3 - (discussed above)
		B·W - failure of the low pressure/containment spray injection Train B tank suction valves and low pressure/containment spray recirculation Train A sump suction valves; $P(B \cdot W) = 2.7 \times 10^{-5}$ (double maintenance removed).
$S_3 \cdot C \cdot X$	3.5×10^{-8}	S_3 - (discussed above)
		C·X - failure of the low pressure/containment spray injection Train A tank suction valves and low pressure/containment spray recirculation Train B sump suction valves; $P(C \cdot X) = 2.7 \times 10^{-5}$ (double maintenance removed).

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$; category 2

$P(\beta) = 0.0073$; category 4

$P(\varepsilon) = 0.5$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence S_2FH α, β, ε:

This sequence is initiated by a rupture in the RCS piping in the range $4" < D \leq 10"$ (S_2), followed by failure of the containment spray recirculation system (F), and emergency coolant recirculation system (H). Containment failure is predicted by one of the following: vessel steam explosion (α), penetration leakage (β), or base mat melt through (ε).

This sequence is similar to the S_3FH sequence discussed previously. The only difference is that for this size LOCA, different combinations of emergency core cooling subsystems are required. This, however, does not affect the dominant cut sets of the sequence frequency.

The frequency is estimated as:

$$S_2FH = 1.3 \times 10^{-6}$$

Cut Set	Cut Set Frequency	Description
$S_2 \cdot WXCM$	1.2×10^{-6}	S_2 - rupture of RCS piping, 4"<D≤10"; $F(S_2) = 4 \times 10^{-4}$
$S_2 \cdot X \cdot W$	3.5×10^{-8}	(WXCM, X·W, B·W, and C·X terms discussed in sequence S_3FH description)
$S_2 \cdot B \cdot W$	1.1×10^{-8}	
$S_2 \cdot C \cdot X$	1.1×10^{-8}	

The dominant containment failure mode probabilities and release category placements were as follows:

$P(\alpha) = 0.01$; category 1

$P(\beta) = 0.0073$; category 4

$P(\varepsilon) = 0.8$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_2MLUO γ, β, ε:

This sequence is initiated by a loss of the power conversion system (T_2M), followed by the failure to restore the power conversion system and failure of the emergency feedwater system (L), failure of the high pressure injection system (U), and failure of the reactor building cooling system (O). Containment failure is predicted by overpressure due to hydrogen burning (γ), penetration leakage (β) or base mat melt through (ε).

This sequence is similar to the T_2MLU sequence discussed at the beginning of this section, except in this case, the reactor building cooling system also fails.

The frequency of this sequence is estimated to be:

$$T_2MLUO = 8.1 \times 10^{-6}$$

The dominant cut sets are quite different from the T_2MLU sequence, however, due to the dependence of the systems which comprise events L, U, and O, on the low pressure service water system. These cut sets are:

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot PCSNR \cdot F1 \cdot G1$	6.0×10^{-6}	T_2M - loss of power conversion system; $F(T_2M) = 3/R\text{-yr}$.
		PCSNR - failure to restore the power conversion system; $P(PCSNR) = .1$
		$F1 \cdot G1$ - failure of both low pressure service water pump trains. They supply cooling water to the reactor building cooling system heat exchangers, high pressure injection system pumps and emergency feedwater system pumps; $P(F1 \cdot G1) = 2.0 \times 10^{-5}$

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot PCSNR \cdot F1 \cdot CH4$	2.1×10^{-6}	T_2, M, PCSNR (discussed above) $F1 \cdot CH4$ - failure of both low pressure service water pump trains. One fails to continue operation (F1) and the other fails to start due to faults in the actuation circuit (CH4); $P(F1 \cdot CH4) = 7 \times 10^{-6}$

The containment failure mode probabilities and release category placements were assessed as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = .0073$; category 5

$P(\varepsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_2MKU γ, β, ε:

This sequence is initiated by a loss of the power conversion system (T_2M) followed by failure of the reactor protection system (K), and the failure of the high pressure injection system (U). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β) or base mat melt through (ε).

This sequence is of the type known as Anticipated Transients Without Scram (ATWS). This type of transient for B&W reactors has been studied in depth (NUREG-0460). This report states that if a loss of main feedwater is followed by a failure to scram (reactor protection system failure), RCS peak pressures in the 4000-5000 psi range may result. It is unknown what effect this peak pressure would have on RCS integrity and components. The sequence modeled here does not address this unknown. It is assumed that the RCS would survive the peak pressure.

Following the pressure pulse, the reactor would most likely equilibrate at a power level which matches the heat removal capacity of the emergency feedwater system. In some situations it may equilibrate at a higher level. (This is due to competing effects of a negative temperature reactivity coefficient and a positive Doppler coefficient. For more details see Appendix C.) For these situations the high pressure injection system must be actuated by the operator to inject borated water (i.e., negative reactivity) to successfully shut down the reactor. This sequence assumes that the high pressure injection fails followed by an eventual core melt.

The frequency of this sequence is estimated as:

$$T_2KMU = 7.8 \times 10^{-6} \quad .$$

The dominant cut set is:

Cut Set	Cut Set Frequency	Description
T_2·K·M·HPMAN	7.8×10^{-6}	T_2M - loss of power conversion system; $P(T_2M) = 3/R\text{-yr}$
		K - failure of the reactor protection system due to primarily test and maintenance faults; $P(K) = 2.6 \times 10^{-5}$
		[1]HPMAN - operator fails to start the high pressure injection system; P(HPMAN) = 0.1

[1]The probability of HPMAN for ATWS sequences was assigned a value of 0.1 rather than the value of 0.015 used in other sequences to reflect an extremely high stress situation.

The containment failure mode probabilities and release category placements were assessed as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; categoi. 5

$P(\epsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

<u>Sequence S_2D α, γ, β, ϵ</u>:

This sequence is initiated by a rupture in the RCS piping in the range $4" < D \leq 10"$ (S_2), followed by failure of the emergency coolant injection system (D). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is similar to the S_1D sequence discussed previously except that a different combination of ECCS subsystems must fail to cause a core melt. The equipment required for this size LOCA are defined in the FSAR as one high pressure injection pump train and one low pressure injection pump train.

The frequency of this sequence is estimated as:

$$S_2D = 2.0 \times 10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
S_2·LPISCM	1.2×10^{-6}	S_2 - rupture of RCS piping, $4" < D < 10"$, $P(S_2) = 4 \times 10^{-4}$/R yr

Cut Set	Cut Set Frequency	Description
		LPISCM - failure to reclose low pressure pump train test valves; P(LPISCM) = 3×10^{-3}
$S_2 \cdot C1 \cdot B1$	1.4×10^{-7}	C1·B1, A1·B1, CH1·B1 -
$S_2 \cdot A1 \cdot B1$ $S_2 \cdot CH1 \cdot B1$	1.4×10^{-7} 7.2×10^{-8}	Double hardware and/or human failures in the high pressure injection system P(C1·B1) = 3.4×10^{-4} P(A1·B1) = 3.4×10^{-4} P(CH1·B1) = 1.8×10^{-4}
$S_2 \cdot E \cdot D$ $S_2 \cdot B \cdot D$ $S_2 \cdot E \cdot C$ $S_2 \cdot E \cdot CH3$	2.0×10^{-7} 2.5×10^{-8} 2.5×10^{-8} 4.8×10^{-8}	E·D, B·D, E·C, E·CH3, CH4·D - Double hardware and/or human failures in the low pressure injection system
$S_2 \cdot CH4 \cdot D$	4.8×10^{-8}	P(E·D) = 4.9×10^{-4} P(B·D) = 6.3×10^{-5} P(E·C) = 6.3×10^{-5} P(E·CH3) = 1.2×10^{-4} P(CH4·D) = 1.2×10^{-4} (double maintenance removed)

The containment failure mode probabilities and release category placements were as follows:

$P(\alpha) = 0.01$; category 1

$P(\gamma) = 0.2$; category 3

$P(\beta) = 0.0073$; category 5

$P(\varepsilon) = 0.8$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence $S_3D\ \gamma, \beta, \varepsilon$:

This sequence is initiated by a rupture in the RCS piping in the range $0" < D \leq 4"$ (S_1), followed by failure of the emergency coolant injection system (D). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is similar to the S_1D sequence discussed earlier except that a different combination of ECCS subsystems must fail to cause a core melt. The equipment required for injection for this size LOCA is defined in the FSAR as one high pressure pump train.

The frequency of this sequence is estimated as:

$$S_3D = 1.4 \times 10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	Description
$S_3 \cdot C1 \cdot B1$ $S_3 \cdot A1 \cdot B1$ $S_3 \cdot CH1 \cdot B1$	4.4×10^{-7} 4.4×10^{-7} 2.3×10^{-7}	S_3 - rupture of RCS piping, D<4". $F(S_3) = 1.3 \times 10^{-3}$/R-yr.
$S_3 \cdot C1 \cdot CH2$ $S_3 \cdot A1 \cdot CH2$ $S_3 \cdot CH1 \cdot CH2$	6.4×10^{-8} 6.4×10^{-8} 3.3×10^{-8}	C1·B1, A1·B1, CH1·B1, C1·CH2, A1·CH2, CH1·CH2 - double hardware and/or human failures in the high pressure injection system $P(CH \cdot B1) = 3.4 \times 10^{-4}$ $P(A1 \cdot B1) = 3.4 \times 10^{-4}$ $P(CH1 \cdot B1) = 1.8 \times 10^{-4}$ $P(C1 \cdot CH2) = 4.9 \times 10^{-5}$ $P(A1 \cdot CH2) = 4.9 \times 10^{-5}$ $P(CH1 \cdot CH2) = 2.5 \times 10^{-5}$
$S_3 \cdot RCSRBCM$	4.2×10^{-8}	RCSRBCM - Common mode miscalibration of the sensor/bistables which actuate the HPIS. The sensor groups are the RCS low pressure and Reactor Building Hi pressure. $R(RCSRBCM) = 3.2 \times 10^{-5}$

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$: category 3

$P(\beta) = 0.0073$: category 5

$P(\varepsilon) = 0.5$: category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_1MLUO γ, β, ε:

This sequence is initiated by a loss of offsite power (T_1M), followed by the failure to restore the power conversion system (offsite power must be restored) and failure of the emergency feedwater system (L), failure of the high pressure injection system (U), and failure of the reactor building cooling system (O). Containment failure is predicted by overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ε).

This sequence is identical to the T_2MLUO sequence discussed earlier except that the initiating event is a loss of offsite power. The cut sets are also identical. The probability of failing to restore the power conversion system is approximately unity for this sequence as opposed to 10^{-1} for the T_2MLUO sequence.

The frequency of this sequence is estimated to be:

$$T_1\text{MLUO} = 5.4 \times 10^{-6}$$

The dominant cut sets are:

Cut Set	Cut Set Frequency	Description
$T_1 \cdot M \cdot F1 \cdot C1$	4.0×10^{-6}	T_1 - Loss of offsite power; $F(T_1)$ = .2/reactor-year.

Cut Set	Cut Set Frequency	Description
		M - Interruption of the PCS; $P(M) = 1.0$
$T_1 \cdot M \cdot F1 \cdot CH4$	1.4×10^{-6}	(Terms $F1 \cdot G1$ and $F1 \cdot CH4$ are described in T_2MLUO sequence)

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\epsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence $T_3MLUO\ \gamma,\ \beta,\ \epsilon$:

This sequence is initiated by a reactor trip with the power conversion system initially available (T_3), followed by the failure of the power conversion system (M), failure of the emergency feedwater system (L), failure of the high pressure injection system (U), and failure of the reactor building cooling system (O). Containment failure is predicted by overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is similar to the T_2MLUO sequence discussed earlier except that the initiating event is a reactor trip with the power conversion system initially available. In the T_2MLUO sequence, the PCS is interrupted and must be recovered. Nonrecovery of the PCS is represented by the term PCSNR and is assessed to be .1. For the T_3MLUO sequence, the PCS is initially available. Event M represents interruption of the PCS and is given a value of .01 for this sequence.

The frequency of this sequence is estimated to be:

$$T_3MLUO = 1.1 \times 10^{-6}$$

The dominant cut sets are:

Cut Set	Cut Set Frequency	Description
$T_3 \cdot M \cdot F1 \cdot G1$	8.0×10^{-7}	T_3 - Transients requiring shutdown with the PCS initially available; $F(T_3)$ = 4/reactor-year. M - Interruption of the PCS; P(M) = .01. (Terms F1·G1 and F1·CH4 are discussed in sequence T_2MLUO description)
$T_3 \cdot M \cdot F1 \cdot CH4$	2.8×10^{-7}	

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\varepsilon) = 0.05$; category 7

Multiplying the sequence frequencies with the containment failure mode probabilities results in the values presented in Figure 6-1.

Sequence T_2MQ-D γ, β, ε:

This sequence is initiated by a loss of the power conversion system (T_2M) followed by failure of one pressurizer safety/relief valve to reclose (Q), and failure of the emergency coolant injection system (D). Containment failure is predicted by one of the following: containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt through (ϵ).

This sequence is a transient induced LOCA (T_2MQ) in which the emergency core cooling system fails during the injection phase (D).

It is assumed in this sequence that the emergency feedwater system is successful or the PCS is restored by their initiation is delayed. This delay would cause the RCS pressure to rise causing a demand of the pressurizer safety/relief valves. Failure of one of these valves to reclose would constitute a small-small LOCA. The high pressure injection system which is called upon to provide emergency core cooling in response to the LOCA also fails.

The frequency of this sequence is estimated as:

$$T_2MQ\text{-}D = 1.5 \times 10^{-6}$$

The dominant cut sets are identical to those previously described in the S_3D sequence. The only difference is that this sequence is a transient induced LOCA rather than a pipe rupture.

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot C1 \cdot B1$	5.1×10^{-7}	T_2M - loss of power conversion system $F(T_2M) = 3/R$ yr $\overline{P}_1$ - pressurizer safety/relief valves demanded open; $P(\overline{P}_1) = 0.01$ Q - failure of one pressurizer safety/relief valve to reclose; $P(Q) = 0.05$ $C1 \cdot B1$ (described in S_3D sequence)
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot A1 \cdot B1$	5.1×10^{-7}	(The rest of the cut set terms are described in S_3D sequence)

Cut Set	Cut Set Frequency	Description
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot CH1 \cdot B1$	2.7×10^{-7}	
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot C1 \cdot CH2$	7.4×10^{-8}	
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot A1 \cdot CH2$	7.4×10^{-8}	
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot CH1 \cdot CH2$	3.8×10^{-8}	
$T_2 \cdot M \cdot \overline{P}_1 \cdot Q \cdot RCSRBCM$	4.8×10^{-8}	

The containment failure mode probabilities and release category placements were as follows:

$P(\gamma) = 0.5$; category 3

$P(\beta) = 0.0073$; category 5

$P(\epsilon) = 0.5$; category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 6-1.

6.2 Comparison With the Dominant Accident Sequences in the Reactor Safety Study

The Surry sequences which dominated the seven PWR core melt release categories in the RSS are presented in Figure 6-2. A short description of these are presented below:

TMLB'-δ, γ, ϵ: failure of the feedwater delivery system (power conversion (M) and auxiliary feedwater systems (L) given the initiating transient event of loss of offsite AC power (T) with failure to recover either onsite or offsite AC power within about 3 hours, preventing containment ESF mitigation of accident (B') consequences. Containment failure due to overpressure, hydrogen burning, or melt through.

V: interfacing systems LOCA due to failure of the LPIS check valves.

S_2C-δ: failure of the containment spray injection system (C) given a small LOCA (S_2) (1/2" $\leq$ D $\leq$ 2"). Containment failure due to overpressure.

AD-ϵ: failure of the emergency coolant injection system (D) given a large LOCA (A) (D≥6"). Containment failure due to melt through.

AH-ϵ: failure of the emergency coolant recirculation system (H) given a large LOCA (A) (D≥6"). Containment failure due to melt through.

S_1D-ϵ: failure of the emergency coolant injection system (D) given a small LOCA (2"<D≤6"). Containment failure due to melt through.

S_1H-ϵ: failure of the emergency coolant recirculation system (H) given a small LOCA (2"<D≤6"). Containment failure due to melt through.

S_2D-ϵ: failure of the emergency coolant injection system (D) given a small LOCA (1/2"<D≤2"). Containment failure due to melt through.

S_2H-ϵ: failure of the emergency coolant recirculation system (H) given a small LOCA (1/2"<D≤2"). Containment failure due to melt through.

TML-ϵ: failure of the feedwater delivery system (power conversion (M) and auxiliary feedwater (L)) given a transient initiating event (T). Containment failure due to melt through.

TKQ-ϵ: failure of the reactor protection system (K) to shutdown the reactor and failure of at least one pressurizer safety/relief valve to reclose (Q) given a transient initiating event (T). Containment failure due to melt through.

TKMQ-ϵ: failure of the reactor protection system (K) to shutdown the reactor; failure of power conversion system (M) and failure of at least one pressurizer safety/relief valve to reclose (Q) given a transient initiating event (T). Containment failure due to melt through.

These Surry sequences dominate the seven PWR release categories after applying the RSS curve smoothing technique. They should be compared with the Oconee sequences placed in categories 2, 3, 6 and 7, since they also dominate the seven release categories after application of curve smoothing.

The equivalent of the Surry TMLB' is the Oconee $T_1(B_3)$MLUOO'. The core melt frequency of the Oconee sequence is about two orders of magnitude lower. This is due primarily to the increased availability of emergency AC power at Oconee.

The V sequence is important at both plants. The Oconee sequence was estimated to have more than an order of magnitude greater frequency due primarily to the closed MOV upstream of the isolation of check valves.[1] This closed valve required the dominant failure mode, caused by failure of both valves to reseat, to be included in the frequency calculation. The equivalent Surry MOV was in the open position.

The Surry TML and the equivalent Oconee sequences T_1MLU, T_2MLU, and $T_1(B_3)$MLU, T_1MLUO, T_2MLUO, and T_3MLUO, are also important at both plants. The Oconee sequences have a total frequency estimate which is a factor of three higher than the comparable Surry sequences. The reason for the higher frequency estimate for Oconee is primarily due to a common mode failure of the systems defined by events L, U, and O. These systems require low pressure service water for component cooling and will fail if cooling is not provided. The similar Surry systems do not have a comparable common mode failure.

Several LOCA sequences which involved failure of the emergency core cooling system, either during the injection or recirculation phases, were important at Surry (e.g., AD, AH, S_1H, S_2D and S_2H). These LOCAs were caused by a random rupture of the RCS piping. Several LOCA sequences were also important at Oconee. At Oconee, however, these LOCAs were due to random RCS ruptures, as well as

---

[1]It has been recently learned that Duke Power has introduced changes which significantly reduce the frequency of this sequence. Refer to discussion of Sequence V in Section 6.1.

stuck open valves (i.e., transient induced LOCAs). In the RSS, transient induced LOCAs were conservatively assumed to lead to core melt and were not analyzed in detail. The overall core melt frequency, due to LOCAs, (other than the V LOCA) is similar for both plants. If one sums the Oconee random and transient induced LOCA sequence frequencies given in Tables 4-9 and 4-10 of Chapter 4, and compares the sum of the Surry LOCA sequences, it can be noted that there is less than a factor of two difference in the totals.

LOCA sequences involving failure of the CSRS (Event F) and the ECRS (Event H) were important at Oconee, but not at Surry. At Oconee, the failure of both systems is dominated by the common mode failure of the operator to realign both systems from the injection to recirculation mode. This common mode failure does not exist at Surry since the operator must manually realign only the ECRS. At Surry, the CSRS is automatically initiated.

Another important core melt sequence at Surry was S_2C. 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 and core melting will eventually occur. Due to the presence of the Oconee reactor building cooling system, which performs a redundant containment overpressure protection function to the containment spray injection system, the S_2C sequence does not result in core melt. The equivalent core melt sequence at Oconee would be S_3CY. This sequence is not as significant a risk contributor for the Oconee plant as the equivalent Surry sequence due to its much lower sequence probability.

At Surry, sequences where there is failure to achieve reactor shutdown accompanied with a stuck open pressurizer relief valve (TKQ and TKMQ), were assessed to be core melts. As mentioned previously, transient induced LOCAs, such as these, were not analyzed in detail in the RSS and were conservatively assumed to lead to core melt. More detailed research conducted during this study indicated that these sequences do not lead to core melt at Oconee. A reanalysis of the Surry TKQ and TKMQ sequence would most likely indicate that these sequences are also non core melts.

6.3 Conclusions and Limitations

6.3.1 Conclusions

Several insights can be gained by comparing the Surry and Oconee plants:

- Details in such items as operating procedures and systems valve status can be very important to the risk associated with a plant. This is evident upon comparing the frequency estimate of the interfacing system LOCA, event V, for both plants. The only significant design difference is that a motor operated valve is normally closed at Oconee, whereas the equivalent valve at Surry is normally open.
- Several plant systems and design features which are important to the public risk are different for the Oconee PWR and the Surry PWR. However, there do exist plant systems, even though design details may differ, which are important to public risk for both PWR plants.
- The methods used for determining public risk in the RSS are equally applicable to a Babcock and Wilcox PWR.

Several conclusions can be drawn by comparing the Surry and Oconee dominant accident sequences:

- The frequency of core melt due to LOCAs (other than an interfacing system LOCA) is similar for both plants (i.e., estimated within a factor of two).
- The frequency of an interfacing system LOCA event V, was assessed to be much higher at Oconee.[1] This frequency could be reduced to a level comparable with the Surry event V by simply changing the motor operated isolated valves from normally closed to normally open.
- The frequency of core melt accidents initiated by transients is similar for both plants (i.e., estimated within a factor of two).
- Containment overpressure failure due to hydrogen burning was assessed to be more important at Oconee. The reason for this is that the Surry accident sequences which dominated the release category in which hydrogen burning is usually placed, failed the containment by overpressure due to steam prior to core meltdown. Since the hydrogen is produced during the meltdown, this containment failure mode for these accident sequences is precluded.
- The overall frequency of a core melt accident was assessed to be similar for both plants (8×10^{-5} for Oconee vs. 5×10^{-5} for Surry).

---

[1]Duke Power has recently introduced changes which significantly reduce the frequency of this sequence (i.e., less than or equal to in Section 6.1.

6.3.2 Limitations

The following limitations were identified in the RSSMAP program:

- The Oconee FSAR, technical specifications and discussions with plant personnel during a single plant visit were the primary sources of information utilized in this study. A more rigorous analysis would require additional information. This upgraded information base should also include as built piping and instrument diagrams, plant procedures, and direct personnel contacts at the plant and reactor vendor for purposes of answering questions.
- The transient event tree initiating events chosen in this study were the same three chosen in the RSS. A more rigorous analysis should consider more transient initiators.
- The majority of the data base utilized in this study was compiled as part of the RSS. This data base was found to be deficient in several areas. An example of this can be noted in the data used in performing the interfacing systems LOCA frequency calculation. The dominant failure mode is both check valves failing to reseat. This is a demand failure which occurs immediately after a low pressure injection system flow test. The data utilized to calculate this reseat failure probability, however, is expressed in failures/hr. rather than failures/demand. (For details, see Appendix A3). Another example is the failure probability of a safety/relief valve to reclose after being demanded open. All available data sources quote failure to reclose probabilities after passing steam. On several of the Oconee transient sequences, however, these valves

would be passing solid water (e.g., TMLs, TKs). Since these valves are not designed to pass solid water, the reclosure failure probability would be expected to be much higher. If, for instance, the reclosure failure probability is an order of magnitude greater after passing solid water, the frequency assessed for several of the Oconee transient induced LOCAs would be underestimated by an order of magnitude. A more thorough analysis should account for these, as well as several other data deficiencies.

This study attempted to identify human errors which could degrade or lead to failure of the safety systems responding to a LOCA or transient. These human errors were of two basic types. Those errors occurring during routine operation, such as inadvertantly leaving valves in the wrong position, and errors which occur during the course of an accident such as the incorrect termination of the high pressure injection system by the operator (e.g., an operator error in the TMI accident). In order to assess operator errors during the course of an accident, the analyst must be aware of the plant parameter indications which the operator is relying upon to make decisions in the control room (e.g., at TMI the operator terminated the high pressure injection system because of a high pressurizer level indication). To gain these types of insights, it is recommended that future, more complete analyses, perform computer simulations of the detailed plant system dynamics associated with each accident sequence.

Table 6-1

SYMBOLS USED IN FIGURE 6-1

Initiating Events

T_1 - Loss of Offsite Power Transient

T_2 - Loss of Power Conversion System Transient Caused By Other Than a Loss of Offsite Power

T_3 - Transients with the Power Conversion System Initially Available

S_1 - Intermediate LOCA (10"<D≤13.5")

S_2 - Small LOCA (4"<D≤10")

S_3 - Small-Small LOCA (D≤4")

V - Interfacing Systems LOCA

System Failures

(B_3)-Emergency Power System

D - Emergency Coolant Injection System

F - Containment Spray Recirculation System

H - Emergency Coolant Recirculation System

K - Reactor Protection System

L - Emergency Feedwater System, Recovery of Power Conversion System and High Head Auxiliary Feedwater System

M - Power Conversion System (Normal Operation)

Q - Reclosure of Pressurizer Safety/Relief Valves

U - High Pressure Injection System

Table 6-1. SYMBOLS USED IN FIGURE 6-1 (Continued)

Containment Failure Modes

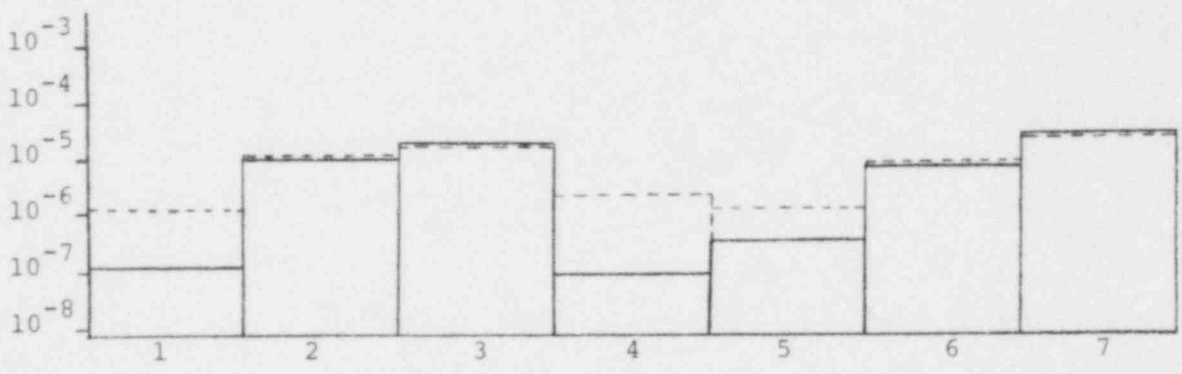
α - Vessel Steam Explosion

β - Penetration Leakage

γ - Overpressure Due to Hydrogen Burning

ϵ - Base Mat Melt Through

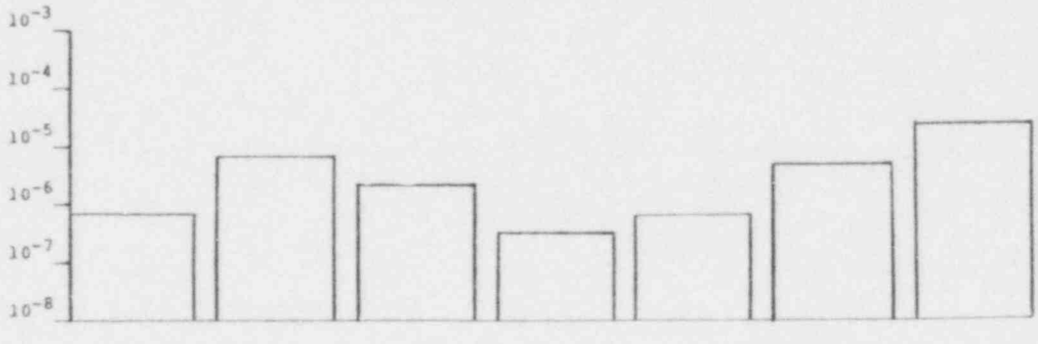
RELEASE CATEGORY	1	2	3	4	5	6	7
T_2MLU			$\gamma\, 6.0\times10^{-7}$		$\beta\, 8.8\times10^{-9}$		$\epsilon\, 6.0\times10^{-7}$
T_1MLU			$\gamma\, 1.0\times10^{-6}$		$\beta\, 1.5\times10^{-8}$		$\epsilon\, 1.0\times10^{-6}$
V		$V<4.0\times10^{-6}$					
$T_1(B_3)MLU$			$\gamma\, 1.1\times10^{-6}$		$\beta\, 1.6\times10^{-8}$		$\epsilon\, 1.1\times10^{-6}$
T_2MQ-H			$\gamma\, 5.5\times10^{-6}$		$\beta\, 8.0\times10^{-8}$		$\epsilon\, 5.5\times10^{-6}$
S_3H			$\gamma\, 5.0\times10^{-6}$		$\beta\, 7.3\times10^{-8}$		$\epsilon\, 5.0\times10^{-6}$
S_1D	$\alpha\, 6.7\times10^{-8}$		$\gamma\, 1.3\times10^{-6}$		$\beta\, 4.9\times10^{-8}$		$\epsilon\, 5.4\times10^{-6}$
T_2MQ-FH		$\gamma\, 2.5\times10^{-6}$		$\beta\, 3.7\times10^{-8}$		$\epsilon\, 2.5\times10^{-6}$	
S_3FH		$\gamma\, 2.1\times10^{-6}$		$\beta\, 3.1\times10^{-8}$		$\epsilon\, 2.1\times10^{-6}$	
S_2FH	$\alpha\, 1.3\times10^{-8}$			$\beta\, 9.5\times10^{-9}$		$\epsilon\, 1.0\times10^{-6}$	
T_2MLUO			$\gamma\, 4.1\times10^{-6}$		$\beta\, 5.9\times10^{-8}$		$\epsilon\, 4.1\times10^{-6}$
T_2KMU			$\gamma\, 3.9\times10^{-6}$		$\beta\, 5.7\times10^{-8}$		$\epsilon\, 3.9\times10^{-6}$
S_2D	$\alpha\, 2.0\times10^{-8}$		$\gamma\, 4.0\times10^{-7}$		$\beta\, 1.5\times10^{-8}$		$\epsilon\, 1.6\times10^{-6}$
S_3D			$\gamma\, 7.0\times10^{-7}$		$\beta\, 1.0\times10^{-8}$		$\epsilon\, 7.0\times10^{-7}$
T_1MLUO			$\gamma\, 2.7\times10^{-6}$		$\beta\, 3.9\times10^{-8}$		$\epsilon\, 2.7\times10^{-6}$
T_3MLUO			$\gamma\, 5.5\times10^{-7}$		$\beta\, 8.0\times10^{-9}$		$\epsilon\, 5.5\times10^{-7}$
T_2MQ-D			$\gamma\, 7.5\times10^{-7}$		$\beta\, 1.1\times10^{-8}$		$\epsilon\, 7.5\times10^{-7}$
CATEGORY TOTAL[1]	1.1×10^{-7}	1.0×10^{-5}	2.9×10^{-5}	9.7×10^{-8}	4.6×10^{-7}	7.3×10^{-6}	3.5×10^{-5}



[1]This is an unsmoothed total which includes the contribution from all the nondominant sequences not shown.

Figure 6-1. Oconee Dominant Accident Sequences

RELEASE CATEGORY	1	2	3	4	5	6	7
TMLB'		$\delta 2\times10^{-6}$ $\gamma 7\times10^{-7}$				$\epsilon 6\times10^{-7}$	
V		$V 4\times10^{-6}$					
S_2C			$\delta 2\times10^{-6}$				
AD							$\epsilon 2\times10^{-6}$
AH							$\epsilon 2\times10^{-6}$
S_1D							$\epsilon 3\times10^{-6}$
S_1H							$\epsilon 3\times10^{-6}$
S_2D							$\epsilon 9\times10^{-6}$
S_2H							$\epsilon 6\times10^{-6}$
TML							$\epsilon 6\times10^{-6}$
TKQ							$\epsilon 3\times10^{-6}$
TKMQ							$\epsilon 1\times10^{-6}$
CATEGORY TOTAL	9×10^{-7}	8×10^{-6}	4×10^{-6}	5×10^{-7}	7×10^{-7}	6×10^{-6}	4×10^{-5}



Note: The probabilities for each release category are the summations of values of the dominant accident sequences plus a 10% contribution from the adjacent release category probability. Categories 1, 4, and 5 are totally dominated by sequences in other categories due to this smoothing.

Figure 6-2. Surry Dominant Accident Sequences

References

1. Oconee Nuclear Station, "Final Safety Analysis Report," Duke Power Company.nd, na.

2. U.S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants." WASH-1400 (NUREG-75/014), October 1975.

3. A. M. Kolaczkowski, P. A. Baranowsky, "A Probabilistic Safety Analysis of DC Power Supply Requirements at Nuclear Power Plants," Sandia National Laboratories, Draft Report, will be NUREG-666, Fall 1980.

4. U.S. Nuclear Regulatory Commission, "Anticipated Transients Without SCRAM for Light Water Reactors," Unresolves Safety Issue Program, Office of Nuclear Reactor Regulation, NUREG-0460, March 1980.

5. R. B. Worrell, D. W. Stack, "A SETS User's Manual for the Fault Tree Analyst," SAND77-2051, Sandia National Laboratories, Albuquerque, New Mexico, November 1978.

6. Wooton, R. O., and Avci, H. I., "MARCH, Meltdown Accident Response Characteristics, Code Description and User's Manual," Battelle Columbus Laboratories (NUREG/CR-1711, BMI-2064), October 1980.

7. R. J. Burian and P. Cybulskis, "CORRAL-2 User's Manual," Battelle Columbus Laboratories, January 1977.

8. W. B. Murfin, "A Preliminary Model for Core/Concrete Interactions," SAND77-0370, Sandia National Laboratories, August 1977.

9. Wooton, R. O., Denning, R. S., and Cybulskis, P., "Analysis of the Three Mile Island Accident and Alternative Sequences," NUREG/CR-1219, Battelle Columbus Laboratories, January 1980.

APPENDIX A1

LOCA EVENT TREE - OCONEE PLANT

Table of Contents

Table of Contents (Cont.)

1. INTRODUCTION

The Oconee LOCA event tree is shown in Figure A1-1. For comparison, the Surry LOCA event trees are shown in Figures A1-2, 3, and 4. A discussion of the functions the Oconee plant systems perform following a LOCA and the criteria which defines function success is discussed in Section 2.1. The Oconee LOCA system event tree is explained in detail in Section 2.2. Following, in Section 3, a comparison of the Oconee and Surry LOCA event trees is made.

2.0 OCONEE LOCA EVENT TREES

2.1 Event Tree Functions and Functional Success Criteria

There are four basic functions which the Oconee safety systems perform given a LOCA:

1) render reactor subcritical
2) provide emergency core cooling
3) prevent containment overpressure failure due to steam evolution
4) remove radioactive materials from containment atmosphere

Except for the first function which must be performed immediately following a LOCA, each of the remaining functions can fail either during the injection phase (water drawn from BWST) or after the switch over to the recirculation (water drawn from containment sump) phase for a sustained protection. This results in seven functions involving the success or failure of various safety systems.

The combinations of plant systems which are required to successfully perform these functions for a variety of LOCA sizes will now be discussed. Refer to Table A1-1 for a summary of this discussion.

2.1.1 Reactor Subcriticality Success Criteria

To halt the fission process and thus achieve reactor subcriticality following small LOCAs, the Reactor Protection System (RPS) is required to insert its control rods into the core. For LOCA sizes greater than about 6" in diameter, however, the reactor is automatically rendered subcritical due to core voiding caused by the LOCA and subsequent core reflood by borated water from the core flood tanks or emergency core cooling system. These larger LOCAs, therefore, do not require the RPS.

Based on discussions with designers of the Oconee reactor RPS, successful reactor subcriticality can be achieved for small LOCAs by the insertion of at least half of the control rod groups into the core.

2.1.2 Containment Overpressure Protection From Steam Evolution Success Criteria

This is stated in 6.2.3 of the FSAR, Design Evaluation of the Reactor Building Spray System (p. 6-18) as follows: "... redundant alternative methods to maintain containment pressure at a level below design pressure. Any of the following combinations of equipment will provide sufficient heat removal capabil ty to accomplish this:

a. The reactor building spray system alone.

b. Three cooling units alone.

c. Two cooling units and the reactor building spray system at one-half capacity (one spray pump train)."

The air cooling units require operation of the Low Pressure Service Water System (LPSWS). The FSAR states (p. 9-32) "The LPSWS requirement following a loss of coolant accident can also be supplied by one pump."

This criteria for success has been found in subsequent research by Battelle Columbus Laboratories to be overly conservative. Their research has shown that one spray train or one fan cooling unit will provide adequate pressure control during the injection phase. Battelle has also shown that one containment spray train operating in conjunction with one low pressure recirculation train and one low pressure service water train can provide adequate pressure control during the recirculation phase (the spray flow is cooled by mixing with the LPRS flow in the sump). One fan cooling unit will also provide adequate containment pressure control during the recirculation phase. This more realistic criteria will therefore be used. Refer to Section 6.0 in Appendix C.

2.1.3 Post Accident Radioactivity Removal Success Criteria

In addition to its depressurization function, the containment spray system scrubs the containment atmosphere of radioactive materials. The operation of one spray subsystem is adequate to perform this function during both the injection and recirculation phases.

2.1.4 Emergency Core Cooling Success Criteria

The FSAR states on page 14-57:

"The high-pressure injection system, with only one pump operating, can protect the core for leaks up to 4 in. in diameter. A combination of one high-pressure and one low-pressure injection pump will protect the core for leaks up to 10 in. in diameter, (0.5 ft^2) whereas, one high-pressure and two low-pressure pumps provide protection for leak areas up to 1 ft^2. For larger break areas, the operation of one high-pressure injection pump, one low-pressure injection pump, and the core flood tanks provides the coolant necessary to keep the core protected."

These FSAR criteria constitute the success criteria for emergency core cooling during the injection phase for the entire spectrum of reactor coolant system break sizes.

For the smallest break range,during the early recirculation phase, the operation of one high pressure train, which draws from the discharge of one low pressure train, provides adequate core cooling. For the larger breaks, the system depressurizes to a low enough level so that the operation of one low pressure train is all that is required.

2.2 Event Tree Definitions and Tree Development

The Oconee LOCA event tree is displayed in Figure A1-1. The systems which perform the seven functions make up the event tree headings. Dependencies among these systems dictate the event tree structure. A single LOCA event tree is an adequate representation for the entire spectrum of break sizes, since the tree structure and tree headings are identical for all breaks. However, some of the tree headings definitions do differ. A discussion of the heading definitions and tree structure follows.

2.2.1 Events A, S_1, S_2, S_3 - Breaks in the Reactor Coolant System (RCS)

The LOCA initiating events are due to random ruptures of the RCS, which fall in the following break size ranges:

LOCA	Equivalent Diameter (D)
A	$D>13.5"$
S_1	$10"<D\leq 13.5"$
S_2	$4"<D\leq 10"$
S_3	$D\leq 4"$

In addition to random ruptures, LOCAs can be transient induced. This latter type is caused by the failure of an RCS relief valve to reclose after being demanded in response to a transient. This LOCA would fall in the S_3 LOCA break size range.

2.2.2 Event K - Reactor Protection System (RPS)

The definition is the same as the reactor subcriticality function given in Section 2.1.1.

The RPS is given a success/failure choice following S_2 and S_3 LOCAs. There is no choice following S_1 and A LOCAs. This is because the operation of the RPS doesn't matter since the reactor is already subcritical due to the initiating event.

2.2.3 Event C - Containment Spray Injection System (CSIS)

This system is known as the Reactor Building Spray System at the Oconee plant. It delivers spray to the containment to remove radioactive material from the containment atmosphere during the period after the RCS break and can have some affect on radioactive material after melt occurs. The spray system provides one means of reducing containment building pressure buildup caused by blowdown energy, protecting against containment failure. The CSIS consists of dual redundant spray headers and pumps that deliver cool water from the borated water storage tank (BWST). Successful CSIS operation requires flow from one of two pump trains.

The success or failure of the CSIS does not depend on the LOCA size or RPS and thus, a success/failure choice is always given.

2.2.4 Event Y - Reactor Building Cooling System (RBCS) During Injection Phase

This system draws the containment atmosphere past cooling coils which are cooled by the low pressure service water system to remove heat from containment. It is thus a means of reducing containment building pressure buildup caused by blowdown energy, protecting against containment failure. The RBCS consists of three air fans and associated coolers. During normal operation the system is in a partial use mode for normal building cooling. The system is automatically turned on full in case of an accident. Successful operation requires cooling from one of three fan units.

The success or failure of the RBCS does not depend on any events preceeding it so a success/failure choice is always given.

2.2.5 Event D - Emergency Coolant Injection System (ECIS)

The ECIS is a group of three subsystems that operate in different combinations to prevent core damage for various break sizes. These subsystems are the core flood system (CFS), the high pressure injection system (HPIS), and the low pressure injection system (LPIS). The CFS consists of two core flooding tanks which automatically deliver borated water to the reactor vessel when system pressure is below 600 psig. The LPIS and HPIS consists of three pumps each, which deliver water to the vessel from the BWST. Successful operation of the ECIS as a function of break size requires the following combinations of subsystems:

LOCA	Functional Success
A	2 of 2 CFS and 1 of 3 HPIS and 1 of 2 LPIS
S_1	1 of 3 HPIS and 2 of 2 LPIS
S_2	1 of 3 HPIS and 1 of 2 LPIS
S_3	1 of 3 HPIS

This combination of equipment is required if the RPS (event K) succeeds. If RPS does not succeed, the following defines success:

LOCA	Functional Success
A	Same as before
S_1	Same as before

LOCA	Functional Success (Cont.)
S_2	2 of 3 HPIS and 1 of 2 LPIS and $\geq$720 gpm from emergency feedwater system
S_3	2 of 3 HPIS and $\geq$720 gpm from emergency feedwater system

The success or failure of the ECIS does not depend on any events preceeding it, so a success/failure choice is always given.

2.2.6 Event F - Containment Spray Recirculation System (CSRS)

This is the recirculation mode of the containment spray system and uses most of the same equipment as the CSIS. Its two pump trains recirculate sump water to the containment spray headers to provide for long-term containment overpressure protection and radioactivity removal. Successful CSRS operation requires flow from one of two pump trains.

Since the CSIS and CSRS share most of the same equipment, failure of the CSIS precludes success of the CSRS. Therefore, no success/failure choice is given for event F, given the failure of event C.

2.2.7 Event Z - RBCS During Recirculation Phase

The system and its requirements for success are identical to event Y previously discussed. No change of system operating state is required, as is the case with the containment spray and emergency core cooling systems, which must be realigned from the BWST to the sump at the start of the recirculation phase. All that is required is the continued operation of the RBCS. This event is included in order to discern RBCS failure, which occurs during the recirculation phase. Since the timing of this system's failure can affect the consequences of an accident sequence, event Z was included.

Since the RBCS is represented by both events Y and Z, failure of event Y precludes success of event Z. Therefore, no success/failure choice is given for event Z given the failure of event Y.

2.2.8 Event H - Emergency Coolant Recirculation System (ECRS)

The high pressure recirculation system (HPRS) and low pressure recirculation system (LPRS) provide for recirculation of coolant in the RCS following a rupture. For small breaks, recirculation is accomplished by the LPRS drawing from the sump and delivering to the suction of the HPRS pumps, which in turn deliver to the core. (It should be noted that the HPRS requires successful LPRS operation.) For larger breaks, the RCS pressure is low enough so that the HPRS is not required and thus, the LPRS delivers to the core. The HPRS and LPRS represent the recirculation modes of the HPIS and LPIS realigned to take coolant from the sump rather than from the BWST. Success of the ECRS requires the following combinations of subsystems as a function of LOCA size:

LOCA	Functional Success
A	1 of 3 LPRS
S_1	1 of 2 LPRS
S_2	1 of 2 LPRS
S_3	1 of 2 LPRS and 1 of 3 HPRS

Since the HPIS/HPRS and LPIS/LPRS share most of the same equipment, failure of the HPIS and LPIS precludes success of the HPRS and LPRS. Therefore, no choice is given for event H given the failure of event D. (It was assumed, though not entirely correct, that failure of event D implies failure of event H. It can be noted by referring to Section 2.2.5, for example, that for an A LOCA, event D could fail due to failure of the CFS only. If this event D failure mode occurs, event H would not be precluded. This assumption was also made in the RSS.)

2.2.9 Event G - LPRS Heat Exchange (LPRSX)

As discussed in Section 2.1.2 of this appendix, there are two methods of providing containment overpressure protection during the recirculation phase of a LOCA.

The first method requires successful operation of 1 of 3 Reactor Building Cooling System fan trains. Failure of containment overpressure protection during recirculation by this method is represented by Event Z on the LOCA event.

The second method of containment overpressure protection during recirculation requires successful operation of 1 of 2 CSRS trains and 1 of 2 LPRS trains and the Low Pressure Service Water System (LPSWS) train associated with the operating LPRS train. Containment overpressure protection is achieved since the CSRS will condense steam in the containment and heat will be removed by the LPRS heat exchanger and LPSWS.

Event G represents failure of both LPRS trains or their associated LPSWS trains to provide cooling using the LPRS heat exchangers. Success/failure choices for Event G are only given when the RBCS has failed (events Y or Z) and the CSRS and ECRS have succeeded. This information reflects the fact that if the RBCS succeeds, containment overpressure protection using the CSRS and LPRS is not required. Also, if the CSRS and ECRS (of which the LPRS is part of) have both failed (events C, F, D, or H), then containment overpressure protection as described by the second method is assured to fail.

3.0 COMPARISON OF OCONEE AND SURRY LOCA EVENT TREES

The RSS constructed three LOCA trees representing plant response to three different break size ranges for the Surry reactor (see Figures A1-2, 3, 4). Due to substantial differences in event tree structure and the event tree headings, a single LOCA tree was not an adequate representation of the plant response and thus, three trees were created. For the Oconee reactor, as discussed previously, one tree was an adequate representation.

Due to plant design differences, events Y and Z appear only on the Oconee event tree. These events represent the RBCS which is a system not present at Surry. Likewise, the Surry event trees included an event I, the sodium hydroxide addition system; a corresponding system does not exist at Oconee.

The Surry event trees include an event depicting the loss of electric power, event B. Since the electric power systems do not, in themselves, perform a post accident mitigating function, it was decided to incorporate these systems into a special initiating event. The Oconee $T_1(B_3)$ sequences are those where offsite power is lost and the emergency AC sources fail (diesels, hydros, etc). This serves to simplify the Oconee event tree structure.

The Surry A LOCA tree had an event called emergency cooling, functionability, event E. This event represented those occasions when ECIS operates, but the core was uncoolable (e.g., failure of core supports resulting in an uncoolable geometry, steam binding from excessive secondary side steam leakage, etc.) This event was based on conservative assumptions regarding lack of functionability. It was not included on the Oconee trees because it is a relatively small contributor to core cooling failure when compared with the unavailability of the ECIS itself. If it were included, the event tree structure subsequent to its success/failure would be identical to that already represented by the structure subsequent to event D. Eliminating event E, therefore, simplifies the event tree structure and was removed on the Oconee tree.

The Surry S_2 LOCA tree has an event L which is not present on the Oconee tree. At Surry for a small LOCA, the RCS must be depressurized by the Auxiliary Feedwater System (AFWS) so that the ECIS can operate. At Oconee the ECIS produces an adequate pressure head such that the AFWS is not required.

And finally, the Surry event trees treated LOCAs initiated by transients (e.g., stuck open RCS relief valves) directly on the transients event tree and assumed they were core melts. The Oconee transient event tree treats these sequences as special events (see Appendix A2). Once that it is determined that the transient has become a LOCA, the sequence is no longer continued on the transient tree, but is analyzed as an S_3 LOCA on the LOCA tree.

Table A1-1. Alternate Equipment Success Combinations for Functions Incorporated into the Oconee LOCA Event Tree

LOCA Size	Reactor Subcriticality	Injection Phase: Containment Overpressure Protection Due to Steam Evolution	Injection Phase: Post Accident Radioactivity Removal	Injection Phase: Emergency Core Cooling[1]	Recirculation Phase: Containment Overpressure Protection Due to Steam Evolution	Recirculation Phase: Post Accident Radioactivity Removal	Recirculation Phase: Emergency Core Cooling
0-4" (0-.087 ft^2) S_3LOCA	>5 Control Rod Groups Inserted Into Core by the Reactor Protection System (RPS)	1/2 Containment Spray Injection (CSIS) OR 1/3 Reactor Bldg. Fan Coolers (RBCS	1/2 CSIS	1/3 High Pressure Injection (HPIS)[3]	1/2 Containment Spray Recirc. (CSRS) with the LPRS heat exchanger OR 1/3 RBCS	1/2 CSRS	1/3 High Pressure Recirc. (HPRS)[2] with Associated Low Pressure Recirc. (LPRS)
4"-10" (.087-.55 ft^2) S_2 LOCA				1/3 HPIS AND 1/2 Low Pressure Injection (LPIS)			1/2 LPRS
10"-13.5"D (.55-1.0 ft^2) S_1LOCA				1/3 HPIS AND 2/2 LPIS			
(>1.0 ft^2) D > 13.5" 'A' LOCA				1/3 HPIS and 1/2 LPIS and 2/2 CFT			

[1]The ECCS success criteria utilized in this study was taken from the FSAR. Duke Power has recently proposed an alternate criteria. The Duke criteria is: 1/3 HPIS for < 4" breaks, 1/3 HPIS and 1/2 LPIS and 2/2 CFT for 4"-10" breaks, 1/2 LPIS and 2/2 CFT for 10" breaks. Utilization of this criteria would not change significantly the results of this study.

[2]It is assumed that the HPRS pumps can operate at greater than 200°F (the pump design temp is 200°F). In some sequences, water temperatures of greater than 200°F may occur (i.e., success of ECR with the LPRS heat exchangers unavailable).

[3]See Table 4-3 for variation depending on success or failure of event K.

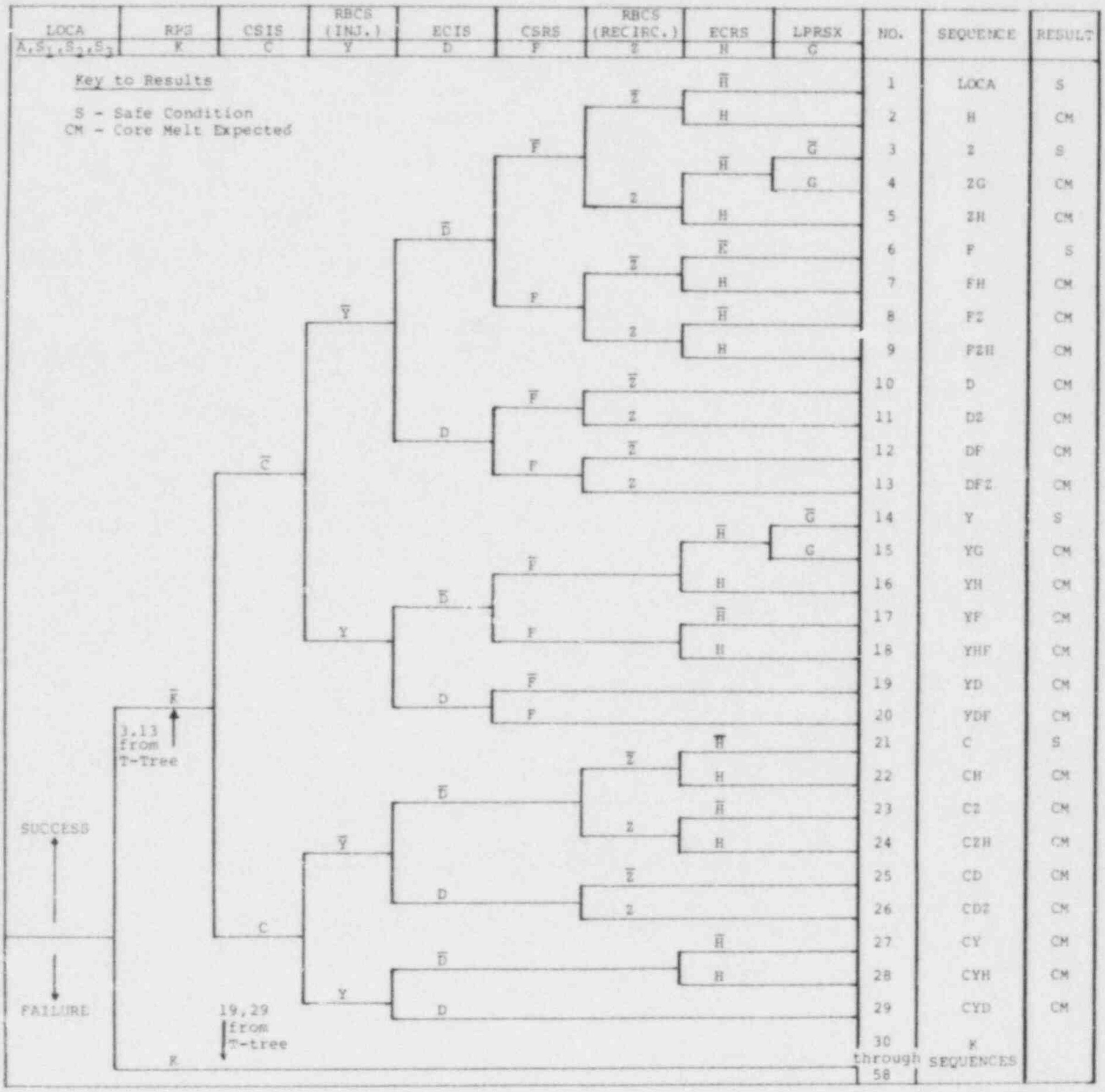


Figure A1-1. Oconee LOCA Event Tree[1]

[1]See discussion given in Table 4-12.

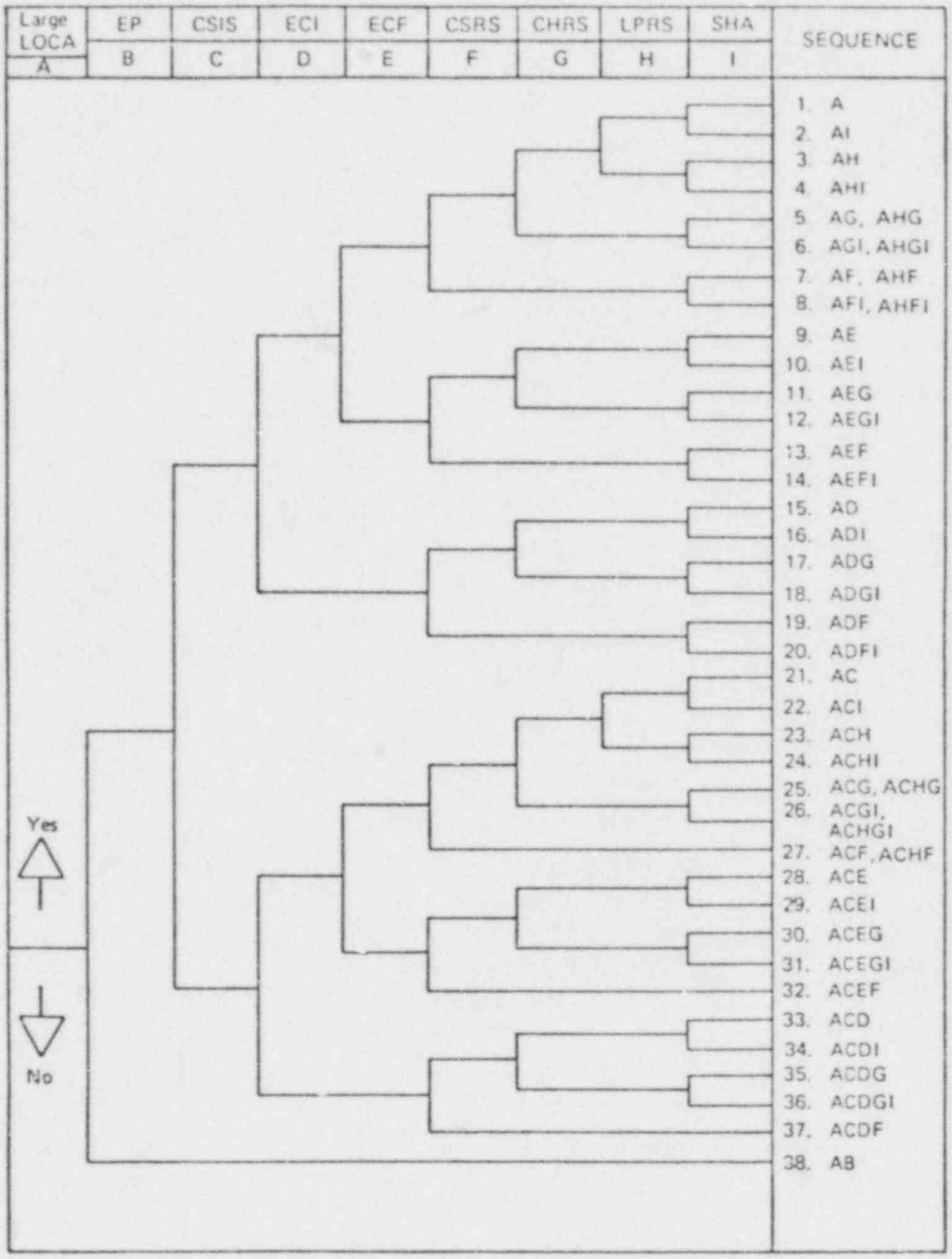


Figure A1-2. RSS PWR Large LOCA Event Tree

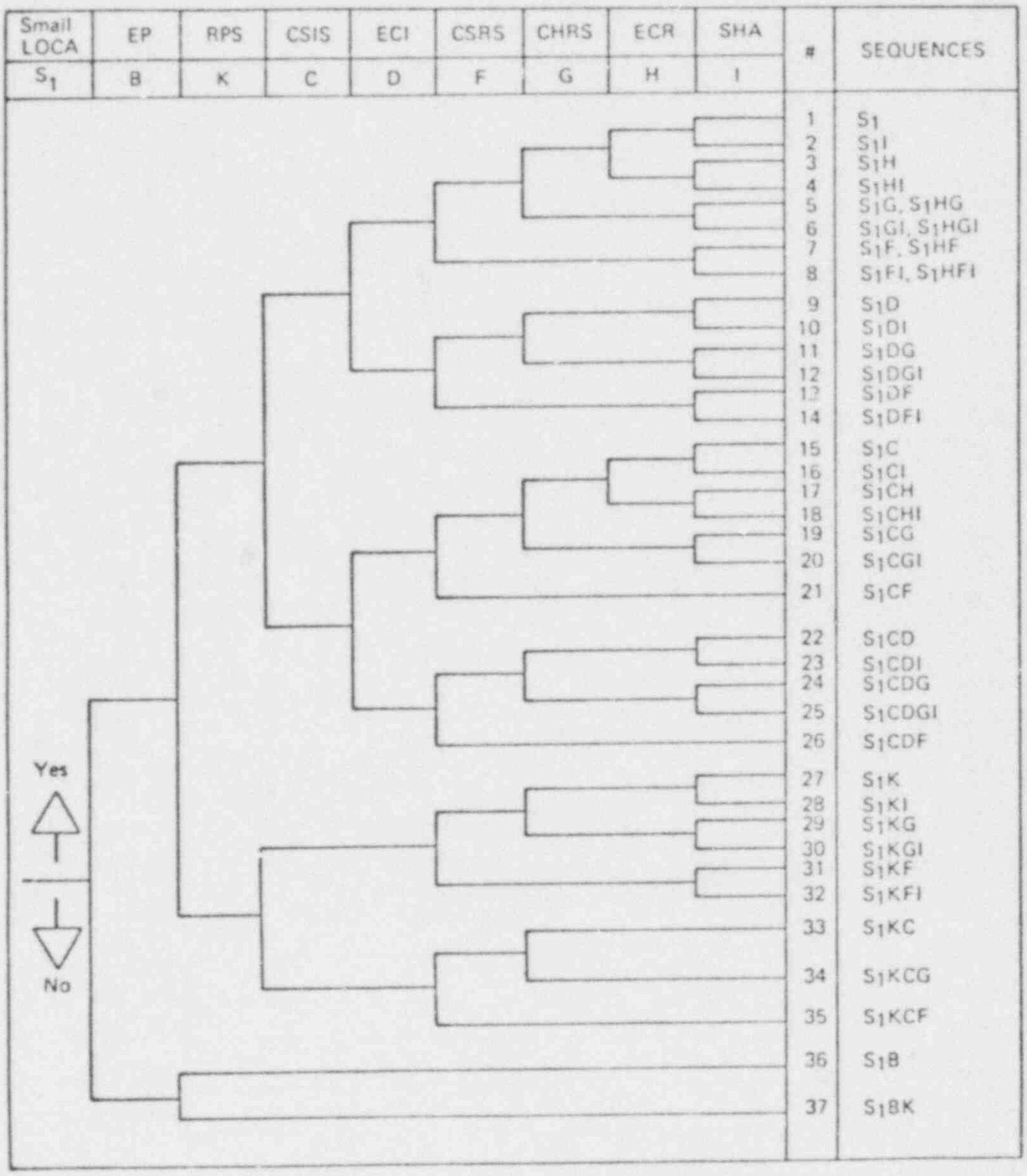


Figure A1-3. RSS PWR Small (S_1) LOCA Event Tree

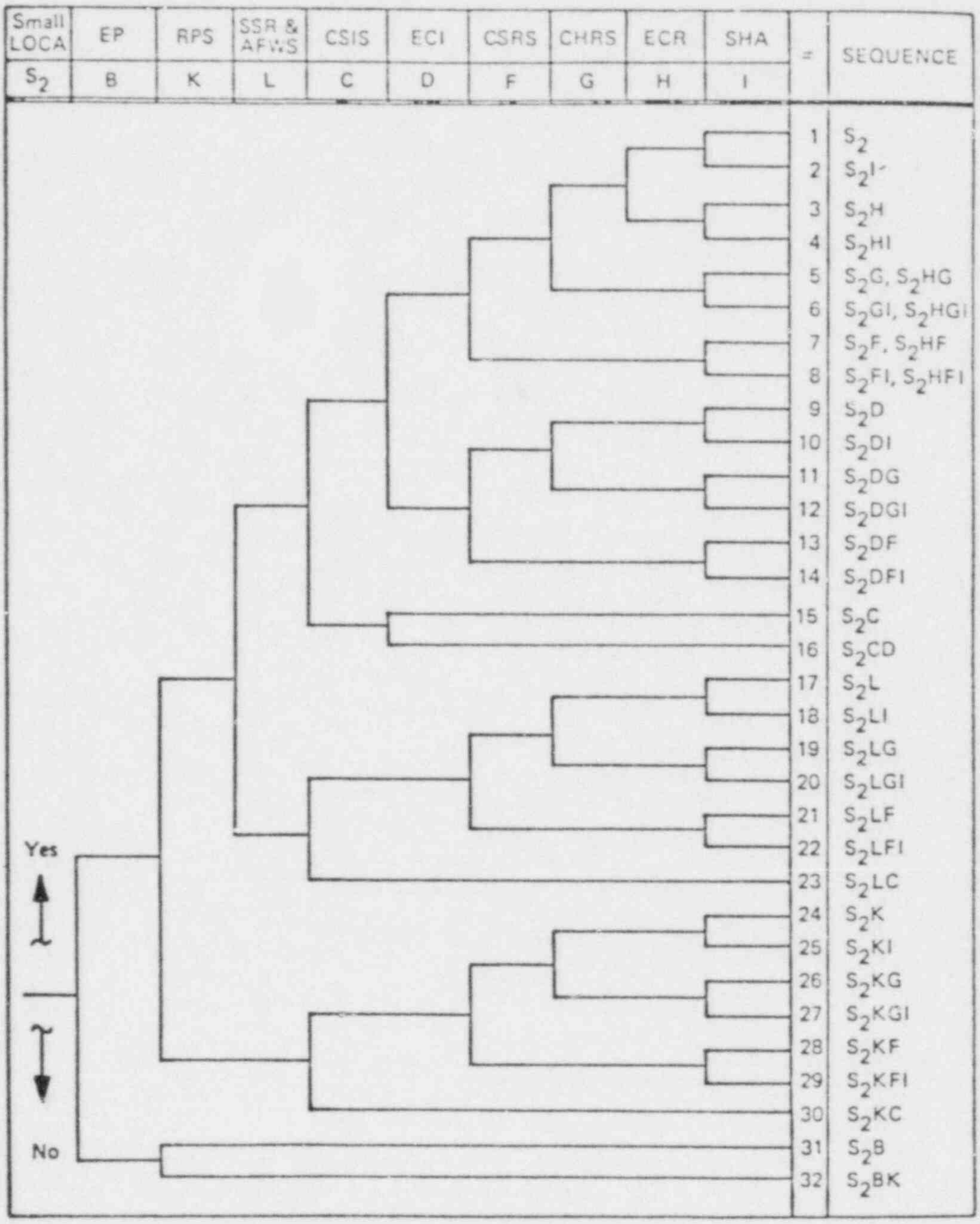


Figure A1-4. RSS PWR Small (S_2) LOCA Event Tree

APPENDIX A2

TRANSIENT EVENT TREE - OCONEE PLANT

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

SECTION PAGE

1.0 INTRODUCTION

The Oconee transient event tree is shown in Figure A2-1. For comparison, the Surry transient event tree is shown in Figure A2-2. A discussion of the functions the Oconee plant system perform following a transient and the criteria which defines function success is discussed in Section 2.1. The Oconee transient system event tree is explained in detail in Section 2.2. In Section 3, a comparison of the Oconee and Surry transient event trees is made.

2.0 OCONEE TRANSIENT EVENT TREES

2.1 Event Tree Functions and Functional Success Criteria

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

1) render reactor subcritical
2) prevent reactor coolant system (RCS) overpressure
3) provide RCS integrity
4) provide core cooling

Reactor subcriticality must be achieved immediately following the transient. RCS overpressure protection is required if a delay is experienced in achieving core cooling. RCS integrity is required to prevent a small small (S_3) LOCA after the successful performance of the RCS overpressure protection function. According to Babcock and Wilcox, core cooling must be provided within 30-40 minutes to prevent core damage.

The functions stated above are required to bring the plant to a hot shutdown condition. Since Oconee can be maintained in a hot shutdown condition without threatening a core melt for an extended period of time, the above functions are an adequate representation of the important Oconee PWR transient functions.[1]

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

5) radioactivity removal from the containment atmosphere

6) containment overpressure protection from steam evolution

The combinations of plant systems which are required to successfully perform these functions for a variety of transients will now be discussed. Refer to Table A2-1 for a summary of this discussion.

2.1.1 Reactor Subcriticality Success Criteria

To halt the fission process and thus achieve reactor subcriticality following transients (non-LOCA induced), the Reactor Protection System (RPS) is required to insert its control rods into the core.

---

1. It should be noted that during the feed and bleed method of core cooling containment overpressure protection from steam evolution is required.

Based on discussions with designers of the Oconee reactor and RPS, successful reactor subcriticality can be achieved for transients by the insertion of $\geq$ 6 control rod groups into the core.

2.1.2 Core Cooling Success Criteria

After achieving reactor subcriticality, post shutdown decay heat must be removed from the reactor coolant system. This is normally accomplished by delivering approximately 6 percent of full feedwater flow to the steam generators and boiling off of this water to the condenser or to the atmosphere via the secondary safety/relief valves. If, however, the shutdown involves a loss of the power conversion system, several backup decay heat removal systems may be utilized.

The first backup system is the emergency feedwater system. This system consists of two 100 percent capacity electric driven pumps and one 200 percent capacity steam driven pump. Successful emergency feedwater system operation requires flow from the turbine driven pump to at least one steam generator or from one motor driven pump to its associated steam generator.

Another backup system is the high head auxiliary service water system. Success of this system requires flow from the single pump to one of two steam generators. Based on discussions with plant personnel, this system would only be utilized if all onsite and offsite AC power were unavailable.

If all methods of achieving decay heat removal via the steam generators are unavailable, decay heat may also be removed directly from reactor coolant system. This may be accomplished by establishing a "feed and bleed" operation. Success of this method requires the flow from one of three high pressure injection pumps and boiloff of the reactor coolant system water through the pressurizer relief valves.

The four methods of core cooling discussed thus far have assumed that reactor subcriticality was achieved. If reactor subcriticality is not achieved, and a failure of the power conversion system also occurs, a RCS pressure of approximately 4000 psi may occur (see NUREG 0460). If the RCS does not rupture, analysis by Battelle Columbus Laboratories has shown that the core can be successfully cooled with the operation of one of three high pressure injection pumps and the emergency feedwater system.

2.1.3 Reactor Coolant System (RCS) Overpressure Protection Success Criteria

For those reactor shutdowns in which reactor subcriticality is achieved immediately and core cooling via the steam generators is achieved within approximately 15-20 minutes, RCS overpressure protection is not required.

For these transients, the surge capacity of the pressurizer would suffice to accept the transient event with only a small surge in the pressure occurring. For more severe transients, such as those involving failure of the RPS to terminate core power, the operability of the pressurizer safety/relief valves would be required to prevent a potential rupture of the RCS.

Two RCS pressurizer safety valves and one solenoid operated relief valve are provided for the Oconee reactor. For those anticipated transients where the RPS operates, operation of only one of the two pressurizer safety valves would limit the RCS overpressure transient to less than 110 percent of RCS design pressure.

For those anticipated transients without scram (ATWS), all three valves are needed to limit RCS pressure to less than 150 percent of the design pressure (Reference 4). It is not clear whether this requirement can be met (e.g. NUREG 0460 quotes peak RCS pressures in the neighborhood of 4000 psi).

2.1.4 RCS Integrity Success Criteria

The RCS pressurizer safety/relief valves that open as a result of a transient event must all reclose to prevent a discharge of an excessive quantity of coolant from the RCS. Otherwise, a valve sticking open following the transient event of interest would result in a loss of coolant event covered in small small (S_3) LOCA sequences.

2.1.5 Containment Overpressure Protection from Steam Evolution Success Criteria

It is stated in 6.2.3 of the FSAR, Design Evaluation of the Reactor Building Spray System (p. 6-18), that: redundant alternative methods exist to maintain containment pressure at a level below design pressure. Any of the following combinations of equipment will provide sufficient heat removal capability to accomplish this:

a. The reactor bui.ding spray system alone.

b. Three cooling units alone.

c. Two cooling units and the reactor building spray system at one-half capacity (one spray pump train).

The air cooling units require operation of the Low Pressure Service Water System (LPSWS). The FSAR states (p. 9-32) that the LPSWS requirement following a loss of coolant accident can also be supplied by one pump.

This criterion for success has been found in subsequent research by Battelle Columbus Laboratories to be conservative. Their research has shown that one spray subsystem or one fan cooling unit will provide adequate pressure control if required following a transient initiating event. This more realistic criteria will therefore be used. It should be noted that containment overpressure protection following a transient is required during the "feed and bleed" core cooling method or during a core meltdown.

2.1.6 Post Accident Radioactivity Removal Success Criteria

In addition to its depressurization function, the containment spray system scrubs the containment atmosphere of radioactive materials. The operation of one spray subsystem is adequate to perform this function during the "feed and bleed" core cooling method or during a core meltdown.

2.2 Event Tree Definitions and Tree Development

The Oconee transient event tree is displayed in Figure A2-1. The systems which perform the six functions make up the event tree headings. Dependencies among these systems dictate the event tree structure. A single transient event tree was deemed to be an adequate representation for all transient initiating events considered. A discussion of the heading definitions and tree structure follows.

2.2.1 Events T_1, T_2, T_3 - Transients Requiring a Rapid Reactor Shutdown

The same three transients chosen in the RSS were also chosen to represent a spectrum of transient initiators at Oconee. These were designated:

T_1 - Reactor shutdown initiated by a loss of offsite power

T_2 - Reactor shutdown initiated by a loss of the power conversion system caused by other than a loss of offsite power

T_3 - Reactor shutdown initiated by other causes in which the power conversion system is initially available

2.2.2 Event K - Reactor Protection System (RPS)

The definition is the same as the reactor subcriticality function given in Section 2.1.1.

The RPS is given a success/failure choice following all three transients.

2.2.3 Event M - Uninterrupted Operation of the Power Conversion System (PCS)

One of the main functions of the PCS at Oconee is to provide feedwater to the steam generators during normal operation. Following a reactor trip the system is also capable of delivering feedwater at a lesser rate to provide the function of decay heat removal. This is accomplished by throttling the power conversion system feedwater flow to approximately 6 percent and allowing this water to boiloff to the condenser or atmosphere.

One method of successful PCS decay heat removal at Oconee can be accomplished by delivering steam generator feedwater with one of two high pressure steam driven feedwater pumps. If these pumps are lost, an alternate method requires the steam generator pressure to be reduced by the operator and feedwater delivery provided by a combination of one of three low pressure electrically driven hotwell pumps and one of three low pressure electrically driven condensate booster pumps. In both modes of operation the heat sink is either the condenser or the secondary steam system safety valves.

Successful PCS operation following a T_3 transient initially requires the automatic throttling of the feedwater flow by the Integrated Control System to approximately 6 percent. Once this has been accomplished, all that is required is the continued operation of the feedwater system. Continued operation is estimated to fail with a probability of 10^{-2} based on RSS insight.

In response to a loss of feedwater transient caused by a hardware problem (T_2) or a loss of offsite power (T_1), successful feedwater operation requires the recovery of the system. (Recovery of the PCS is modeled as part of event L, but will be described here.) In order to recover following a T_1 initiator, offsite power must be restored followed by several operator actions to regain the PCS. In order to recover following a T_2 initiator, the problem must be assessed and corrected. Based on discussions with plant personnel, roughly 90% of the T_2 type transients could be expected to be recovered within 30 minutes. No estimate was given following T_1 transients and, thus, no credit was conservatively given for PCS recovery within 30 minutes. (Refer also to the discussion of the PCS in Chapter 3 of the main report.)

The PCS is given a success/failure choice following all three transients. However, since the PCS will be interrupted by T_1 and T_2 transients, event M will always follow these initiators.

2.2.4 Event L - Emergency Feedwater System (EFS)/ High Head Auxiliary Service Water System (HHASWS)/ PCS Recovery

In the event of a PCS interruption, decay heat may be removed via the steam generators by the EFS or HHASWS. The EFS consists of separate steam generator feed trains supplied by two 100 percent capacity motor driven pumps and/or one 200 percent capacity turbine driven pump, and a combined suction source. The HHASWS consists of a single 2250 gpm motor driven pump which has the capacity of providing adequate shutdown cooling to the steam generators of all three Oconee units simultaneously. Following a loss of the PCS, the EFS is initiated automatically. If the EFS is also unavailable, the operator may initiate the HHASWS remote manually. Based on discussions with plant personnel, the HHASWS would only be utilized if all onsite and offsite AC power was unavailable (i.e., $T_1(B_3)$ transients discussed in Appendix B1, Section 5.1). Credit is therefore not given to this system for T_1, T_2, or T_3 transients in which either offsite or onsite AC power is available.

Successful EFS operation requires the attainment of flow from the turbine driven pump to at least one steam generator or from one motor driven pump to its associated steam generator. Successful HHASWS operation requires the delivery of 500 gpm from the single motor driven pump to one of two steam generators.

If the EFWS and HHASWS are unavailable, the operator will attempt to restore the PCS. (Refer to discussion of PCS recovery in event M.)

Uninterrupted operation of the PCS makes operation of the EFS or HHASWS or recovery of the PCS unnecessary. Thus, success/failure choices for the EFS and HHASWS are given only on sequences involving PCS failure.

2.2.5 Event P_1 - Safety/Relief Valves Demanded (SR/Demand)

Prior to the accident at Three Mile Island the pressurizer pilot operated relief valve (PORV) was demanded to open on most reactor trips. Following the accident, the pressurizer relief valve actuation setpoints and reactor trip setpoints were changed such that the pressurizer relief valves (one PORV and two code safeties) are now not meant to be demanded following a reactor trip if successful core cooling via the steam generators is established within approximately 15 minutes. If core cooling via the steam generators is delayed past this time the RCS pressure will rise to the demand setpoint of the pressurizer relief valves (the PORV being demanded first and closely followed by the demand of the two code safeties). Besides a core cooling delay, the relief valves could also be demanded due to a low miscalibration of the valve setpoints.

Success of "safety/relief valve demand" (event $\overline{P}_1$) is defined as the probabilistic demand of the pressurizer safety/relief valves given a transient in which successful core cooling via the steam generators has been established. This demand probability ($\sim$.01/reactor trip) was roughly estimated based on PWR operating experience reported in NUREG-0611 and NUREG-0635 for Westinghouse and Combustion Engineering reactors respectively. This was done because no data exists for B&W reactors following the post TMI changes to the reactor trip and relief valve actuation setpoints.

A success/failure choice only appears on sequences in which the RPS and EFS/PCS Recovery both succeed. If either the RPS or EFS/PCS Recovery fail, no choice is given since the relief valves will definitely be demanded. If the RPS succeeds and the PCS is uninterrupted ($\overline{KM}$), no choice is given because it is assumed the relief valves will not be demanded.

2.2.6 Event P_2 - Safety/Relief Valves Open (SR/VO)

The definition is the same as the RCS overpressure protection function given in Section 2.1.3.

Success/failure choices appear in all sequences in which the pressurizer safety/relief valves are demanded open (refer to discussion of event P_1 in Section 2.2.5).

2.2.7 Event Q - Safety/Relief Valves Reclose (SR/VR)

The definition is the same as the RCS integrity function given in Section 2.1.4.

Success/failure choices appear in all sequences in which the pressurizer safety/relief valves successfully opened. An exception to this is the accident sequence in which the reactor protection system and all steam generator core cooling fails (KML). For this sequence it is assumed that the safety/relief valves will remain open through core meltdown due to the high RCS pressure. It should be noted that if the pressurizer PORV fails to reclose, it can be isolated by a block valve in series with this valve. The pressurizer safety valves do not have block valves.

2.2.8 Event U - High Pressure Injection System (HPIS)

If all methods of achieving decay heat removal via the steam generators are unavailable (events M and L) core cooling can be accomplished with the high pressure injection system. This requires the operator to establish a "feed and bleed" operation. Success of this mode of core cooling requires the flow from one of three high pressure injection pumps and boil off the RCS water through the pressurizer relief valves.

The "feed and bleed" operation is represented by the HPIS success/failure choice on the accident sequence in which the RPS succeeded, PCS failed and EFS failed (events $\overline{K}$, M, and L, respectively). If the RPS and PCS fail, the emergency feedwater system and the high pressure injection system must both succeed in order to cool the core (refer to Section 2.1.2). This is the reason for the HPIS success/failure choice following events K, M, $\overline{L}$.

2.2.9 Event O - Reactor Building Cooling System (RBCS)

This system draws the containment atmosphere past cooling coils which are cooled by the low pressure service water system to remove heat from containment. It is thus a means of reducing containment pressure caused by steam released into the containment during the "feed and bleed" core cooling method (refer to Section 2.2.8, event U) or during a core meltdown.

The RBCS consists of three air fans and associated coolers. During normal operation the system is in a partial use mode for normal building cooling. The system is automatically turned on full in case of an accident. Successful operation requires cooling from one of three fan cooler units.

RBCS success/failure choices appear on all transient sequences leading to a core melt. A choice is also given on the transient sequences describing the "feed and bleed" core cooling method (sequences 6, 7, and 8).

2.2.10 Event O' - Containment Spray Injection System

This system is known as the Reactor Building Spray System at the Oconee plant. It delivers spray to the containment atmosphere and reduces building pressure caused by steam released into the containment during the "feed and bleed" core cooling method (refer to Section 2.2.8, event U) or during a core meltdown. It can also have some affect on radioactive material release from the containment if a core melt occurs. The CSIS consists of dual redundant spray headers and pumps that deliver cool water from the borated water storage tank (BWST). Successful CSIS operation requires flow from one of two pump trains.

CSIS success/failure choices appear on all transient sequences leading to a core melt. A choice is also given on transient sequences describing the "feed and bleed" core cooling method in which the RBCS has failed.

3.0 COMPARISON OF OCONEE AND SURRY TRANSIENT EVENT TREES

The RSS constructed a single transient event tree which represented the plant response to a variety of transients for the Surry reactor (see Figure A2-2). As discussed previously, a single transient event tree was also chosen to model a spectrum of Oconee transients.

The Surry transient event tree included events U, the chemical volume and control system, and event W, the residual heat removal system. These systems were required to bring the plant from a hot shutdown to a cold shutdown condition. Since Surry can remain in a hot shutdown condition for an extended period of time without threatening a core melt, these systems were not analyzed in detail and were included on the event tree for completeness. Oconee can also remain at hot shutdown for an extended period. The equivalent Oconee systems were not modeled on the Oconee transient event tree for purposes of simplification.

The Oconee transient event tree explicitly includes systems related to containment response (event O and O'). The Surry transient tree did include these systems. Success/failure of these systems were implied, however, in the Surry accident sequence results (refer to Table V3-7 of the RSS; events C and F are t' · containment spray injection system and containment spray recirculation system respectively).

The Oconee event U represents the "feed and bleed" core cooling mode of the high pressure injection system. The Surry event U represents, as discussed earlier, the operation of the chemical and volume control system to bring the plant from hot to cold shutdown. The RSS assumed that a "feed and bleed" core cooling method could not be achieved at Surry.

The Oconee P_1 event, which represents a probabilistic demand of the pressurizer safety/relief valves, does not appear on the Surry tree. The Surry event tree assumed that the relief valves either were or were not demanded with 100 percent certainty.

And finally, the Surry event trees treated LOCAs initiated by transients (e.g., stuck open RCS relief valves) right on the transients event tree and assumed they were core melts. The Oconee transient event tree treats these sequences as special events. Once that it is determined that the transient has become a LOCA, the sequence is no longer continued on the transient tree, but is analyzed as an S_3 LOCA on the LOCA tree.

Table A2-1. Alternate Equipment Success Combinations for Functions Incorporated into Oconee Transient Event Tree

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

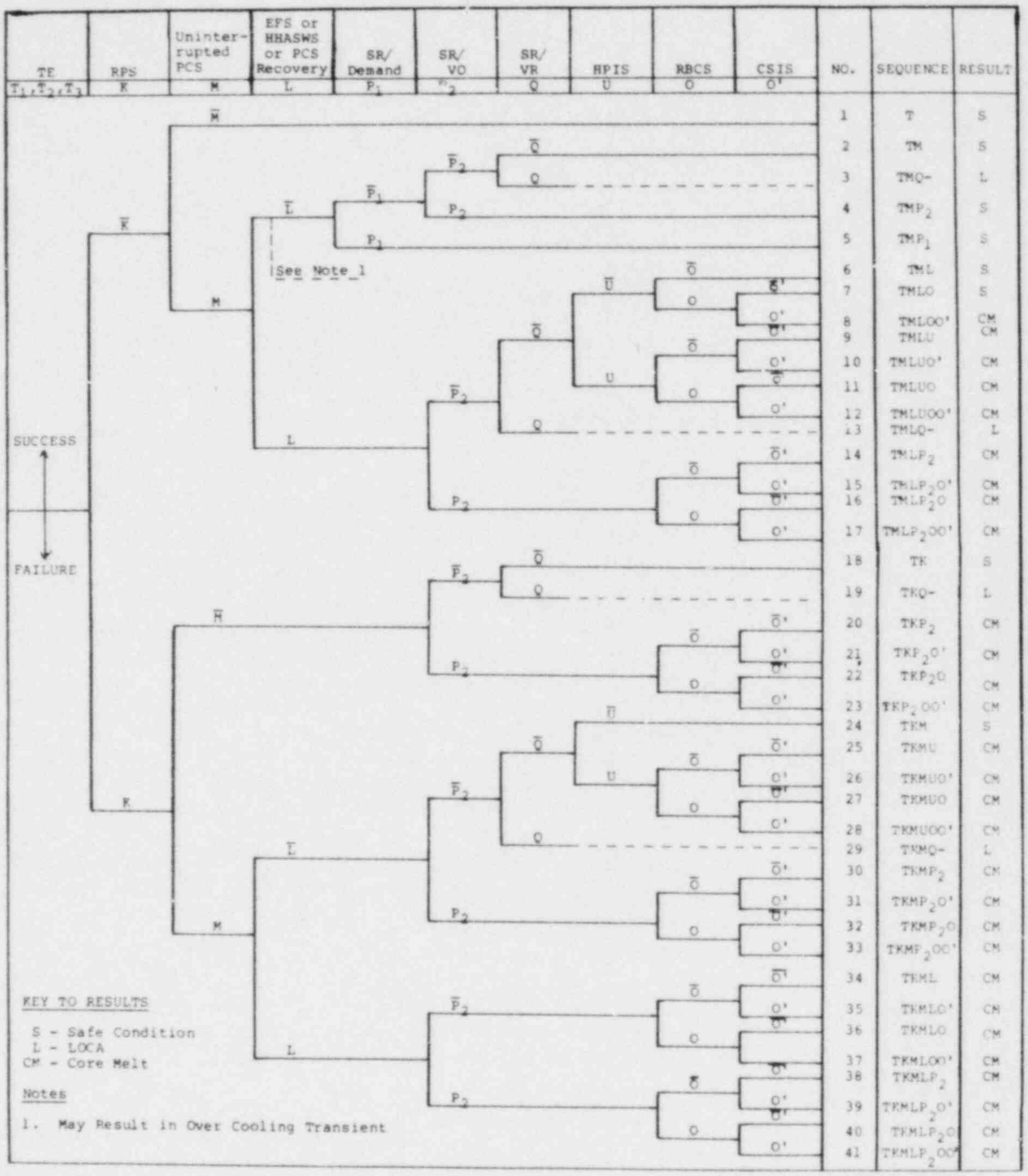


Figure A2-1. Oconee Transient Event Tree[1]

[1]See discussion given in Table 4-12.

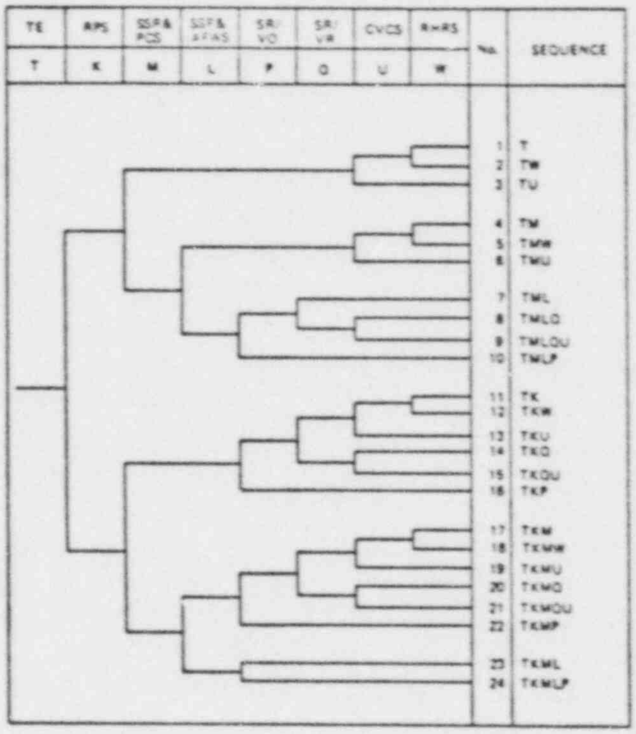


Figure A2-2. RSS Transient Event Tree, PWR

APPENDIX A3

SURVEY AND ANALYSIS
INTERFACING SYSTEMS LOCA - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The systems interfacing with the Reactor Coolant System (RCS) in the Oconee Unit 3 plant which, if certain isolation failures occur, provide a flow path leading to an extra-containment LOCA, were reviewed and compared with the interfacing systems in the similar PWR design (Surry) evaluated in the Reactor Safety Study (RSS). The important interfacing systems for both Oconee and Surry are described and compared in Sections 2 through 4. A point estimate probability of an Oconee interfacing systems LOCA is given in Section 5.

2.0 OCONEE INTERFACING SYSTEMS

2.1 Description

Three major systems, external to the containment, interfacing either directly or indirectly with the Oconee RCS are:

High Pressure Injection and Coolant Makeup System
Low Pressure Injection and Recirculation System
Coolant Storage and Treatment System

To be important to the overall risk, the interfacing system must be susceptible to an extra-containment LOCA caused by containment isolation failure. Of the above interfacing systems, only the LPIS meets this requirement because of its low pressure/low temperature component design which interfaces directly with the high pressure/high temperature RCS. The High Pressure Injection and Coolant Makeup System is designed to meet the RCS design environment and the

Coolant Storage and Treatment System interfaces indirectly with the RCS through low pressure/low temperature let-down and quench tank components located within the containment.

The Oconee LPIS, shown schematically in Figure A3-1 consists of two independent and redundant flow loops containing heat exchangers, served by three pumps with associated piping, valving and control instrumentation. The system draws suction from either the borated water storage tank, the containment sump or one of the RCS hot legs. The system delivers flow through the heat exchangers to the pressurizer spray line and to the two core flooding lines between the core flooding tanks and the core nozzles.

The LPIS suction line is isolated from the high pressure RCS hot leg by a series of three electric motor operated valves, one of which is interlocked with the RCS pressure instrumentation to prevent inadvertent overpressurization through this line. The two LPIS core injection lines are isolated from the high pressure primary system by an electric motor operated isolation valve and two check valves, one of which is common to the core flooding system. The auxiliary spray cooling line is isolated from the pressurizer by a check valve, a manual valve, and one of the two electric motor operated injection isolation valves.

2.2 System Operation

Figure A3-1 shows the LPIS under normal reactor power conditions. Automatic activation is initated by either a RCS pressure of 500 psig or a reactor building pressure of

4 psig. These signals open the borated water storage tank valves and initiate flow of service cooling water through the LPIS heat exchangers. When the borated water storage tank is approximately 94% empty the system is manually reconfigured from the control room to permit circulation of spilled water from the reactor building sump to the core.

During normal reactor shutdown for refueling operations the LPIS may also be manually reconfigured to circulate reactor coolant from one hot leg thru the heat exchangers to the core and pressurizer for long term low pressure/low temperature decay heat removal and pressurizer auxiliary spray cooling. System failures during this low pressure long term shutdown operation, even if coolant spills outside of the containment, will present minimum hazards because the leakage can be quickly stopped by closing the isolation valves. The most likely failure of pump seals will result in small spillage in shielded compartments which drain to the waste disposal system.

The failure mode of concern, with primary risk impact, is the failure of the high pressure isolation valves during reactor power operation which could lead to rupture of the low pressure injection system outside of the containment. These failures may occur in either one of the two redundant low pressure injection lines, the single hot leg suction line or the auxiliary spray cooling line which interconnects with one of the injection lines. A quantitative evaluation of these potential failure paths is provided in Section 5.

At operating conditions, a quarterly test of the LPIS injection isolation MOVs (LP-17, LP-18) is performed by cycling them open and closed. This could provide a leak status check on the outboard injection check valves (LP-47, LP-48). This derives from the fact that during reactor power operation a core flooding pressure of 600 psig exists between the two check valves in the injection lines (Figure A3-1). Should either check valve LP-47 or LP-48 be failed when the isolation MOV is opened, the 600 psig would not be great enough to fail the LPIS with its protective relief valves and would serve as notice to operators to repair this check valve. It has been subsequently learned from plant personnel that prior to opening the isolation MOVs (LP-17, LP-18) the MOVs upstream from them are closed (LP-12, LP-14). Since these valves are between the isolation MOVs and the relief valves, the potential for checking the status of the outboard check valve is lost.

A final assumption for the analysis was that if the outboard check valve fails, the 600 psig accumulator pressure would not fail the 500 psig lines or valves.

3.0 SURRY INTERFACING SYSTEMS

As in the Oconee design, only one of several interfacing systems includes a direct low pressure/high pressure RCS interconnection which would result in an isolation failure induced extra-containment LOCA. This is the Residual Heat Removal System (RHRS) aligned for low pressure emergency coolant injection during reactor power operation. A schematic diagram of the Surry (LPIS) is shown in Figure A3-2. Six isolation protected pipelines interconnect the LPIS with the RCS. These lines interconnect with each of the three hot and three cold legs of the RCS. Based on the number of valves in series and their normal positions, the cold leg injection paths (two series check valves) are the greatest risk contributors.

4.0 COMPARISON BETWEEN OCONEE AND SURRY INTERFACING SYSTEM

The LPIS aligned for emergency core coolant injection during reactor power operation is the only significant interfacing system in both the Oconee and Surry plants. The dominant contributors to failure in the Surry LPIS involved the 3 cold leg injection flow paths to the RCS, each of which contains 2 check valves in series. The dominant failure modes for each pair of valves included: 1) rupture-leak and 2) leak-rupture. Leak-leak was eliminated as a possible failure mode because early detection could be made before any serious problem arose. The probability of rupture-rupture was not significant.

The use of a normally closed motor operated valve in each of the two 10" Oconee LPIS injection lines (along with two isolation check valves) makes the leak-leak failure mode more likely because it may exist undetected during power operation. The rupture-rupture failure probability was an insignificant contributor to the total event V probability. (See discussion of Sequence V in main report.)

Isolation valve failures in the 1-1/2 inch pressurizer spray header (LPIS interfacing) could also go undetected. This will not result in loss of the LPIS, however, because the flow through the 1-1/2" interfacing line is within the capacity of the LPIS relief valves. Isolation of the primary system can still be restored by closing a motor operated valve.

The probability of occurrence for this accident is considerably higher for Oconee due primarily to the inclusion of the leak-leak failure mode in the probability assessment. This failure mode is detectable at Surry but is not at Oconee and dominates the Oconee interfacing systems LOCA probability.

5.0 OCONEE INTERFACING SYSTEMS EVALUATION

5.1 Event Tree Interrelationships

The event LPIS valve failure (event V) does not occur on the LOCA or Transient Event Trees. The event tree, shown in Figure A3-3 was developed in the RSS explicitly for this event and applies also to Oconee. All four sequences result in core melt; valve rupture is assumed to result in core melt regardless of which other systems operate. The effect of the other three systems, electric power, reactor protection, and emergency cooling injection is merely to delay the melt.

Electric power (event B) is necessary for the operation of the high pressure injection portion of the emergency coolant injection (event D). Operation of the ECI will delay core melt until the borated water storage tank has been exhausted. Reactor Portection System operation (event K) will only slightly delay the melt.

5.2 Determination of Oconee Interfacing Systems LOCA Failure Probability

Three failure modes have been identified for Oconee which result in the sequence V (valve failure), extra-containment LOCA:

A. Failure of two check valves and the isolation valve in either one of the two independent low pressure injection lines.

B. Failure of the one check valve, the manual valve and the isolation valve in the low pressure auxiliary spray cooling line.

C. Failure of the three isolation valves in the RCS hot leg low pressure suction line.

Failure modes A and C above will result in a large extra-containment LOCA because of the large pipe sizes. Failure modes A and C are also important because they preclude successful LPIS operation. Failure mode B will be constrained to a small extra-containment LOCA (S_1) by the 1-1/2 " diameter auxiliary spray cooling line.

The dominant failure combinations for the low pressure injection lines of the Oconee LPIS are described here. There are three valves which isolate the LPIS from the high RCS pressure. These include two check valves and a motor operated valve (normally closed). The three valves are arranged in series as shown in Figure A3-1. The dominant failure mode for these three valves would be undetected failure of both check valves either by leakage or rupture, combined with opening of the motor operated valve for quarterly testing.

There are four possible failure mode combinations which dominate event V. For one train they are:

1) CF-14 CV Leaks; LP-48 CV Leaks; LP-17 MOV opened for Quarterly Test
2) CF-14 CV Leaks; LP-48 CV Ruptures; LP-17 MOV opened for Quarterly Test
3) CF-14 CV Ruptures; LP-48 CV Leaks; LP-17 MOV opened for Quarterly Test
4) CF-14 CV Ruptures; LP-48 CV Ruptures; LP-17 MOV opened for Quarterly Test

The analysis was based on the following assumptions:

1) The two check valves in each train (i.e., CF-14, LP-48) fail independently in time rather than sequentially in time as was done in the RSS. The reasoning behind this is that each check valve is pressurized by separate sources (i.e., CF-14 by the RCS, LP-48 by the core flooding tank).
2) Leak failures of concern are those caused by the failure of the check valves to reseat after a semi-annual flow test of the LPIS. These leaks are assumed to be large enough to fail the low pressure piping of the LPIS due to a subsequent water hammer if both check valves are subject to this failure and the MOV is opened. Other

smaller leaks, are not deemed to fail the LPIS since the associated flow rates and water hammer would not be severe enough to rupture the LPIS piping. The time of check valve reseat leak failure is therefore the LPIS flow test.

3) The following are the failure rates used in the analysis:

$$P\ (\text{Leak}) = \lambda_L = 3 \times 10^{-7}/\text{hr.}$$

$$P\ (\text{Rupture}) = \lambda_R = 1 \times 10^{-8}/\text{hr.}$$

The assumption is that these failure rates apply equally to the inboard and outboard check valves even though they are subject to a different pressure differential.

4) The check valve leak demand failure probability can be approximated by[1]:

$$Pd_L \approx P(\ \text{Leak}) \times (\gamma BS)$$

where γBS is the time (4380 hours) between LPIS flow tests (or between shutdowns since this is when the LPIS is flow tested). The reason for this approach is that data does not exist for the reseat failure probability of a check valve.

5) The probability of sequence V per year can be estimated by calculating the probability per year of sequence V based on a 5 year average (this approach was also taken in the RSS). The reason for using this approach is that

[1]See "PWR sensitivity to Alterations in the Interfacing System LOCA," EPRI NP-262, September 1976, pg. 6.

there appears to be no procedure for testing the integrity of the check valves.

The failure probability estimate for each of the four possible failure modes will be discussed separately. These estimates will then be combined to yield the final assessed probability of the Oconee interfacing system LOCA.

1) <u>CF-14 CV Leaks; LP-48 CV Leaks; LP-17 MOV Opened for Quarterly Test</u>

An estimate of the 5 year failure probability for this failure mode can be given as:

$$P(\text{Leak-Leak}) = [10(Pd_{L_{CF-14}})]^{*}\ [10(Pd_{L_{LP-48}})]$$

$$= 1.7 \times 10^{-4}$$

The factors of 10 originate from the fact that there are 10 LPIS flow tests in a 5 year period and therefore 10 opportunities for each check valve to fail to reseat.

It should be noted that in the RSS V assessment for the Surry plant that leak-leak failures were not considered. This is because early detection of this failure mode was possible during RCS heat up due to the fact that the MOV was in the normally open position and this failure would have been sensed by instruments in the control room.

2) <u>CF-14 CV Leaks; LP-48 CV Ruptures; LP-17 MOV Opened for Quarterly Test</u>

An estimate of the 5 year failure probability for this failure mode can be given as

$$P(\text{Leak - Rupture}) \approx [10(Pd_{L_{CF-14}})]*[\lambda_{R_{LP-48}}\tau_5]$$

$$= 5.8 \times 10^{-6}$$

where

τ_5 = Time of 5 years or 43800 hours

3) CF-14 CV Ruptures; LP-48 CV Leaks; LP-17 MOV Opened for Quarterly Test

An estimate of the 5 year failure probability is the same as for the leak-rupture. Therefore:

$P(\text{Rupture-Leak}) = 5.8 \times 10^{-6}$.

4) CF-14 CV Ruptures; LP-48 CV Ruptures; LP-17 MOV Opened for Quarterly Test

An estimate of the 5 year failure probability is:

$$P(\text{Rupture - Rupture}) \approx \left[\lambda_{R_{CF-14}}\tau_5\right] \bullet \left[\lambda_{R_{LP-47}}\tau_5\right]$$

$$= 1.9 \times 10^{-7}$$

The final assessment of the probability of event V is found by summing the above failure mode probability estimates, multiplying the sum by 2 because there are two MOV-check valve trains, and dividing the sum by 5 to yield a per year estimate. This can be stated in equation form as:

$$P(V) \approx \frac{2}{5}\left[P(L - L) + P(L - R) + P(R - L) + P(R - R)\right]$$

$$= 7.3 \times 10^{-5}/\text{reactor year} \quad .$$

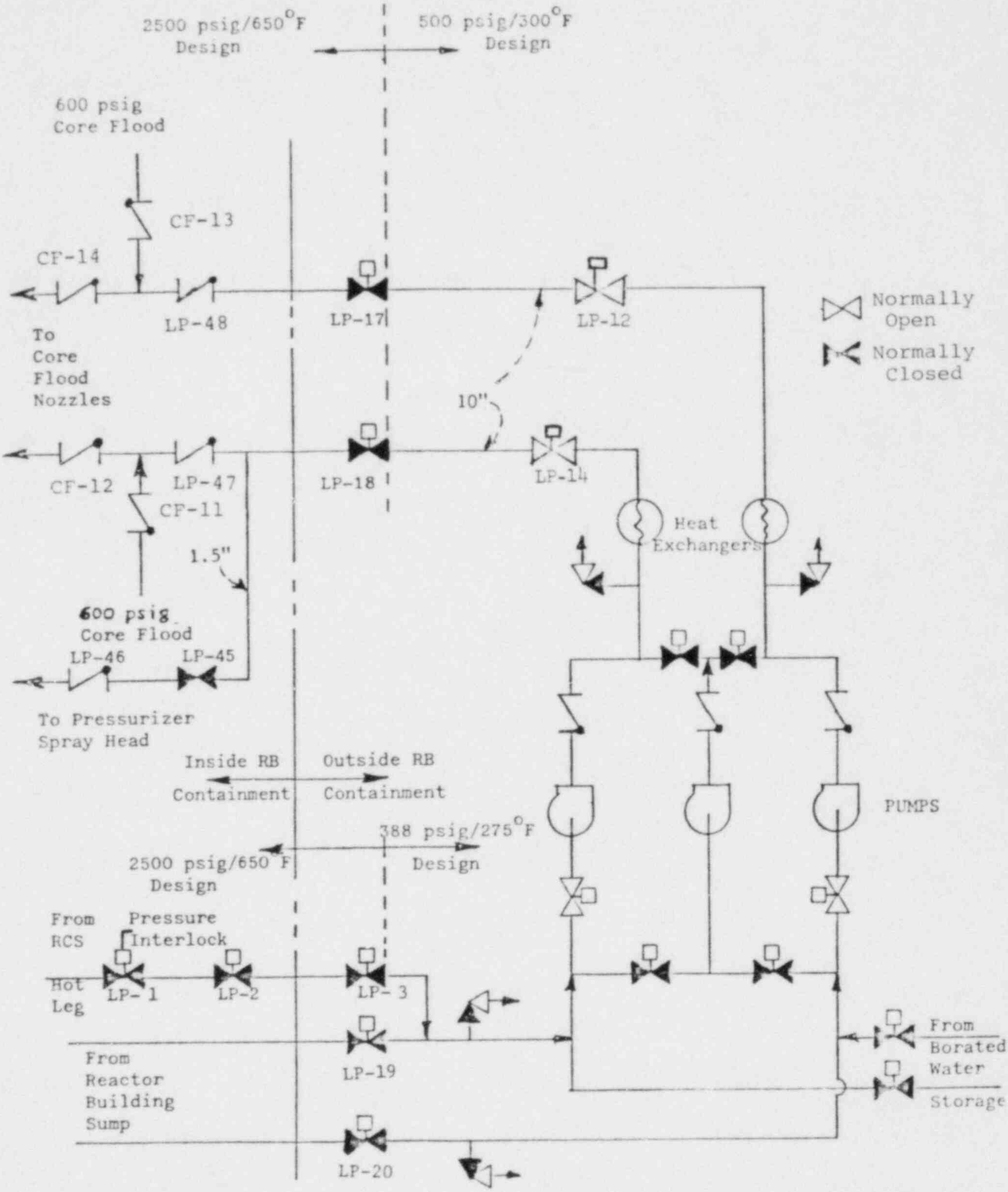


Figure A3-1. Oconee #3 Low Pressure Injection System

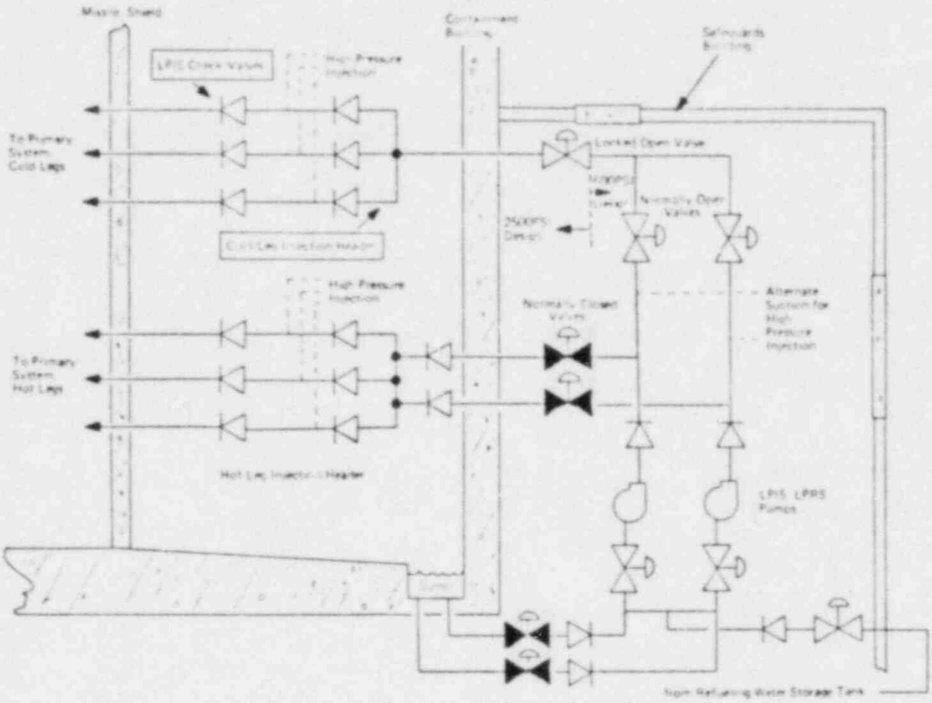


Figure A3-2. Surry LPIS Schematic Diagram

LPIS Check Valve Rupture	EP	RPS	ECI	#	SEQ	CORE
V	B	K	D			
				1	V	M
				2	VD	M
				3	VK	M
				4	VB	M

Figure A3-3. Surry LPIS Valve Rupture Event Tree

APPENDIX B1

SURVEY AND ANALYSIS

EMERGENCY POWER SYSTEM (EPS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Emergency Power System (EPS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The EPS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two emergency power systems is given in Section 4. EPS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a point estimate of the EPS unavailability.

2.0 OCONEE EPS DESCRIPTION

2.1 System Description

2.1.1 Station Emergency Power Systems

The emergency electric power system for Oconee is designed to provide sufficient sources of, and feed path arrangements for, AC power to ensure (1) continuous operability of 4160 volt ES buses and the 600 volt and 208 volt ES auxiliary buses and (2) orderly control of the reactor following a LOCA and/or loss of off-site power.

The following power sources are available to supply emergency power in the event of a LOCA:

(a) 230 kV and/or 500 kV transmission systems

(b) Two 87,500 KVA Keowee hydroelectric generators

(c) 100 kV transmission system from the Lee Steam Station combustion turbine generators

(d) Either of the other two Oconee units.

The preferred switching order is (1) the 230 kV transmission network through the unit startup transformers, (2) one Keowee hydro unit through an underground circuit, and (3) the other Keowee hydro unit through the overhead 230 kV circuit. Whenever the Keowee underground circuit is unavailable, a circuit from the 100 kV transmission network can be connected to standby buses and serve as an emergency power source. A simplified schematic of the Keowee and Lee Steam Station transmission circuits is shown on Figure B1-1.

The 230kV/500kV system serves as the second off-site circuit by disconnecting the generator from the main 19 kV bus and energizing the unit auxiliary transformer by backfeeding through the unit's main step-up transformer.

Power from the two 87,500 KVA Keowee hydro generators, which have a start-up time of 23 seconds, is supplied through two separate and independent circuits. The power generated from one generator is adequate to power the emergency loads for all three Oconee units simultaneously. One circuit is a 4000 foot underground 3.8kV cable feeder to a transformer at the nuclear station which supplies redundant 4160 volt standby power buses. The second circuit is a 230kV transmission to the 230kV switching station at the nuclear station which supplies the unit's startup transformer. Each hydrogenerator is connected to a common 230kV stepup transformer through a 13.8kV metal-enclosed bus and synchronizing air circuit breaker. The 13.8kV underground feeder is arranged with double air circuit breakers so that it can be connected to either 13.8kV generator bus. At the nuclear station a transformer converts the voltage to 4160 volts. Both hydro units are served by a common tunnel-penstock. Unwatering for tunnel or scroll case maintenance will make both units unavailable.

This is expected to occur about one day per year plus four days every tenth year.

The Lee Steam Station provides power to the nuclear station via a 100kV transmission system to a separate transformer located on the opposite side of the 230kV facilities at the Oconee unit. Located at the Lee Steam Station are two 44.1 MVA combustion turbines, which have a startup time of 15 minutes, one of which can be connected to the 100kV line. This line is isolated from the rest of the system and supplies the emergency power to Oconee.

2.1.2 Station Distribution System[1]

The station distribution system (Figure B1-2) consists of the various electrical systems designed to provide electrical power during all modes of station operation and shutdown conditions. The systems are designed with sufficient power sources, redundant buses, and required switching to accomplish this. ES equipment for each unit is arranged onto three load group buses such that the loss of a single bus section for any reason results in only the loss of equipment fed from that bus leaving redundant equipment to perform the same function. In general, the equipment related to unit operation is connected to its respective unit auxiliary electrical buses, whereas equipment common to and serving all units is distributed among unit auxiliary electrical buses. Control of power sources and switching for the unit is from the unit control room.

---

1. Section 2.1.2 is included for completeness. A thorough understanding of this section is not required to understand the derivation of the EPS point estimate unavailability. Many readers may wish to skip this section.

(a) 4160 Volt Auxiliary System

The 4160 volt auxiliary system unit is arranged into a double bus - double circuit breaker switching arrangement. The three power sources; i.e., (1) the unit's auxiliary transformer, (2) the startup transformer and (3) the standby power buses, feed each of the main feeder buses by this double circuit breaker arrangement. Each of the two redundant main feeder buses provide power to each of the three redundant ES switch gear bus sections (3TC, 3TD and 3TE).

(b) 600 Volt Auxiliary System

The 600 volt auxiliary system is arranged into multiple bus sections as is the 4160 volt system. Each bus section is fed from a separate load center transformer which is connected to one of the three 4160 volt switchgear bus sections. Various 600 volt motor control centers are located throughout the station to supply power to equipment within the faulted area. The three ES load centers and associated MCCs are redundant and are supplied independently from the three 4160 volt ES load buses. Each MCC has an alternate feeder with manual transfer to be utilized only for maintenance.

(c) 208 Volt Auxiliary System

The 208 volt auxiliary system is provided to supply instrumentation, control and power loads which require unregulated 280/120 AC power. It consists of MCCs, distribution panels, and transformers fed from redundant 600 volt MCC. The feeder breakers have mechanical interlocks and manual transfers.

(d) DC Power Systems

Three separate DC power systems are provided; namely, a 125 volt DC system provides a source of continuous power for control and instrumentation for normal operation and orderly shutdown, a separate 125/250 volt DC system which provides critical power for switching between alternate off-site power or on-sight emergency power from the EPS, and a separate and independent DC power system for each Keowee hydro units to assure a source of continuous power for normal and emergency operation (See Appendix B2 for further discussion of the DC Power System).

(e) 120 VAC Vital Power Buses

Four redundant 120 volt AC vital instrument power buses are provided to supply power in a predetermined arrangement to vital power, instrumentation, and control loads under all operating conditions. Each bus is supplied separately from a static inverter connected to one of the four 125 volt DC control power panelboards. Upon loss of power from a 125 volt DC bus, the affected inverter is supplied power from the remaining bus through its respective DC control power panelboards and transfer diodes. A tie with breakers is provided to each of the 120 volt vital AC buses from the alternate 120 volt AC regulated bus to provide backup for each vital bus and to permit servicing of the inverters. Each inverter has the synchronizing capability to permit synchronization with the regulated buses.

Each of the four redundant channels of the nuclear instrumentation and reactor protective system equipment is supplied from a separate bus of the four redundant buses. Also, each of the three redundant channels of the Engineered Safeguards Protection System is supplied from a separate bus of the four redundant buses. The two engineered safeguards actuation power buses are supplied from separate vital power buses.

(f) <u>240/120 VAC Essential Power System</u>

Three essential power systems are provided and include:

1) Integrated Control System (ICS) power system - 120 volt AC, single phase.
2) Auxiliary Power System (APS) - 120 volt AC, single phase.
3) Computer Power System (CPS) - 240/120 volt AC, single phase.

Each of these three systems consists of a static inverter, with redundant 125 volt DC supplies from separate 125 volt DC buses, circuit breakers, and distribution panelboard. Also, a static transfer switch is provided in each system as a means for automatic transfer of system loads unavailable. The output of each inverter is synchronized with the AC regulated power system through the static switch in order to minimize transfer time from inverter to the regulated supply.

(g) <u>240/120 VAC Regulated Power System</u>

This system is provided to supply instrumentation, control, and power loads requiring regulated AC power. It also serves as an alternate power source to both the vital power panelboards and to the essential power panelboards. The system consists of two distribution panels, two regulators, and two transformers fed from separate MCCs.

(h) DC and AC Vital Power System Monitoring

Failure and/or misoperation of all DC and AC vital power system equipment is monitored on two local alarm annunciators located in the equipment room near most of the vital equipment. Several variables within each piece of redundant group of equipment are monitored on one of the local panels, with one alarm from each group being taken to alarm panels in the control room. The control room alarms alert the operator if an alarm condition occurs on any piece or group of equipment or if power is lost to the local alarm monitoring equipment.

The DC bus tie breakers, battery breakers and standby charger breaker position indication contacts, the standby charger trouble contact, and the computer, ICS and auxiliary inverter isolating diode trouble contact are monitored directly in the control room.

The other vital alarms are divided into two separate and independent monitoring systems. Alarm for equipment which have battery 1CA for their primary source of power are maintained physically and electrically separate from battery 1CB powered equipment. For example, the distribution center, isolating diodes, breakers, panelboards, inverters and transfer switches associated wtih battery 1CA are alarmed on local and remote annunciators which are physically and electrically separated from the annunciators being used for monitoring battery 1CB associated systems.

2.2 System Operation

The normal power supply to the unit's auxiliary loads is provided through the unit auxiliary transformer connected to the generator bus. If power is not available from the unit's generator bus, the generator is disconnected from its main buses and power to the unit is provided by the 230kV system which is backfed through the auxiliary transformer from the 230kV/500kV switching station through the main step-up transformer. If both of these sources become unavailable the two Keowee hydro units provide station power via a 13.8kV underground feeder and a 230kV overhead line. In the event that the Keowee units are unavailable the Lee Steam Station can provide 100kV from one of the two 44.1 MVA turbines.

2.2.1 Loss of Offsite Power

In the event of a loss of offsite power, the following actions take place:

1) Both Keowee hydro units are started immediately (~23 seconds) and the unit not connected to the 13.8kV underground feeder is connected automatically to the 230kV switching station when the 230kV switching station is isolated from the system network.
2) The 230kV switching station is isolated automatically by energizing the dual trip coils of the 230kV power circuit breakers.
3) The startup transformers (CT1, CT2, and CT3) remain connected to the 230kV switching station.

4) The 13.8 kV underground circuit from Keowee becomes energized as the hydro unit to which it is connected is started.

5) In the event both hydro units are unavailable, the Oconee operator will notify the Lee Steam Station to supply power to the plant. Upon notification, it takes at least 15 minutes for the Lee Station to provide power to the plant.

2.2.2 Loss of Coolant Accident

In the event of a LOCA requiring the engineered safeguards, the following actions take place:

1) Both Keowee hydro units are started immediately (~23 seconds).

   The unit not connected to the 13.8kV underground feeder is run on standby and connected to the 230kV switching station when the switchyard is isolated.

2) The 13.8kV underground circuit from Keowee becomes energized as the hydro unit to which it is connected is started.

3) The 4160 volt redundant main feeder buses of the unit with the accident are switched to the emergency power sources in the preferential order as described in Section 2.1 of this report.

4) The engineered safeguards of the unit with the accident are started and the non-essential loads are shed when power is unavailable from the normal of startup sources.

The initiation of startup is accomplished by control signals from the Oconee control room via the Engineered Safeguards Protective System Logic. Normal startup is by operator action and emergency startup is automatic via redundant signals for both manual and automatic startup. The loads to be supplied are included below. Non-essential loads are shed. Loads other than those listed below can be supplied by the EPS at the operator's option, e.g., condenser circulating pump, air compressor, component cooling pump, etc.

Engineered Safeguards Loads

Description	No. & Size
H.P. Injection Pump	3 @ 600 hp
L.P. Injection Pump	3 @ 400 hp
L.P. Injection Valves	2 @ 20 hp
L.P. Service Pump	2 @ 600 hp
R.B. Spray Pump	2 @ 250 hp
R.B. Cooling Fans	3 @ 150 hp
Penetration Room Vent Fans	2 @ 5 hp
MOVs	(39) 100 hp
	(4778 KVA total)

3.0 SURRY EPS DESCRIPTION

The Surry EPS is configured to provide continuous AC power to the Engineered Safety Features (ESF) 4160 volt buses (1H & 1J) in the event of a LOCA. A simplified block diagram and single line diagram are shown on Figures B1-3, B1-4, and B1-5, respectively. The ESF buses support 480 volt AC emergency buses providing power for a battery charger element of the battery/direct current and static AC inverter vital buses. Dual vital bus systems are cross connected (using regulating transformers) to the 480 volt emergency buses. The DC and AC vital buses permit orderly control of the reactor during momentary 4160 volt AC interruptions.

The source of emergency AC power for Surry consists of a dedicated diesel generator (one for each of two Surry Units) and a backup diesel generator shared by the two Surry Units. The dedicated and shared diesels go on line direct to the 4160 volt ESF buses of the affected unit in the event of a LOCA/ESF demand.

The emergency power distribution system consists of two redundant, and basically independent trains, Trains A and B. Each train consists of a DC network and an AC network. Train A consists of AC buses which include the letter "H" in their designation and DC buses with the letter "A" in their designation. Train B consists of AC buses with the letter "J" in their designation and DC buses with the letter "B". The train alignment of the buses is as follows:

Train A	Train B
4160 V bus 1H	4160 V bus 1J
480 V bus 1H	480 V bus 1J
480 V MCC 1H1-1	480 V MCC 1J1-1
480 V MCC 1H1-2	480 V MCC 1J1-2
125 V DC Dist. Cabinet 1A	125 V DC Dist. Cabinet 1B

(a) 4160V Buses. The 4160 volt buses 1H and 1J are the sources of AC power for Train A and B respectively. Thus, if either of these buses is lost, all AC power to its associated train is also lost. Because of the importance of continuity of service, both these buses are provided with two sources of power: the offsite power source (the preferred source), and the onsite power source (the standby source provided by the diesel generator). In the event of trouble on the preferred source, the emergency source will start automatically and provide power to the affected 4160 volt bus. Each bus has a capacity of 3000 amperes and serves directly the ESF motors that are rated above 300 HP, and distributes power to the lower rated ESF loads via a station service transformer. These 4160 volt buses are normally isolated from each other; however, this isolation can be violated at cubicle 15H1 on 4160 volt bus 1H. This violation occurs when a normally removed bus tie breaker is inserted in the empty cubicle 15H1 and the tie breaker is closed. Such deliberate actions occur only for special maintenance conditions and would not, in themselves, cause the loss of 4160 volt power; however, the independence of the AC power distribution system would be compromised.

(b) <u>480V Load Centers</u>. The 480 volt emergency load center buses 1H and 1J are fed from 4160 volt buses 1H and 1J via 4160-480 volt station service transformers 1H and 1J, respectively. These buses are the main sources of power for the 480 volt trains; therefore, if either of these buses is lost, all 480 volt power to its associated train is also lost. These buses, like the 4160 volt buses, are equipped with drawout type circuit breakers, and serve directly several large ESF motors, and distribute power to the 480 volt motor control centers.

(c) <u>480V Motor Control Centers (MCC)</u>. Motor control centers MCC 1H1-1 and MCC 1J1-1 are energized by 480 volt buses 1H and 1J respectively. These MCCs provide power to motors much smaller than those served by 480 volt buses 1H and 1J, including auxiliary components associated with the larger loads served by 4160 and 480 volt buses 1H and 1J. Typical of the auxiliary loads served by these buses are cooling water pumps for the charging pumps and several valves associated with safety injection. In addition, each MCC distributes primary power to a 125 volt DC cabinet via two feeders, which serve two battery chargers, and to a 480-120 volt transformer to serve two 120 volt vital buses. Because the MCCs serve the relatively small 480 volt loads, they are equipped with combination starters (i.e., molded case breakers plus magnetic contractors) rather than with the larger drawout type circuit breakers. The combination starters provide overload protection by the contractors and short circuit protection by the circuit breakers. Motor control centers MCC 1H1-2 and 1J1-2 are essentially similar to MCC 1H1-1 and 1J1-1. That is, they are energized by 480 volt buses 1H and 1J, respectively, and distribute power via combination starters to the remaining 480 volt ESF loads. In other words, all the supporting 480 volt ESF loads are supplied by the combined distribution networks of MCC 1H1-1 and 1H1-2 (Train A auxiliary loads), or 1J1-1 and 1J1-2 (Train B auxiliary loads).

(d) <u>125VDC System</u>. The main power to the 125-volt DC Distribution Cabinets 1A and 1B is normally supplied from the AC power source by four battery chargers, two for each cabinet. The alignment of service is such that the two battery chargers that supply cabinet 1B are served by MCC 1J1-1 (Train B). Under normal conditions, the DC loads are actually served by the AC systems, and the batteries which are connected to these buses are on floating charge. Upon the loss of AC power, these DC buses are energized from their respective batteries, 1A or 1B.

The DC buses provide control and primary power to several ESF loads, including control power to operate the circuit breakers on 4160 and 480 volt buses 1H and 1J, and operating power for several solenoid valves and two 120 volt vital buses via inverters. These buses are normally isolated from each other; however, this isolation can be bypassed by the closing of a normally open bus tie breaker which places these two buses in parallel. This bus tie breaker can only be closed manually and is under administrative control to permit the sharing of load between buses during certain maintenance conditions such as repair or replacement of a battery charger.

(e) Protective Systems. The EPS is provided with (1) automatic protective devices including differential relays to protect major equipment such as the diesel generator and transformers, (2) undervoltage relays to ensure continuity of service by tripping the preferred source of power upon a low voltage condition, start the diesel generator, and transfer the load to the diesel generator, (3) instantaneous overcurrent relays to protect against short circuits, (4) and time delay relays (actually inverse time elements wherein the time to trip is inversely proportional to the fault current) to protect against equipment malfunctions such as a locked rotor condition or excess friction. The trip settings of the overcurrent relays are coordinated to minimize the effect of any failure of the overall power system. In other words, the breaker that feeds a faulted circuit would be the first to trip, thereby confining the loss of power to the affected feeder. Indicating devices in the form of alarms and annunciators are also provided. Thus, if the automatic devices should fail, the operator may be able to take appropriate action via the manual control devices located at the control room or at the breaker panels.

4.0 COMPARISON OF OCONEE AND SURRY EPS

A comparison of the Oconee and Surry designs produce the following characteristics:

1) The power rating of the Oconee emergency hydro units is much larger than the Surry emergency diesels (87.5 MW each vs. 2.75 MW each). Because of this, one Oconee hydro can power all ESF safeguards for all three Oconee units simultaneously, whereas at Surry, one diesel is dedicated to one train of ESF safeguards at one Surry unit.

2) The loading of the Surry diesel generators is such that they must assume full load within about 15 seconds after a LOCA and loss of offsite power. The inrush current challenges both diesel generators and is a common mode event that could cause both diesel generators to trip. The Oconee Keowee hydro units are sequentially loaded to prevent a large inrush current.

3) Oconee systems below the 4160 volt ES switchgear buses are similar to the Surry Unit 1 systems below the 4160 V ESF buses.

4) The two diesel generators providing emergency power for Surry are connected directly to the 4160V ESF emergency buses, whereas the various sources of emergency power for Oconee require the use of transformers and functioning 230 kV switchgear/ transmission line apparatus for preferred modes of powering the 4160 volt ES switchgear buses.

5) The EPS for Surry is onsite at the Surry Station and as noted in WASH-1400 does not make use of the high voltage switchgear (the offsite grid is considered down for the purpose of LOCA discussion). In contrast, the emergency power sources for Oconee require the use of the 230/500 kV switchyard equipment for preferred modes of operation and as described in the plant FSAR considers the availability of grid power.

6) The median estimate of insufficient power at LOCA as determined by the RSS for Surry is 1.0×10^{-5}. This number includes failure of Surry's EPS and the probability of a loss of offsite power at the time of the LOCA. The similar value for Oconee would be (5×10^{-4}, failure of Oconee EPS) x (1.0×10^{-3}, LOP at LOCA) = 5×10^{-7}.

5.0 OCONEE SYSTEMS EVALUATION

5.1 Event Tree Interrelationships

The EPS does not explicitly appear on the LOCA and transient event trees. For all sequences, except for those involving a loss of offsite power, AC power is assumed to be available from offsite power sources and the EPS is not required. For loss of offsite power sequences, and on particular LOCA sequences which cause a loss of offsite power, operation of the EPS is required. In order to identify station blackout sequences where the EPS fails after an LOP, an event B_3 will appear in parenthesis in the accident sequence. Therefore, the accident sequence $T_1(B_3)X$ is a loss of offsite power followed by a failure of the EPS and system X.

Since either Keowee hydro generator can power all the ESF safeguards for all three Oconee units, failure of the EPS is defined as the loss of both hydros.

5.2.2 EPS Unavailability

Sources of emergency power at Oconee are the emergency Keowee hydro generators and the Lee Steam Station. The preferred source of emergency power, as mentioned previously, originates from the hydros. Since the Lee Steam Station would not be available for at least 15 minutes after a startup command from the control room operator, it is conservatively assumed that it is not available in the short term as a power source in the event of simultaneous loss of both Keowee sources. Credit is given, however, to the long-term availability of the Lee Steam Station (i.e., greater than approximately 40 minutes).

The estimate of a hydro unit unavailability was derived from a combination of plant test data and expected maintenance outages. Since 1973, there have been 12 instances in which a single hydro generator or hydro generator circuit has failed to deliver power to the plant during a variety of hydro demands. There have been no instances in which both hydro generator circuits failed. The unavailability of a single hydro unit, based on this data, can therefore be estimated as

$$\left(\frac{12 \text{ failures}}{\sim 2000 \text{ hydro tests}}\right) = 6 \times 10^{-3} \quad .$$

The unavailability estimate of a single hydro unit given above does not include expected maintenance outages. Oconee technical specifications state that a hydro unit shall not be removed from service for more than 72 hours, after which the reactor will be shut down. The average maintenance interval used in the RSS is 4.5 months, which corresponds to a frequency of 0.22 per month. From the RSS, (Table III 5-3) the lognormal maintenance act duration for components whose range is limited to 72 hours is a mean time of 19 hours. The unavailability of one hydro unit due to maintenance is estimated to be:

$$\frac{19(.22)}{720} = 5.8 \times 10^{-3} \; .$$

In order to deliver the emergency power to the Oconee plant from the Keowee hydro station, two DC power systems are also required to operate. These are the 125-volt DC Keowee station power system (necessary for start-up and control of hydros) and the 125-volt DC switching power system (necessary to connect the EPS to the Oconee plant). A detailed discussion of these systems can be found in Appendix B2. The unavailability estimate for these DC systems is taken from that appendix as 4×10^{-4} and ϵ, respectively

The unavailability of the EPS is therefore estimated as

$$\begin{aligned} Q(EPS) &= 2(5.8 \times 10^{-3})(6 \times 10^{-3}) + (6 \times 10^{-3})^2 + 4 \times 10^{-4} \\ &= 5 \times 10^{-4} \; . \end{aligned}$$

This value represents event B_3 in the Boolean equations.

The unavailability of AC power in the short term (i.e., less than approximately 40 minutes) given the loss of both the hydro generators is dominated by the failure to restore offsite AC power. This is taken from WASH-1400 as 2×10^{-1} and is known as LOPNRE in the Boolean equations.

The unavailability of AC power in the long term was assessed to be dominated by the common mode failure of the Oconee operator to notify Lee Station personnel and manually restore offsite power. This failure probability is estimated as

$$\begin{aligned} Q(\text{AC power with 40 minutes to 3 hours}) &= 3 \times 10^{-3})(5) \\ &= 1.5 \times 10^{-2} \; . \end{aligned}$$

The value 3×10^{-3} is the basic human error of omission. This value is increased by a factor of 5 to reflect a moderately high stress situation (Reference NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications). This value represents event LOPNRL in the Boolean equations.

It should be noted that failures of electric power system components that supply power to particular ESF systems and components (e.g., a particular bus in the plant distribution system) were not considered. The reasons for taking this approach are the following:

1) As mentioned previously, it was assumed that AC power was available to the plant distribution system prior to the transient or LOCA initiator. By making this assumption, the probability of losing a particular portion of the plant distribution system (e.g., 4160 V bus, etc.) during the first 24 hours following the initiator is negligible.

2) Due to the Keowee hydro power and Lee combustion turbine rating and bus inter-ties at Oconee, either hydro or combustion turbine can power all ESF loads simultaneously. Since a particular hydro or combustion turbine is not dedicated to particular ESF loads, both hydros or combustion turbines can be considered to operate as a single unit.

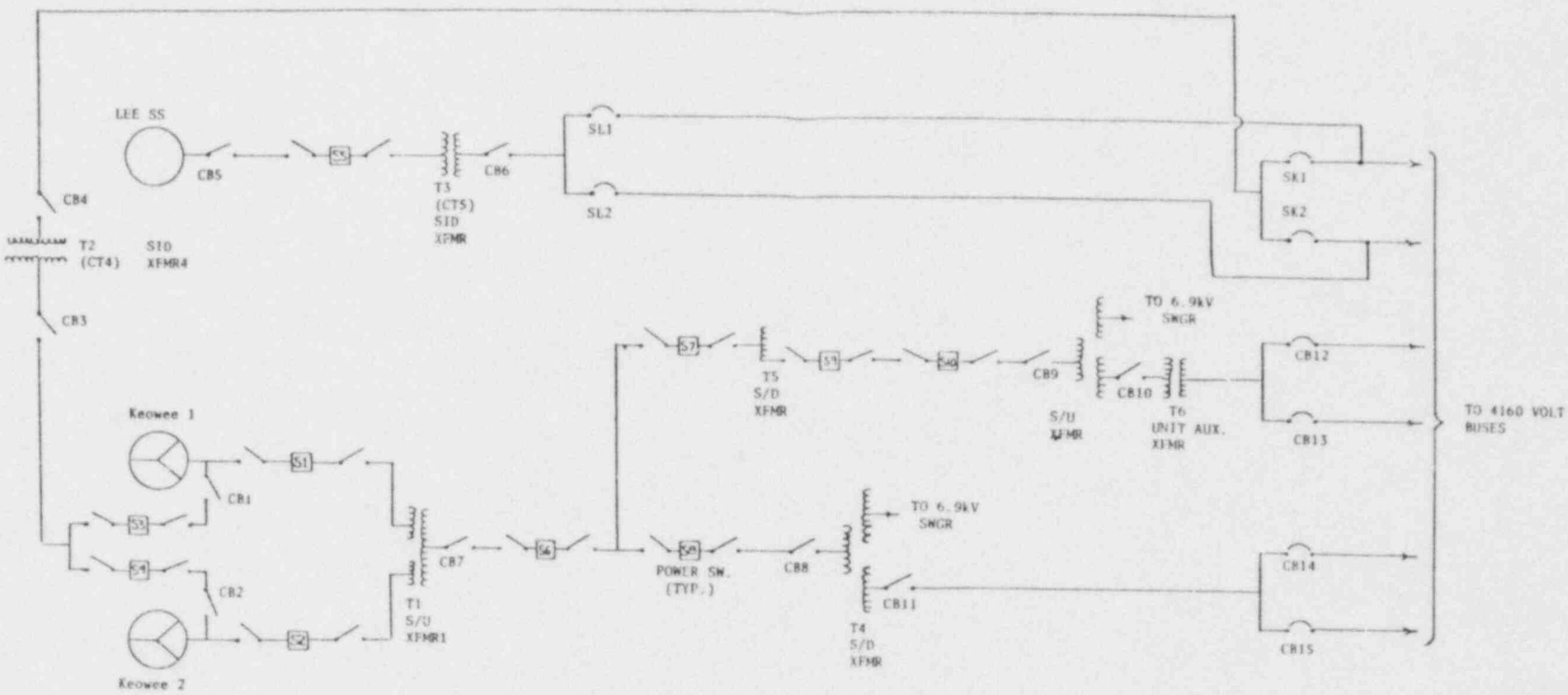


Figure B1-1. Oconee Emergency AC Power System

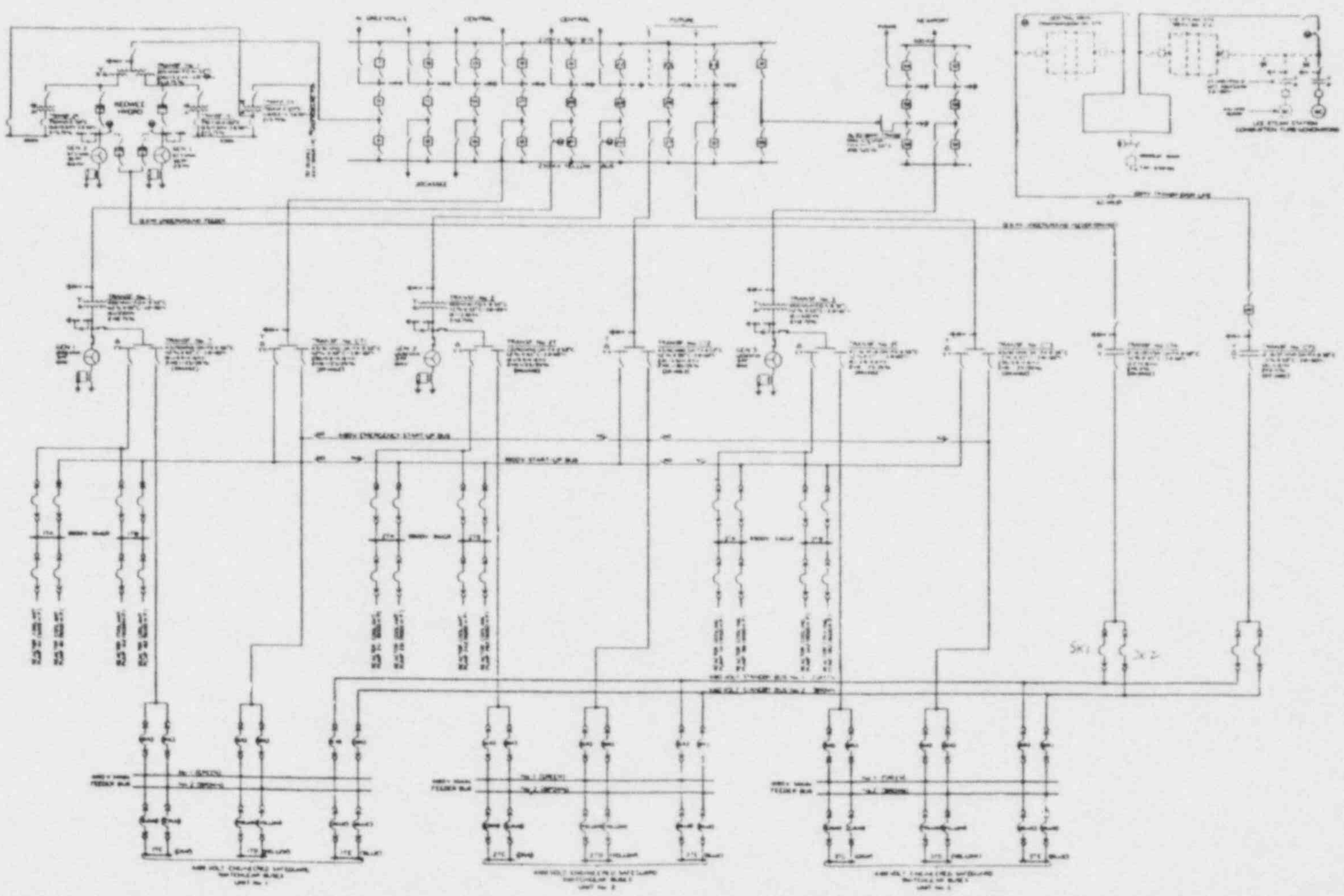


Figure B1-2. Oconee AC Power Distribution System

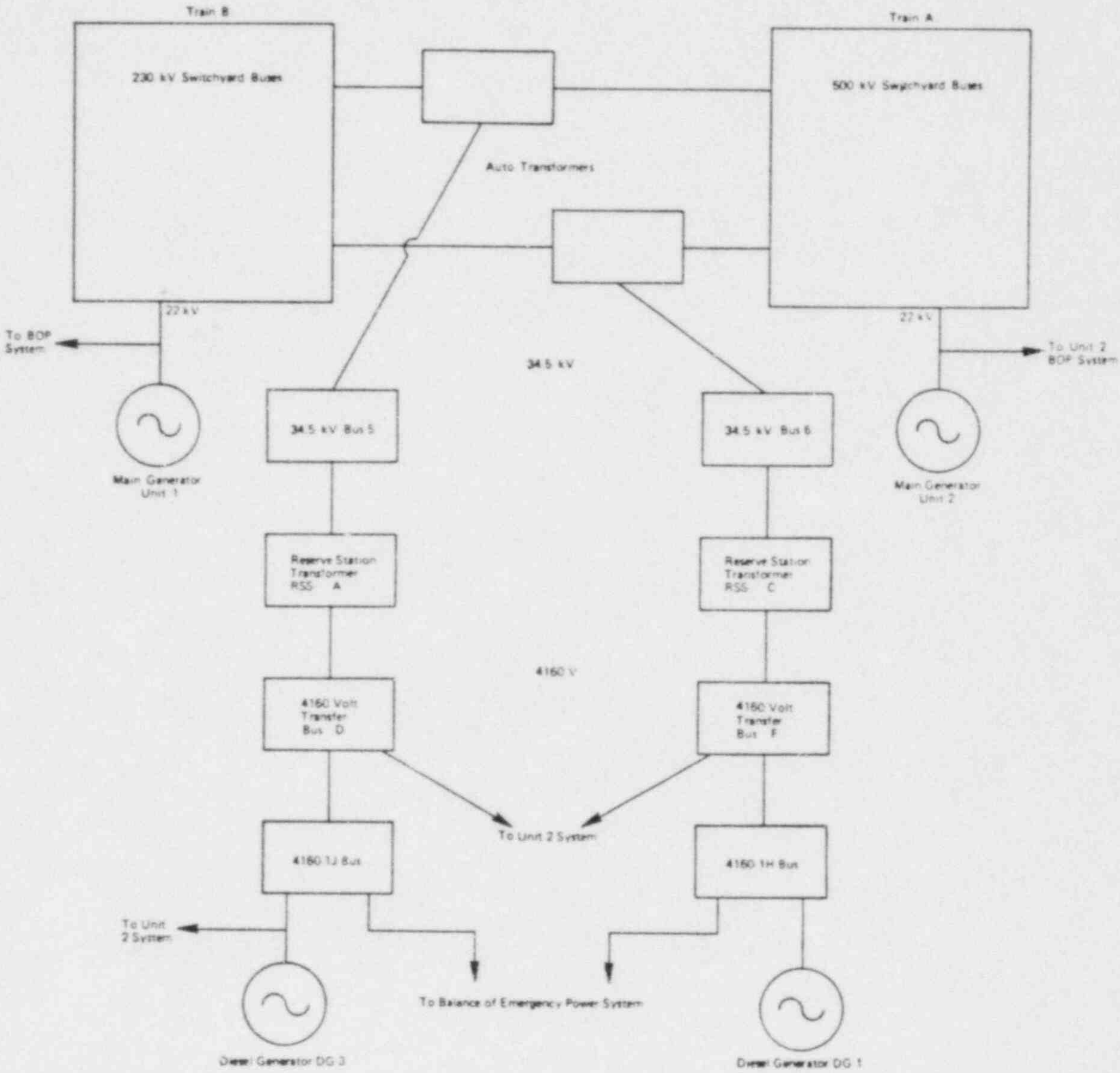


Figure B1-3. Simplified Surry Emergency Power Block Diagram

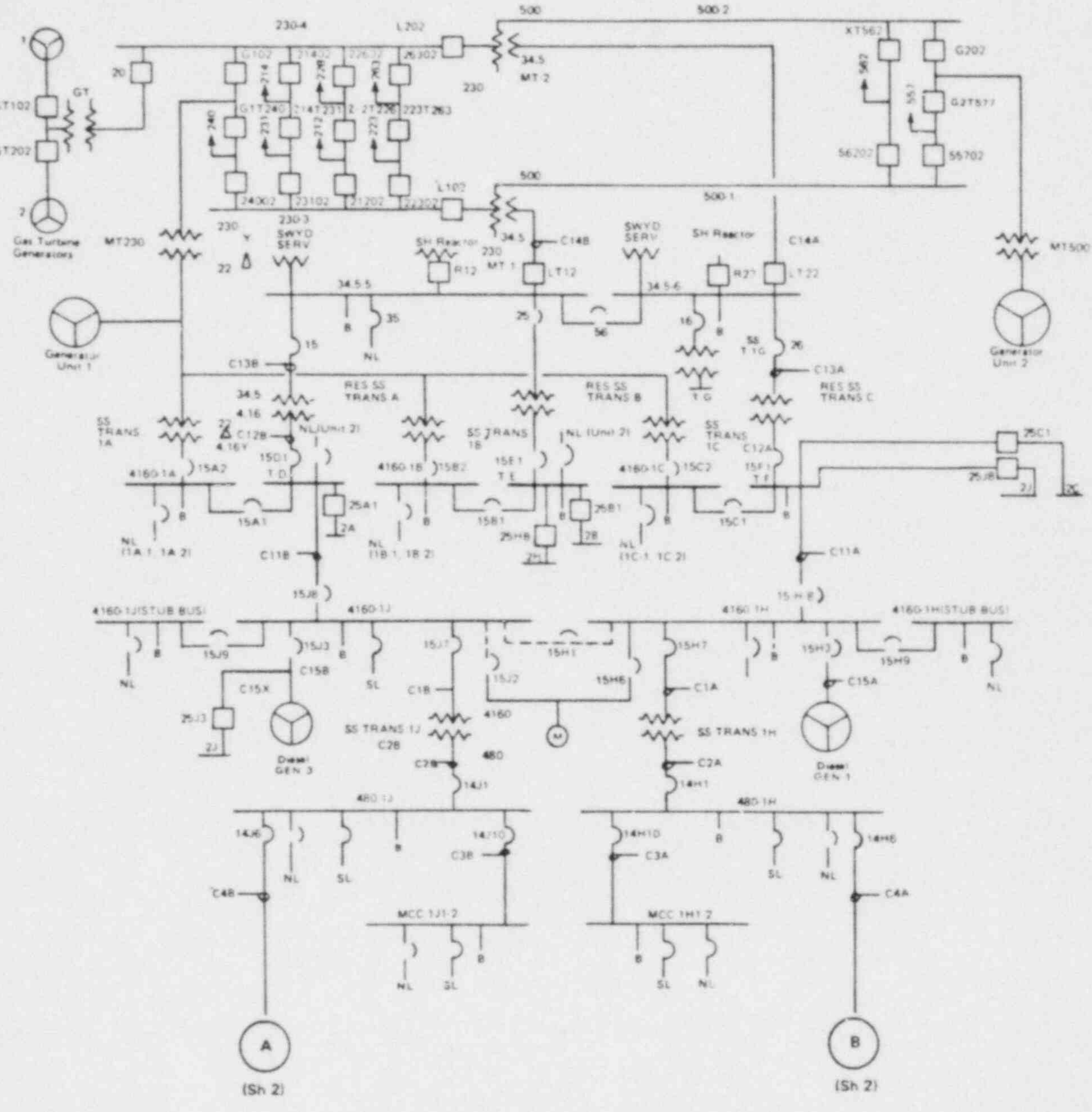


Figure B1-4. Surry Single Line EPS Diagram

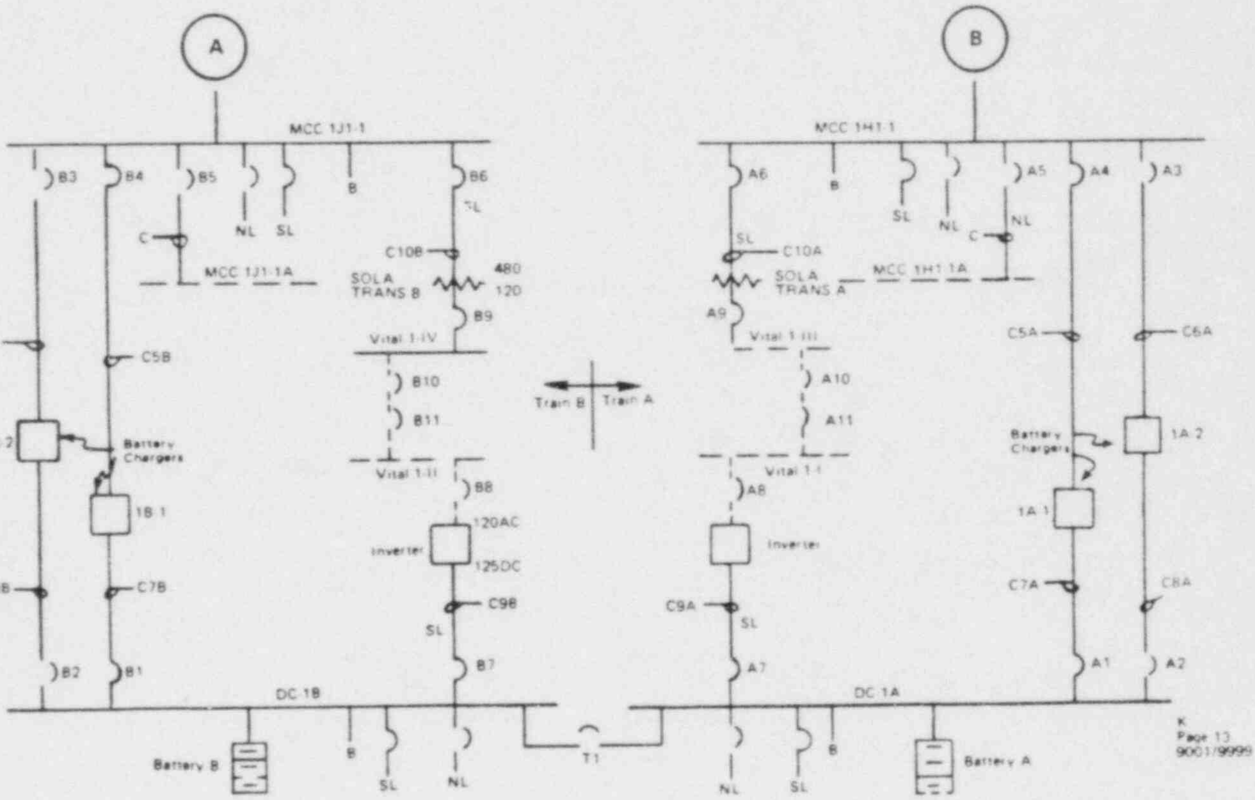


Figure B1-5. Surry Single Line EPS Diagram (cont'd)

APPENDIX B2

SURVEY AND ANALYSIS

DC POWER SYSTEM (DCPS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 DC Power System (DCPS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The system designs for Oconee and Surry are described in Sections 2 and 3 of this report, respectively. A comparison of the two systems is given in Section 4. LPSWS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a estimate of the DCPS unavailability.

2.0 OCONEE DCPS DESCRIPTION

2.1 System Description

The Oconee DC power system is composed of three safety related DC power subsystems. In all three systems the normal supply of DC load current is from an associated battery charger which maintains the appropriate floating voltage on the battery board, supplying the normal and emergency plant load demand while maintaining the battery in a fully charged state for potential loss of AC power operation.

The three safety related DC power systems are:

- The 125-volt DC instrumentation and control (I&C) power system
- The 125-volt DC switching power system
- The 125-volt DC Keowee Station Power System

The 125-volt DC I&C power system supplies vital DC and AC (through inverters) power to reactor instrumentation and protective control systems and is shown in Figure B2-1. For each unit, two independent and physically separated 125-volt DC batteries and DC buses are provided for the vital instrumentation and control power system. The DC buses are two conductor metalclad distribution center assemblies. Three battery chargers are also supplied with two serving as normal supplies to the bus sections with the associated 125-volt DC battery floating on the bus. The batteries supply the load without interruption should the battery chargers or the AC source fail. Each of the three battery chargers are supplied from the redundant 600-volt AC engineered safeguards motor control centers of each unit. One of these three battery chargers serves as a standby battery charger and is provided for servicing and to back up the normal power supply chargers. A bus tie with normally open breakers is provided between each pair of DC bus sections to back up a battery when it is removed for servicing.

Four separate 125-volt DC instrumentation and control panelboards are also provided for each unit. Each panelboard receives its DC power through an auctioneering network of two isolating diode assemblies. One assembly is connected to the unit 3 125-volt distribution system. The functions of the diode assemblies are to discriminate between the voltage level of the two DC distribution systems, pass current from the DC system of higher potential to the instrumentation and control panelboard connected on the output of the diode assemblies, and block the flow of current from one DC distribution system to the other. It was learned from plant personnel that this intertie requires operator action.

Each isolating diode assembly is composed of a series-parallel network of four diodes in each polarity leg of the DC supply to the panelboard it serves. With this series-parallel arrangement of diodes, either an open circuited or short circuited diode can be tolerated without affecting the operability of the diode assembly. The individual diodes are sized for a continuous current of 500 amperes with the maximum panelboard load current being 304 amps. Each diode is also rated for continuous operation with a peak inverse voltage of 800-volts.

The 125-volt DC I&C power system batteries are physically located in separate enclosures to minimize damage exposure. The battery chargers and associated DC bus sections and switchgear are also located in separate rooms and physical separation is maintained between all redundant equipment and cabling.

The 125-volt DC switching power system is shown in Figure B2-2 and consists of two 125-volt DC, two conductor, metalclad distribution center assemblies, three battery chargers, and two 125-volt DC batteries. A bus tie with breakers is provided between the switchgear bus sections to back up a battery when it is removed for servicing. One standby 125-volt DC battery charger is also provided between the two 125-volt DC batteries for servicing. One battery supplies power through panelboards for primary control and protective relaying. Dual feeds from the redundant panelboards are provided to each Power Circuit Breaker (PCB) for closing and tripping control. Separate dual trip coils are provided for each PCB. Isolating diodes are provided for the redundant power feeds to the common closing coil circuit. This system provides critical power for monitoring of the protective relaying, isolating and switching between alternate off-site net power supply systems and the on-site emergency AC power supply system for all three of the Oconee nuclear units during normal or emergency operations.

The 125-volt DC Keowee Station Power System, shown in Figure B2-3, provides the necessary power to automatically or manually start, control and protect the two Keowee hydroelectric power units which, although independent power generation systems, are the primary source of on-site emergency power for the Oconee nuclear plant. As shown in Figure B2-3 for each Keowee hydro unit a separate 125-volt DC power system is supplied. Each system consists of one 125-volt DC power supply battery charger, one 125-volt DC two conductor, metalclad distribution center assembly and one 125-volt DC battery. A bus tie with normally open double circuit breakers is provided between the switchgear bus sections to back up a battery when it is removed for servicing. One standby 125-volt DC battery charger is also provided between the two 125-volt DC batteries for servicing. The batteries, battery charger and distribution center associated with one unit are physically separated in separate enclosures from those associated with the other unit.

Each of the above three safety related DC power systems will provide uninterrupted battery supplied power to its connected loads in the event of loss of all AC power. The design of each system is based on redundancy in that a single failure of any component, passive or active, will not preclude the system from supplying emergency power when required.

Test provisions are included in each isolating diode assembly to allow the in-service checking of the operability of individual diode monitors, and, in addition, to allow the out-of-service periodic checking of the peak inverse voltage capability of each individual diode. The latter test can be conducted on one isolating diode assembly with the other diode assembly in the network in operation. Breakers on the input and output of each isolating diode assembly are provided for complete isolation during maintenance and testing of an assembly.

The batteries are given the following tests and inspection:

a) The voltage and temperature of a pilot cell in each battery is measured and recorded five times per week for the Instrument and Control, Keowee Hydro, and Switching Station batteries.

b) The specific gravity and voltage of each cell is measured and recorded monthly for the Instrument and Control, Keowee Hydro, and Switching Station batteries.

c) Annually, a one-hour discharge test at the required maximum safeguards load is made on the Instrument and Control batteries.

d) Annually, a one-hour discharge test is made on the Keowee Hydro and Switching Station batteries.

The operability of the individual diode monitors in the Instrument and Control and Keowee Station 125 VDC systems is verified monthly by imposing a simulated diode failure signal on the monitor.

The peak inverse voltage capability of each auctioneering diode in the Instrument and Control, Switchyard and Keowee Hydro 125 VDC system is measured and recorded semi-annually.

The tests specified above are considered satisfactory if control room indication and/or visual examination demonstrates that all components have operated properly.

2.2 System Operation

The DC power for each of the three safety related DC power systems is supplied by the appropriate battery charger from its connected 600-volt AC motor control or 480-volt AC switchyard load center during normal plant power operation. In the event of a loss of all AC power the connected floating batteries continue to supply uninterrupted DC and vital AC power (through inverters) to all connected loads for at least one hour to provide vital plant instrumentation and control power, switching power and Keowee start-up and control power for safe reactor shutdown and implementation of emergency on-site AC power generation.

All of the safety related DC power system equipment is monitored and alarmed locally and/or in the main control room. Specific variables being monitored locally with composite alarms in the main control room are system ground, charger operation, circuit breaker positions, diode operation, and bus voltage. The DC bus tie breakers, battery and standby charger circuit breakers and standby charger operation are monitored directly in the control room.

Continuous monitoring of each diode is provided in the design of each isolating diode assembly to detect a shorted or open circuited diode. An alarm relay, connected to an individual control room annunciator point, is provided in each isolating diode assembly to advise the operator of diode trouble in the assembly.

3.0 SURRY DCPS DESCRIPTION

The Surry plant design incorporates two class 1E safety related DC power supply systems plus a series of locally situated self contained battery-powered emergency lighting units for remote areas. A separate independent 125-volt DC power supply system, composed of a battery charger, battery and distribution system is associated with each of the three diesel generator emergency on-site power generation units. This critical system provides power for start-up, monitoring, protection, and control of the on-site emergency AC power system.

The second safety related system is the 125-volt DC vital power system, shown in Figure B2-4 which is composed of two identical redundant service channels for each nuclear unit, each channel containing a battery, two parallel static battery chargers, ungrounded distribution bus and cabling to the remote DC loads. Each channel supplies 125-volt DC power for high voltage switchgear control, turbine bearing and seal oil pump motors, and solenoid valve operating power during normal plant power operation. During loss of AC power emergency operation the pump motor loads are shed and the system supplies un-interrupted battery power for the high voltage switchgear and solenoid valves and picks up emergency lighting for the reactor containment, turbine room and other selected building areas and provides power to the vital inverters for supplying critical AC reactor protection and instrumentation loads to the associated nuclear unit.

The two vital DC channels for each nuclear unit are physically and electrically independent from the battery to each of the remote AC and DC load points. Vital safety loads are redundant on each channel and a manually controlled tie breaker provides a load sharing capability between the DC buses. During normal operation the 125-volt DC load for each channel is fed from the battery chargers, powered by the 480-volt AC emergency buses, with the batteries floating on the system. Upon loss of off-site AC power, the batteries automatically pick up the connected load. The batteries are designed for two hour continuous operation and successful operation of any one of the two redundant vital 125-volt DC systems will insure safe shutdown of the associated nuclear unit with no accompanying accident or auxiliary feedwater system failure. Because of the plant diesel generator sharing design, recovery of AC power by the emergency diesel generators requires successful operation of two of the three diesel generator 125-volt DC power supply systems for either single unit or total plant AC supply.

Both safety related DC systems are fully monitored with voltmeters, ammeters and ground detectors and protected by fuses and circuit breakers which are appropriately displayed and alarmed in the main control room. A program of regular inspection and test of all batteries is in effect and automatic starting and loading of the emergency generators is periodically tested which exercise the related DC power supply.

4.0 COMPARISON OF OCONEE AND SURRY DCPS

The DCPS at both plants include a 125-volt DC power subsystem for instrumentation, on-site switching, and executive protection and control as well as separate 125-volt DC power subsystems for emergency on-site power generation control. The Oconee plant also includes an additional separate safety related 125-volt DC power subsystem for high voltage power switching among the alternate off-site network supply sources and the emergency on-site AC hydro power generation source. All of these 125-volt DC power subsystems are similarly powered by battery chargers, which are supplied by the normal AC power source, and maintain a floating charge on a connected battery for emergency supply of uninterrupted power in event of a loss of normal AC service.

Oconee's design does not require load shedding for the 125-volt instrumentation and control subsystem; Surry's design requires shedding of the main turbine generator bearing and seal oil pumps after the turbine has coasted to a stop. If a loss of all AC power should occur, the Oconee instrumentation and control subsystem is designed to supply emergency loads for one hour while Surry is designed for two.

Based on the technique used for estimating DC system unavailability in the RSS, the Oconee and Surry DCPS have a similar unavailability estimate. However, a recent Sandia National Laboratories DC power system (Reference 3) study identified a DC common mode failure not previously identified in the RSS. This failure is attributed to the miscalibration of the battery charger charging rate which causes the batteries to degrade and fail upon demand following a loss of off-site power. This common mode was judged to be applicable to the Oconee emergency on-site power control 125-volt DC subsystem. The unavailability estimate for this subsystem is greater than two orders of magnitude higher than would have been estimated using the RSS method.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The DCPS does not appear as an explicit event on the LOCA and transient event trees. For loss of off-site power sequences (T_1), the Keowee 125-volt DC subsystem contributes to the unavailability estimate of the Keowee emergency AC power system (event (B_3)). For all other sequences DC power is assumed to be available (see Section 5.2, case 1).

5.2 DCPS Unavailability

The point estimates for the unavailability of the Oconee DCPS were developed for two cases; i.e., 1) AC power available and 2) AC power unavailable.

Case 1 - AC power available.

> With AC power available, both I&C batteries and/or both I&C battery chargers are capable of supplying the necessary DC power. The unavailability of the I&C DCPS for a single Oconee unit was estimated as:

$$Q(\text{I\&C DCPS}) = Q(\text{Both I\&C batteries}).\ Q^2(\text{I\&C Charger})^{1} = \varepsilon$$

Case 2 - AC power unavailable.

> Following a loss of off-site power success of the Keowee DCPS and switching DCPS is required to connect the Oconee plant to the emergency AC hydroelectric power system. The unavailability of these DC power systems therefore contribute to unavailability of the emergency AC power system. The unavailabilities of these two DCPS were estimated as:

---

[1] The form of this equation suggests that the batteries and chargers are independent means of supplying DC power. This may not be entirely correct. While it is true that a battery can supply DC power without the successful operation of its corresponding battery charger, the converse situation may not be true (i.e. battery chargers are designed for steady state operation and may not be able to supply DC load demands which are usually accomodated by the batteries). For this assessment, however, it was assumed that a battery charger could supply DC power without the successful operation of its corresponding battery.

$$Q(\text{Keowee DCPS}) = Q(\text{Both Keowee batteries}) = 4 \times 10^{-4}/\text{reactor year}$$

$$Q(\text{Switching DCPS}) = Q(\text{Both Switching batteries}).Q^2(\text{Switching Charger})$$
$$= \varepsilon$$

These unavailabilities were input to the unavailability estimate of the emergency AC hydroelectric power system (see Appendix B1).

The failure of "both Keowee batteries" unavailability estimate was based on insights gained from a Sandia National Laboratories DC power system study. The dominant contributor to the unavailability is due to a common mode failure. This failure is attributed to the miscalibration of the charging rate on both Keowee battery chargers. This human error would cause both batteries to degrade and fail upon demand (Reference 3).

It should be noted that an unavailability estimate of the I&C DCPS was not made for case 2. This is because the Oconee plant, as analyzed, is AC dependent (e.g. ECCS and emergency feedwater system require AC power to successfully operate).

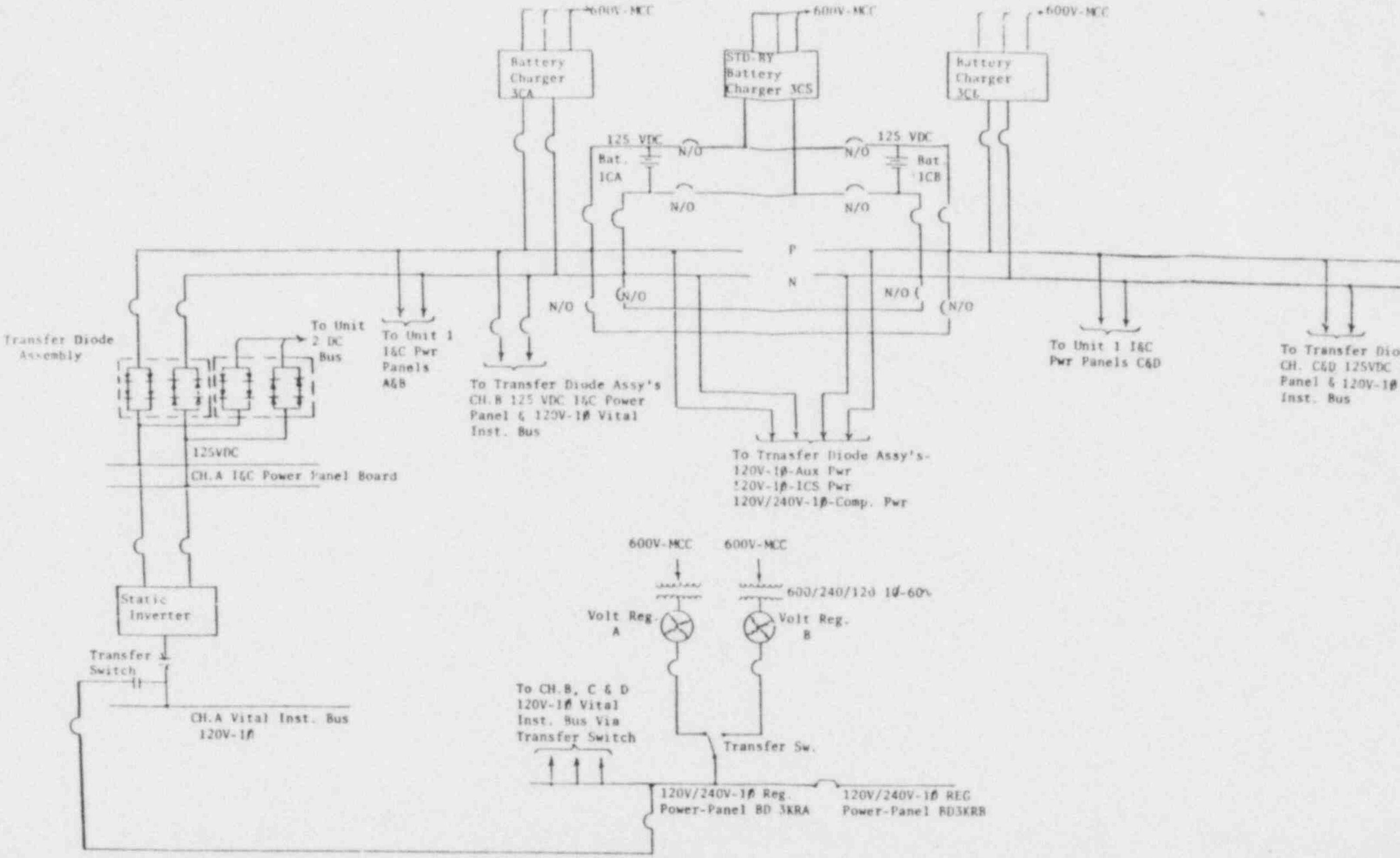


Figure B2-1. Oconee 125-volt DC Instrumentation and Control Power System (One of Three Units Shown)

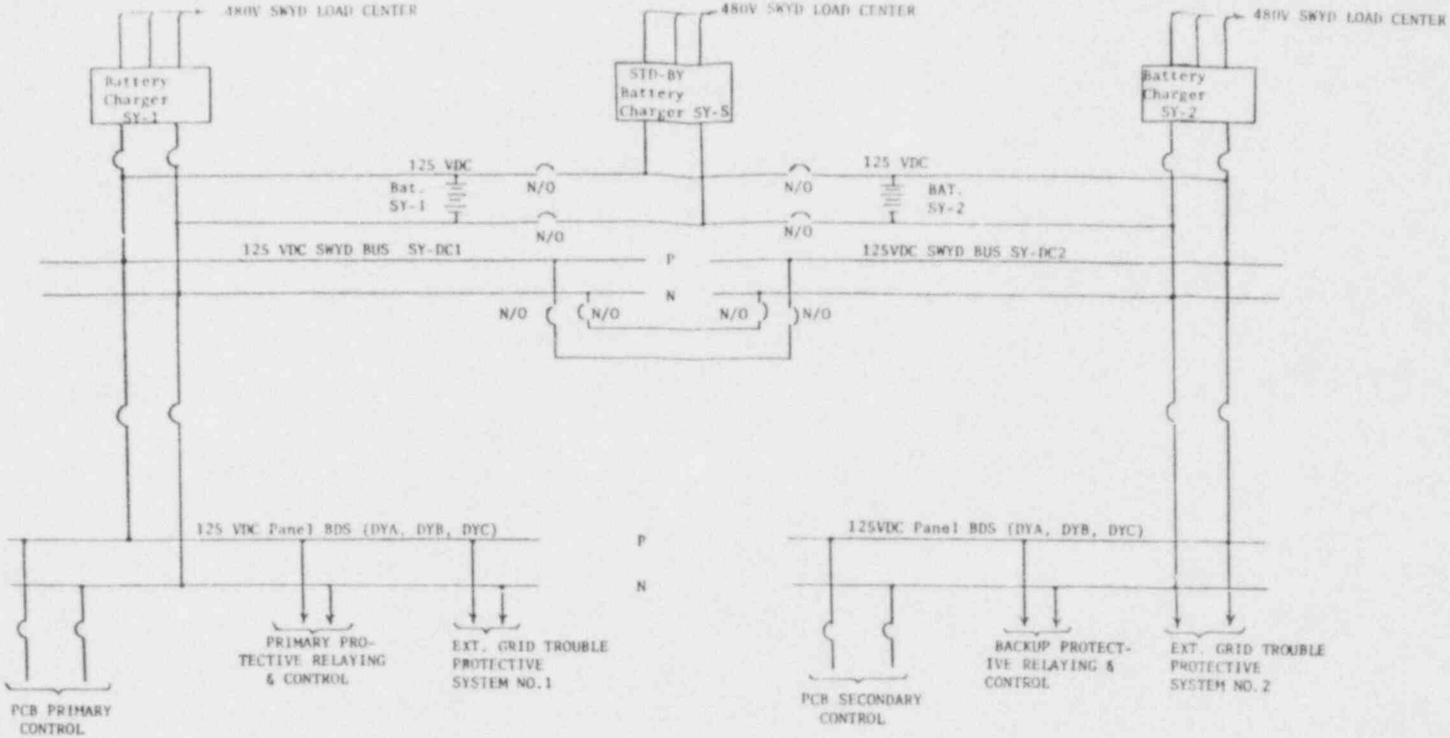


Figure B2-2. Oconee 125-volt DC Switching Power System

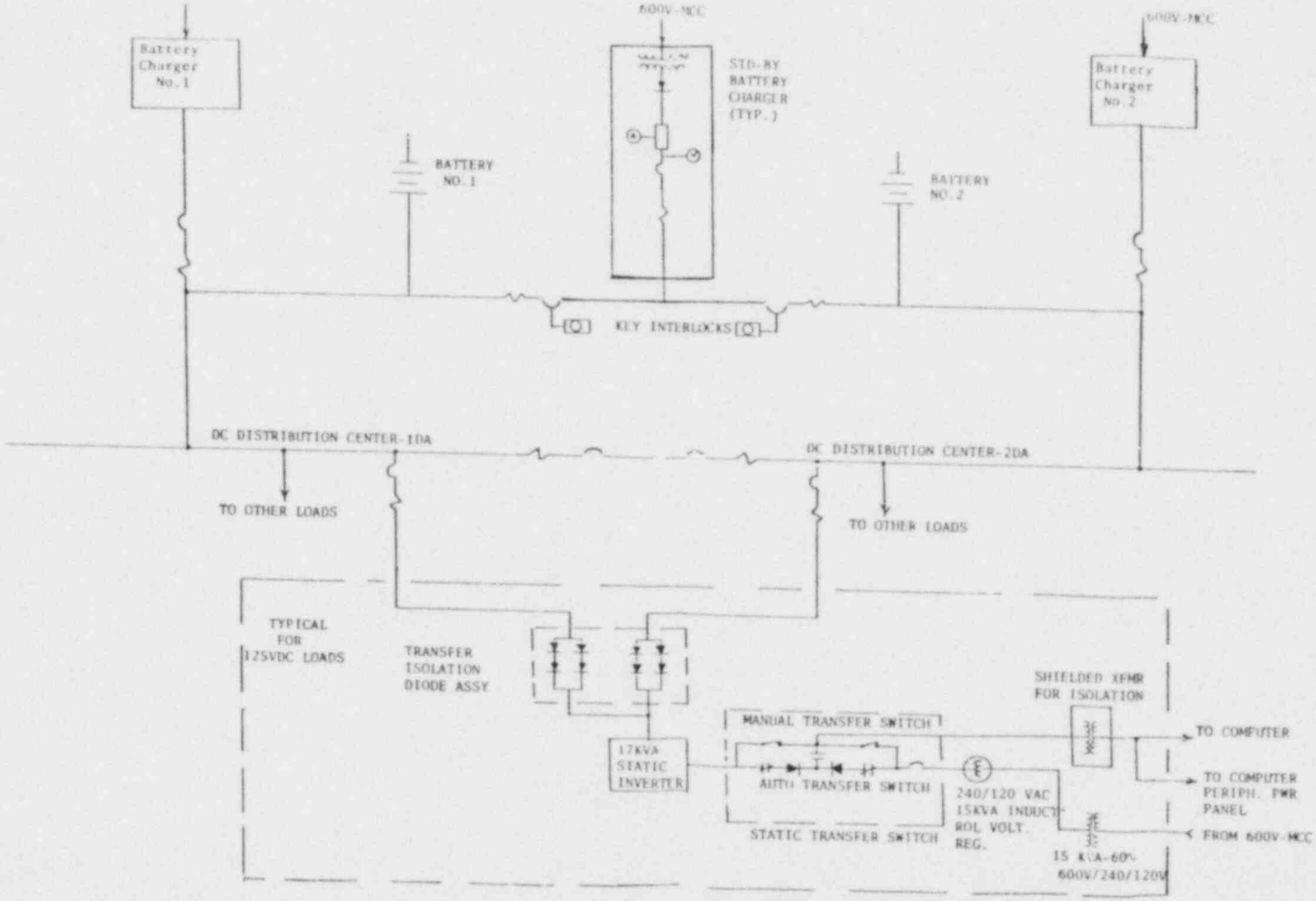


Figure B2-3. Oconee 125-volt DC Keowee Power System

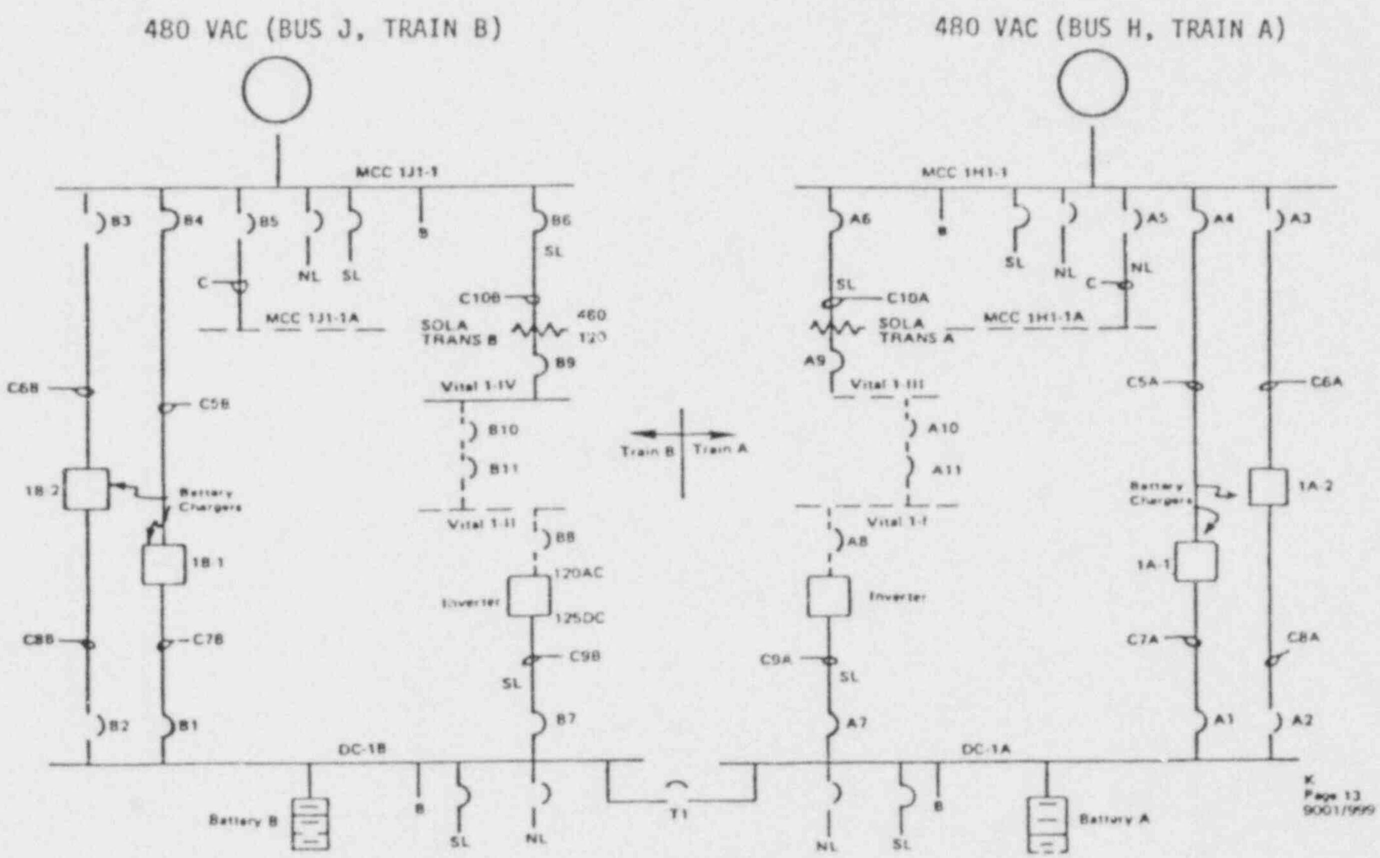


Figure B2-4. Surry DC Power System

APPENDIX B3

SURVEY AND ANALYSIS

REACTOR PROTECTION SYSTEM (RPS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Reactor Protection System (RPS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The RPS designs for Oconee and Surry are described in Section 2 and 3 of this report respectively. A comparison of the two reactor protection systems is given in Section 4. RPS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the reduced RPS fault tree model and a point estimate of the system unavailability.

2.0 OCONEE RPS DESCRIPTION

2.1 System Description

The RPS consists of control rod assemblies (CRA), circuit breakers, instrumentation and electronic logic. The logic, in response to input signals from the instrumentation, shuts down the reactor by removing power from the CRAs which then drop into the core under the influence of gravity.

There are a total of 69 CRAs, arranged in eight groups including four safety groups, three regulating groups and one axial power shaping group. The rod drive control system includes (1) five identical, dual channel DC supplies which power the regulating and axial power shaping groups and (2) two DC holding power supplies which power the safety groups. The DC supplies are fed from two 480 VAC, 3ϕ sources; i.e., a main bus and a secondary bus. Two primary breakers (A, B), two secondary breakers (C, D), and contactors (E, F), interrupt power to the CRA drive motors when a trip is commanded.

The trip logic includes four identical channels, each consisting of logic circuits and trip relays, which maintain the trip breakers and contactors energized under normal operating conditions. In response to input signals from sensors (See Table B3-1), the channel logic deenergizes associated trip relays which in turn deenergize the trip breakers and contactors thereby removing power to the CRAs and causing the regulating and safety CRAs (61) to drop into the core. The axial power shaping rods do not drop into the core when their associated drive motors are deenergized.

2.1.1 Control Rod Assembly

The CRA includes 16 control rods, mounted in a stainless-steel spider, and a control rod drive mechanism (CRDM). The CRDM, which positions the CRA in the reactor core, is a non-rotating translating lead screw coupled to the CRA. The screw is driven by split roller nut assemblies which are rotated magnetically by a motor stator located outside the pressure boundry. For rapid insertion, power is removed from the drive motor causing the nut halves to separate and release the screw and CRA which then drop into the reactor core under the influence of gravity.

The CRA are arranged into groups at the control rod drive control system patch panel. Typically twenty-eight CRA are assigned to the regulating groups (groups 5, 6, 7, 8) while forty-one CRA are assigned to the safety rod groups (groups 1, 2, 3, 4). Group 8 includes eight axial power shaping rod assemblies which do not drop into the core when power is removed from their drive motors during a reactor trip.

The rod drive control system, which is shown in Figure B3-1, consists of (1) drive motor DC power supplies, (2) system control logic, and (3) trip breakers and contactors. The DC power system includes four group power supplies. Identical power supplies (redundant half-wave rectifier design) are used for the regulating groups and the auxiliary power supply. The DC power supplies are fed from two 480 VAC, 3 ϕ sources; i.e., a main bus and a secondary bus.

The system logic encompasses those functions which command control rod motion in the manual or automatic modes of operation, including CRD sequencing, safety and protection features, and the manual trip function. Major components of the logic system are the Operator's Control Panel, CRA position indication panels, automatic sequencer, and relay logic. Switches are provided at the operators control panel for selection of the desired rod control mode. Control modes are: (1) Automatic mode -- where CRA motion is commanded by an integrated control system; and (2) Manual mode -- where CRA motion is commanded by the operator. Manual control permits operation of a single CRA or a group of CRA. Alarm lamps on the RDC panel alert the operator to the systems status at all times. The group 8 control rods can only be controlled manually even when the remainder of the system is in automatic control. The sequence section of the logic system utilizes rod position signals to generate control interlocks which regulate group withdrawal and insertion. The sequencer operates in both automatic and manual modes of reactor control, and controls the regulating groups only. Analog position signals are generated by the reed switch matrix on the CRA, and an average group position is generated by an averaging network. This average signal serves as an input to electronic grip units which are activated at approximately 25 and at 75 per cent of group withdrawal. Two bistable units are provided for each regulating group. Outputs of these bistables actuate "enable" relays which permit the groups to be commanded in automatic or manual mode. The automatic sequencer circuit can control only CRA groups 5, 6 and 7. The safety CRA groups, groups 1-4, are controlled manually, one group at a time. In addition, the operator must select the safety group to be controlled and transfer it to the auxiliary power supply before control is possible. The automatic sequencer cannot affect the operations required to move the safety CRA. Automatic insertion of rods can only be commanded by the integrated control system when the control rod drive system is in the automatic mode.

Positioning of regulating CRA is accomplished by SCR switching via a motor driven multichannel photo-optic encoder. The safety CRA are positioned via the auxiliary power supply and maintained in the desired position by the holding power supplies.

Trip breakers and contactors are provided for removing power to the CRDM motors. The AC power feed breakers are of the three-pole, stored-energy type and are equipped with instantaneous undervoltage trip coils. Each AC feed breaker is housed in a separate metal clad enclosure. The secondary trip breakers are also of the stored-energy type with two parallel-connected instantaneous undervoltage trip coils consisting of two 2-pole breakers mechanically ganged to interrupt DC busses. All breakers are motor-driven-reset to provide remote reset capability. Each undervoltage trip coil is operated from the Reactor Protection System. The trip breakers are tested monthly.

2.1.2 Trip Logic

The Reactor Protection Logic System consists of four identical channels, each terminating in a trip relay within a rector trip module. The primary source of AC power for the RPS comes from four vital 120 VAC busses, one for each protective channel. In the normal untripped state, each channel maintains the trip relay energized via the closed normally open (N/O) contacts of bistables associated with the various reactor sensors. Should any bistable become deenergized the trip relay deenergizes. Each trip relay has four N/O contacts, each controlling a logic relay in one reactor trip module. Therefore, each reactor trip module has four logic relays controlled by the four channels. The four logic relays combine to form a 2-out-of-4 coincidence network in each reactor trip module.

Manual trip may be accomplished from the control console by a trip switch. This trip is independent of the automatic trip system. Power from the control rod drive power breakers' undervoltage coils comes from the RT modules. The manual trip switches are between the reactor trip module output and the breaker undervoltage coils. Opening of the switches opens the lines to the breakers, tripping them. There is a separate switch in series with the output of each reactor trip module. All switches are actuated through a mechanical linkage from a single pushbutton.

Each channel is provided with two key-operated bypass switches, a channel bypass switch and a shutdown bypass switch.

The channel bypass switch enables a channel to be bypassed without initiating a trip. Actuation of the switch initiates a visual alarm on the main console which remains in effect during any channel bypass. The key switch will be used to bypass one protective channel during on-line testing. Thus, during on-line testing the system will operate in 2-out-of-3 coincidences. The use of the channel bypass key switch is under administrative control. The shutdown bypass switch enables the power/imbalance/flow, power/RC pumps, low pressure, and pressure-temperature trips to be bypassed allowing control rod drive tests to be performed after the reactor has been shutdown and depressurized below the low reactor coolant pressure trip point. Before the bypass may be initiated, a high pressure trip bistable - which is incorporated in the shutdown bypass circuitry - must be manually reset. The set point of the high pressure bistable (associated with shutdown bypass) is set below the low pressure trip point. If pressure is increased with the bypass initiated, the channel will trip when the high pressure bistable (associated with shutdown bypass) trips. The use of the shutdown bypass key switch is under administrative control.

Each of the four channels are physically separate and are electrically isolated from the regulating instrumentation. The modules, logic, and analog equipment associated with a single protective channel are contained wholly within two Reactor Protective System cabinets. Within these cabinets, there is a meter for every analog signal employed by the protective channel, and a visual indication of the state of every logic element.

At the top of one cabinet, and visible at all times, is a protective channel status panel. Lamps on this panel give a quick visual indication of the trip status of the particular protective channel and of the RT module associated with it. Additional lamps on the panel give visual indication of a channel bypass or a fan failure.

The RPS equipment is designed for continuous operation in a room environment of $40^{O}F$ to $110^{O}F$ and up to 75% relative humidity. All modules are designed for a $30^{O}F$ temperature rise inside the equipment cabinets over the ambient room conditions. Two 100% capacity central station type chilled water systems, and two 50% capacity outside air booster fans are provided for environmental control of the equipment area.

2.2 System Operation

The coincidence logic contained in the RPS channel A controls trip breaker A in the control rod drive system, channel B controls breaker B, channel C controls breaker C and contactor E, and channel D controls breaker D and contactor F. The control rod drive circuit breaker combinations that initiate reactor trip include (1) AB, (2) ADF, (3) BCE, and (4) CDEF. This is a 1-out-of-2 twice logic. When any 2-out-of-4 channels trip, all reactor trip modules trip (deenergize) all control rod drive breakers and contactors. The four RPS channel trip whenever the reactor conditions tabulated in Table B3-1 exist.

The use of 2-out-of-4 logic between protective channels permits a channel to be tested on-line without initiating a reactor trip. Maintenance to the extent of removing and replacing any module within a protective channel may also be accomplished in the on-line state without a reactor trip. Each logic channel is tested monthly. The RPS sensors are checked during each shift and are tested monthly. To prevent either the on-line testing or maintenance features from creating a means for unintentionally negating protective action, a system of interlocks initiates a protective channel trip whenever a module is placed in the test mode or is removed from the system. However, provisions are made in each protective channel to supply an input signal which leaves the channel in a non-tripped condition for testing or maintenance. The test scheme for the reactor protective system is based upon the use of comparative measurements between like variables in the four protective channels, and the substitution of externally introduced digital and analog signals as required, together with measurements of actual protective function trip points. A digital voltmeter is provided for making accurate measurements of trip point and analog signal voltages.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the reactor protective system. The following conditions are annunciated for each reactor protective system channel:

a. channel trip
b. fan failure in channel
c. channel on test
d. shutdown bypass initiated
e. manual bypass initiated
f. dummy bistable installed

Any time a test switch is in other than the operate position, annunciator (c) will be lit and the associated protection channel will be tripped. Under this condition, annunciator (a) will be lit unless annunciator (e) is lit (i.e., the channel is bypassed).

3.0 SURRY RPS DESCRIPTION

The RPS is defined to consist of 48 CRAs, their magnetic jack assemblies, breakers and motor generator sets that provide power to the magnetic jacks and the electronic logic that controls the trip circuit breakers in response to the monitoring of certain reactor parameters such as pressurizer pressure or reactor coolant temperature (see Figure B3-2). The RSS analysis did not consider the rod control system, which is used to slowly raise or lower individual control rods for the "shimming" of reactor power. Since the entire rod control system gets its power from the reactor trip breakers, tripping the reactor by opening the breakers disables the rod controls and removes all power to the magnetic jacks. Without power, all magnetic jacks will release their hold on the control rods and allow them to fall into the core unless mechanical damage restrains them. Thus the rod shim control system has no effect on the success of a trip. The rods and jacks thus will only be involved in the analysis as mechanical faults.

The Reactor Protection System or Trip System rapidly drops the Control Rod Assemblies when conditions exist requiring reactor shutdown. Control rods are normally held in position by the magnetic jacks. The Control Rod Assemblies are dropped during the trip by removal of power to the rod control system through the opening of either reactor trip breaker 52/RTA or reactor trip breaker 52/RTB. Breaker 52/RTA is controlled by RPS Train A and Breaker 52/RTB is controlled by RPS Train B.

The two series connected trip breakers RTA and RTB control power from two parallel connected motor generator sets. The two motor generators provide isoltaion from the 480-volt busses they are powered from and provide power to the magnetic jack controls with a three-phase non-synchronous voltage which would be difficult to sustain by shorting to any other source of power in the plant. Thus the potential fault of trip bus power remaining present due to shorts to other busses when the trip breakers open is very unlikely. Since the motor generator sets receive power from two 480-volt busses, failure of power on both of these busses will result in an inadvertent trip.

The two reactor trip breakers are each bypassed by a special test breaker of the same type as the trip breakers. These are called BYA-bypass A, connected across RTA, and BYB connected across RTB. Both bypass breakers are normally open. BYA is tripped by reactor Train B and BYB is tripped by Train A. A typical test use of these breakers would be to close BYA for a test of breaker RTA. Test signals are sent through Train A which will trip our RTA. Instruments monitoring RTA will indicate that it tripped properly. After testing, RTA is closed again and BYA is opened, and the system is left with only the original closed series connection of RTA and RTB. If during the test (when RTA, RTB, and BYA were closed) a trip condition would exist, all three breakers would open and a reactor trip would occur. The two bypass breakers are interlocked electrically so that both may not be closed at the same time. The bypass breakers are also used for repairing of the trip breakers RTA and RTB. If RTA fails to trip in the test mode, BYA will be closed and RTA will be "racked out" and repaired without removing power or scramming the reactor.

The tripping signals which trip the various breakers come from two logic trains which are identical in design. Each is composed of relay logic and has the purpose of combining various transducer bistable signals into a single command to trip the reactor. The initiating bistable signals are combined together into eight functional signals called RT1 thru RT7 and manual trip. Each of the eight is capable of initiating a trip by itself. This relay logic, called trip Trains A and B, consists of all logic between the bistable relays of the analog instrumentation and the trip breakers.

The eight divisions of each train are:

1. RT-1 - Primary System,
2. RT-2 - Primary System and Nuclear Flux Differential,
3. RT-3 - Pressurizer System,
4. RT-4 - Steam Generator Low-Low Level,
5. RT-4 - Steam Generator Feed-Flow Mismatch,
6. RT-6 - Miscellaneous Trips,
7. RT-7 - Nuclear Flux Instrumentation, and
8. Manual Trip.

Although there are reactor trips from many sources, definition of failure to trip for the small liquid leak LOCA considers only three of those divisions as the initiating signals attempting to provide a trip. They are:

1. RT-3 - The pressurizer signals: low pressure;
2. RT-1 - The primary system: overtemperature; and
3. RT-6 - Trips through SICS initiation: low pressurizer coincident with low pressurizer level...

On each of these circuits, except for RT6, transducers provide analog signals which result in bistable relay signals for each out of tolerance parameter. Since there are usually three analog instrumentation channels for each parameter, the relay logic provides a 2-out-of-3 determination for each parameter. This signal combined with others generates the RT1 and RT3 trips. RT6 on the other hand is composed of the logical "or" of both output signals of the SICS. Since the analysis is only concerned with the small LOCA, it is assumed that the only initiating signals which will trigger the SICS are pressurizer low pressure and level. It should be noted that the same six pressure and level transducers used in the RT3 trips are used for triggering the SICS; however, different comparators are used.

4.0 COMPARISON OF OCONEE AND SURRY RPS

The Oconee RPS differs significantly from the Surry RPS in the method of interrupting power to the CRA. The Surry RPS accomplishes the reactor trip by deenergizing combinations of 1-out-of-2 primary circuit breakers via the logic channels. The Oconee RPS accomplishes the reactor trip by deenergizing combinations of two primary and two secondary circuit breakers and two groups of contactors. The primary breakers interrupt power to all CRA drive motors while the secondary breakers interrupt power to the safety rod groups and the contactors interrupt power to the regulating rod groups.

The Oconee RPS logic employs 4 logic channels with each breaker and contactor. The Surry RPS logic employs 3 sensor logic channels feeding into 2 output trains which, in turn, input to the circuit breakers. The Oconee sensor logic is a 2-out-of-4 system whereas the Surry sensor logic is a 2-out-of-3 system; i.e., any 2 of the logic channels will trip the reactor when an abnormal condition occurs.

The point estimates per reactor year for the Oconee and Surry RPS failure probability are:

$$Q(\text{RPS, Oconee}) = 2.6 \times 10^{-5}$$

$$Q(\text{RPS, Surry}) = 4.8 \times 10^{-5}$$

The dominant contributor for both reactor protection systems was the test and maintenance contribution which results in a decreased system redundancy during the test and maintenance operation.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

Failure of the RPS appears as event K on the Oconee LOCA and transient event trees. For the analysis of large LOCAs, the RPS event is assumed to succeed since the vessel will quickly blow down and borated ECCS water will prevent the fission process from restarting even if the RPS fails. For all other accidents the RPS is required to successfully function.

5.2 Determination of RPS Unavailability

A simplified fault tree for the Oconee RPS is shown in Figure B3-3. The major contributor was found to be the failure to remove power from the rod drive motors. Test and maintenance faults made up 88% of this failure.

As shown in Figure B3-3, the RPS unavailability for Oconee was estimated to be:

$$Q(RPS) = 2.6 \times 10^{-5}/\text{reactor year} .$$

Table B3-1. Reactor Trip Summary

Trip Variable	Number of Sensors	Steady-State Norm.. Range	Condition for Trip
Over Power	4 Flux Sensors	0-100%	107.5% of rated power
Nuclear Over-Power Based on Flow and Imbalance	4 Two-Section Flux Sensors 8 ΔP Flow	N/A	1.08 times flow minus reduction due to imbalance
Power/RC Pumps	4 Pump Monitors	2 to 4 Pumps	Loss of one operating coolant pump and reactor neutron power exceeds 55% rated power
			Loss of two operating reactor coolant pump motors in one loop
		2 pumps	Loss of one of two operating reactor coolant pump motors in one loop
Reactor Outlet Temperature	4 Temperature Sensors	532-604°F	619°F
Pressure/Temperature	4 Temperature Sensors 4 Pressure Sensors	N/A	$(13.26T_{out}-5989) \geq P$
Reactor Coolant Pressure	4 Pressure Sensors	2090-2220 psig	2355 psig - High 1800 psig - Low
Reactor Building Pressure	4 Pressure Sensors	0 psig	4 psig

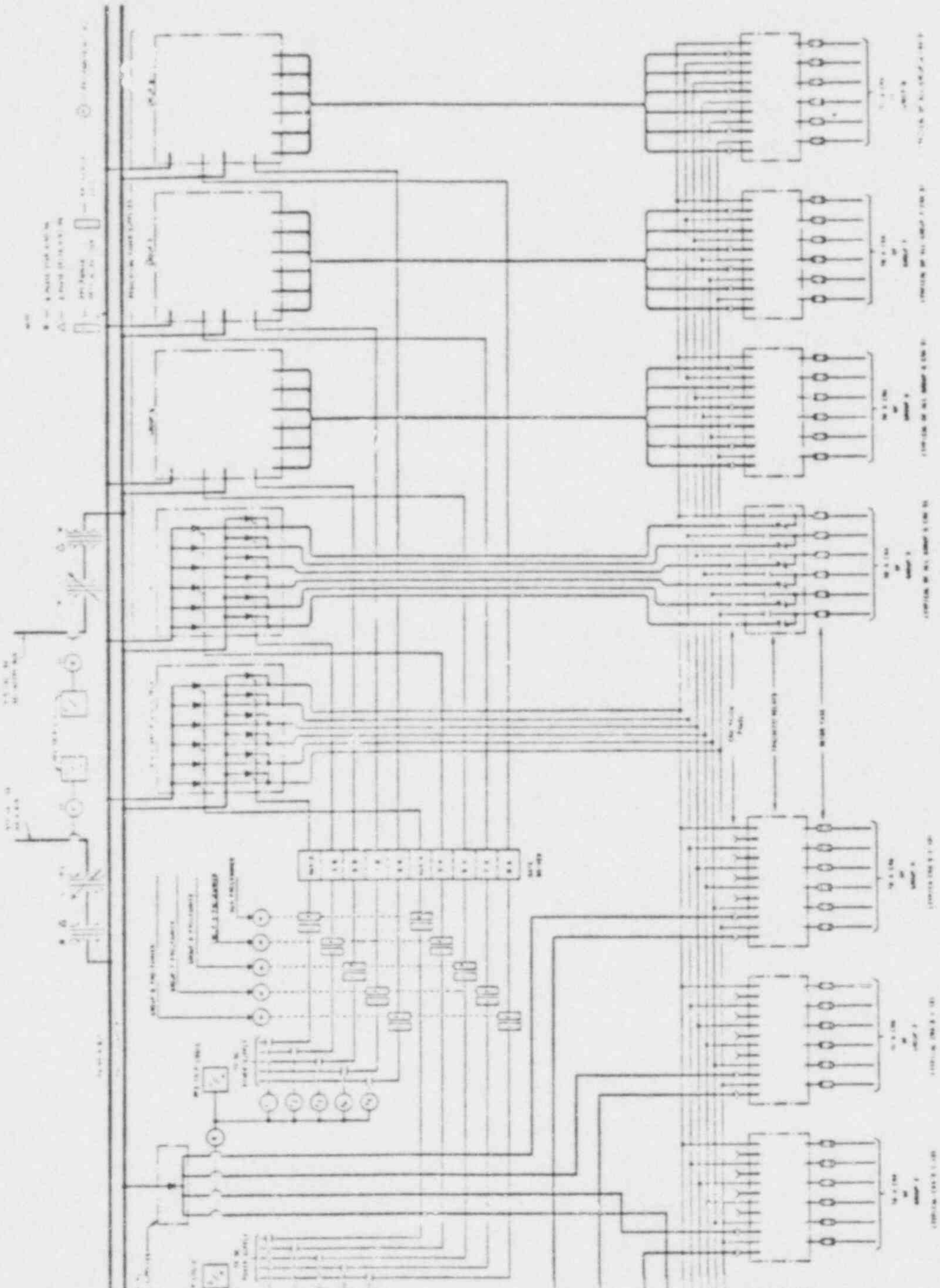


Figure B3-1. Oconee Rod Drive Controls

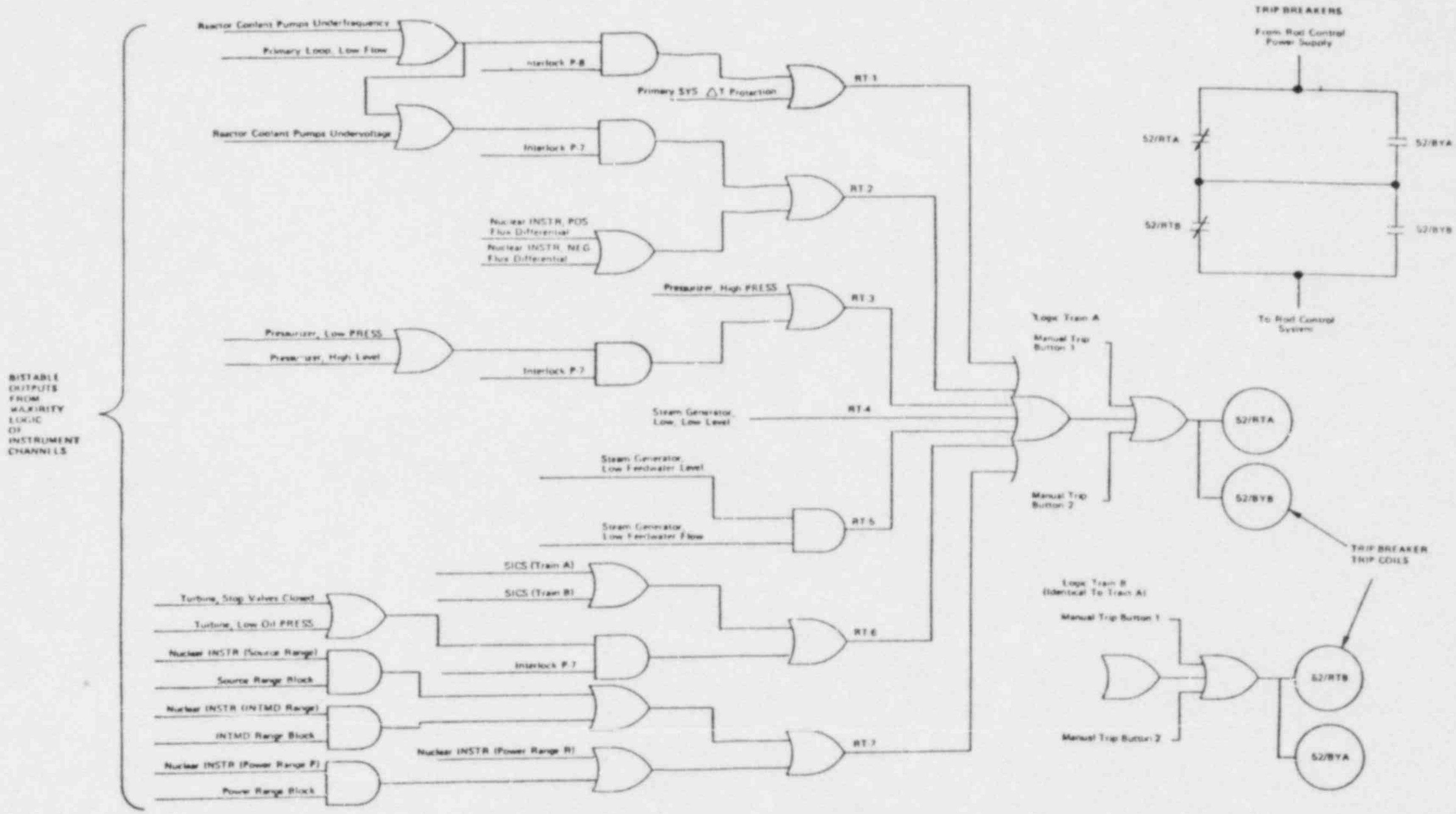


Figure B3-2. Surry Reactor Protection System Logic Diagram

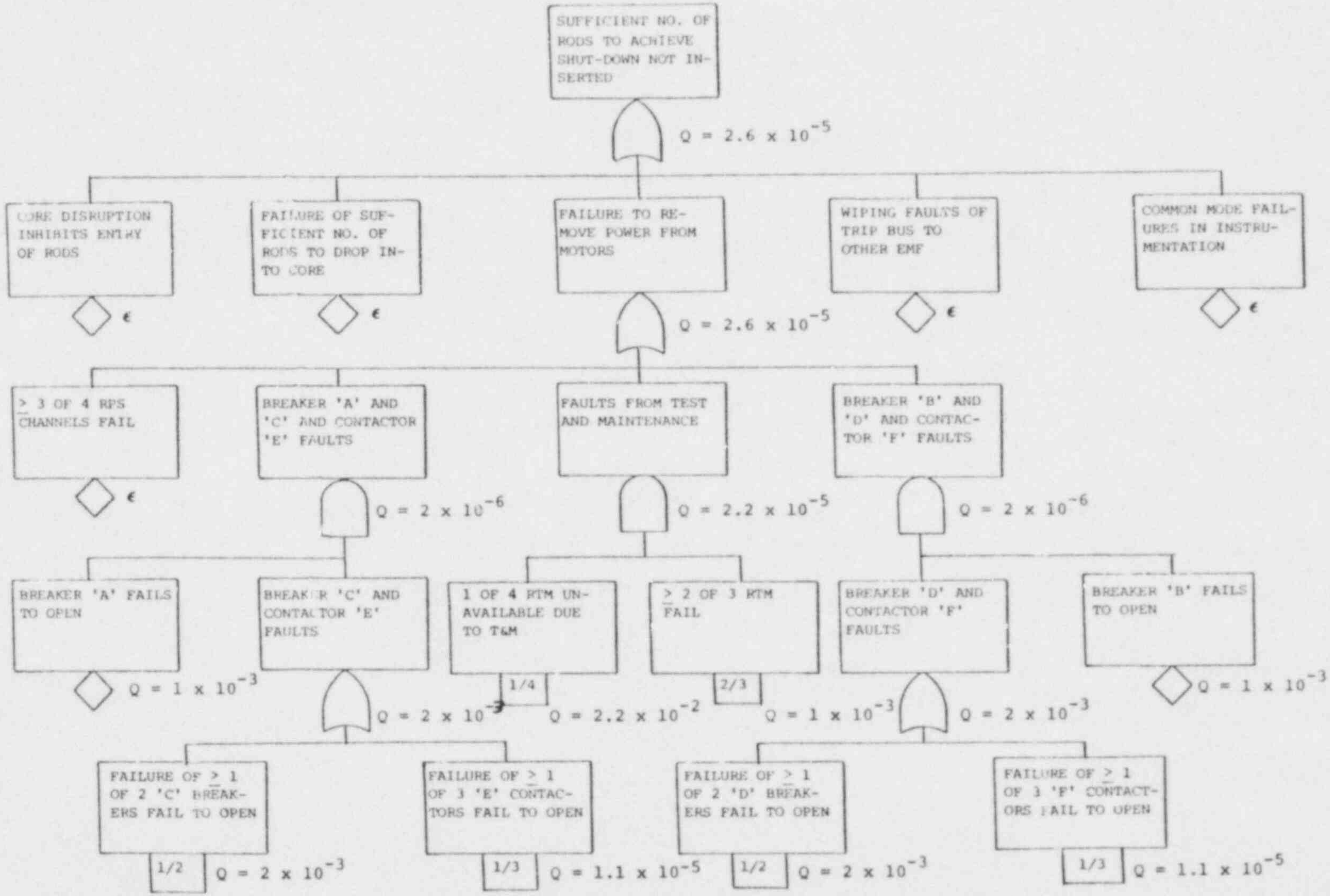


Figure B3-3. Oconee RPS Fault Tree

APPENDIX B4

SURVEY AND ANALYSIS

CONTAINMENT LEAKAGE (CL) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 systems and components which are designed to contain the release of radioactivity from the primary system in the event of an accident were reviewed and compared with the analogous system and components of the Surry plant analyzed in WASH-1400. The probabilities of failure of these systems or components define the containment leakage (CL) probability as was used in the containment event tree. As in WASH-1400, containment leakage was defined as that leakage which provides a flow path to the atmosphere equivalent to a 4" diameter hole or greater.

The designs to minimize containment leakage for Oconee and Surry are described in Section 2 and 3, respectively, of this Appendix. A comparison of the Oconee and Surry design is given in Section 4. The use of the 'CL' probability in the containment event tree is specified in Section 5. Also included in Section 5 is a point estimate of the Oconee 'CL' probability.

2.0 OCONEE CONTAINMENT INTEGRITY SUMMARY

2.1 Description

The Oconee Unit 3 reactor building is a prestressed, post-tensioned, concrete containment structure with a 1/4" steel liner. The liner plate, which is designed to maintain its integrity under all postulated loading conditions, is attached to the concrete by an angle grid system stitch welded to the liner plate and embedded in the concrete. The liner plate over the foundation slab is protected by a concrete cover. The reactor building, normally at atmospheric pressure, is designed to withstand an internal pressure of 59 psig. Under this maximum design pressure, the leakage rate is designed not to be greater than .25% containment volume in 24 hours. A schematic of the reactor building ventilation system is shown on Figure B4-1.

There are approximately 60 major piping penetrations into the containment. Fluid penetrations which are required to be isolated after an accident are classified into four categories:

Type I. Each line connected directly to the reactor coolant system has two isolation valves. One valve is inside and the other valve is outside the reactor building. These valves may be either a check valve and a remotely operated valve, or two remotely operated valves, depending upon the direction of normal flow.

Type II. Each line connected directly to the reactor building atmosphere has two isolation valves. At least one valve is outside and the other may be inside or outside the reactor building. These valves may be either a check valve and a remotely operated valve or two remotely operated valves, depending upon the direction of normal flow.

Type III. Each line not directly connected to the reactor coolant system or not open to the reactor building atmosphere has at least one valve, either a check valve or a remotely operated valve. This valve is located outside the reactor building.

Type IV. Lines which penetrate the reactor building and are connected to either the building or the reactor coolant system, but which are not normally open during reactor operation, may have manual valves with provisions for locking in a closed position.

The design basis for isolation valves on containment penetrations is that leakage through all fluid penetrations not serving accident consequence limiting systems, be minimized by a double barrier. Thus, no single failure of an active component will result in loss of containment integrity. In addition, the containment is equipped with 3'6" X 6'8" double door personnel hatch, a 30" diameter double door emergency personnel escape hatch, a 19" diameter single door equipment hatch and a fuel transfer tube. Both personnel hatches are interlocked and alarmed to prevent the simultaneous opening of these double doors. All penetrations, except those listed below are grouped within or are vented to the penetration room:

(a) main steam lines

(b) sump drain lines

(c) reactor building equipment drain lines

(d) decay heat removal lines

(e) refueling tube

Lines (a) through (d) are not likely to be sources of significant leakage because they are welded to the liner plate at points of penetration. The refueling tube is equipped with a blind flange which is removed only during shutdown to provide a transfer path for fuel to the spent fuel pool.

Plant technical specifications require local leak tests of the personnel hatches at least every 12 months. The equipment hatch and fuel transfer tube seals must be leak tested after each opening or at least every 12 months. Integrated leak tests of the containment are required at least two times in a ten-year interval.

As indicated above, the Oconee containment is also equipped with a penetration room in which most of the major containment penetrations have been grouped or are vented to. The penetration room has a separate ventilation system which processes post accident containment leakage to minimize environmental activity levels.

2.2 Operation

During normal operation, reactor building ventilation and air cooling is provided by the reactor building ventilation system. Specifically, the normal function of cooling reactor building air is performed by the recirculation of containment air through two of three fan cooling units. The fan cooling units are cooled by the low pressure service water system. During accident conditions, all three fan cooling units are operated to provide containment cooling. (This provides a redundant mode of cooling to the containment spray system). The fan cooling units are entirely within the containment, necessitating a containment penetration only for the low pressure service water. Containment ventilation is provided to the containment by purge lines directly linking the containment to the atmosphere. The purge lines are monitored and alarmed to minimize excess radiation leakage. Each purge line has three isolation valves in series which receive an ESPS signal to close on high reactor building pressure (4 psig) or low reactor coolant system pressure. This same signal also isolates other penetrations not serving accident mitigation functions and starts the penetration room ventilation system.

3.0 SURRY CONTAINMENT LEAKAGE DESCRIPTION

The containment building is a steel-lined, reinforced concrete structure, including foundations, access openings, and penetrations designed to maintain an essentially leak-tight barrier against the release of fission products under conditions up to and including any design basis accident. Normally, the 60 psia design presure containment operates at a subatmospheric pressure of 9 to 11 psia. The containment system is designed for a maximum leakage rate of less than 0.1 volume percent per day at design pressure.

Access to the containment structure is provided by a 7'0" ID personnel hatch penetration and a 14'6" ID equipment hatch penetration. Other smaller containment structure penetrations include hot and cold pipes, main steam and feedwater pipes, fuel transfer tube, and electrical conductors and containment purge lines. Figure B4-2 is a cross-section of the containment structure.

The Surry nuclear plant containment isolation is achieved by applying common criteria to penetrations (e.g., the two barrier criterion) in all the interfacing fluid systems and by using ESF signnals to activate appropriate valves. Signals which activate the safety injection control system (SICS) and the consequence limiting control system (CLSC) are used to close these isolation valves.

Depending on the specific application, the two barriers previously mentioned consist of one of the following valving arrangements:

1. Two automatic isolation valves, one on each side of the containment wall.

2. An automatic isolation valve and a membrane barrier.

3. An administratively controlled, manually operated valve outside, and a sealed system inside the containment.

4. Two administratively controlled, manually operated valves, one on each side of the containment wall.

5. A sump recirculation pipe and valve arrangement, conservatively designed and fabricated, and enclosed by a special valve pit.

A membrane barrier consists of either pipe, tubing, component wall. An incoming line from a centrifugal pump or a surge tank is considered an open line and a check valve is used in incoming lines instead of an autmatic isolation (auto-trip) valve. However, check valves, single or in pairs, are not used to provide the only means for isolating a penetrating line.

There are about 50 major piping penetrations through the containment structure. These can be grouped in five functional classes according to the implementation of the design bases. Class I piping is open to the outside atmosphere and is connected to the reactor coolant system, or a connecting system, or is open to the containment atmosphere. Class II piping is connected to a closed system outside the containment, and is connected to the reactor coolant system, or a connecting system, or is open to the containment atmosphere. Class III piping is connected to open systems outside the containment and is separated from the coolant system, or a connecting system, and the containment atmosphere by a closed valve under administrative control or a membrane barrier. Class IV piping must remain open after a loss-of-coolant accident. Class V piping is connected to normally closed systems outside the containment, and is separated from the reactor coolant system, and connecting systems, and the containment atmosphere by a closed valve and/or membrane barrier.

4.0 COMPARISON OF OCONEE AND SURRY CL CONTRIBUTORS

As discussed in the main report, insights from WASH-1400 were used wherever possible to evaluate the reliability of each part of the Oconee design. Thus, on the basis of the WASH-1400 analysis, and in consideration of the leak tests required by technical specifications, structural failure of the containment shell, failure of the blind flange on the refueling tube and major leakage through the equipment hatch were not judged to be dominant contributors to the CL probability. Further, the probability of a significant leakage path through the containment spray injection line was not judged significant because, unlike Surry, Oconee uses the same line for containment spray recirculation as for injection. Back leakage through the LPIS lines was also judged not significant because of the numerous check valves in each line.

Conversely, dominant contributors to the Oconee CL probability, which were not present at Surry, developed from the difference between Surry's subatmospheric design and Oconee's atmospheric containment. Specifically, the probability of significant open penetrations of the containment which go unnoticed for some time was precluded at Surry because normal operation requires internal containment pressure to be significantly below atmospheric pressure, i.e., the containment is constantly leak tested. However, at Oconee, where there is no constant leakage monitoring system, and the containment is kept at atmospheric pressure, a significant unnoticed leakage path was judged to be more likely.

5.0 OCONEE CL EVALUATION

5.1 Event Tree Relationship

Containment leakage, CL, appears as event β on the containment event tree.

5.2 Estimate of CL Probability

As discussed in Section 4.0 of this Appendix, a significant contributor to the CL probability was judged to be the possibility of a significant violation of the containment integrity going unnoticed for some time. To estimate the probability of this failure mode, Licensee Event Reports (LERs) were surveyed for the period 1969 to mid-1980. During this period approximately 184 years of PWR operation was amassed for plants with other than a subatmospheric containment design (average capacity factor of 74.6% assumed).[1] The LERs were screened to yield incidents in which a containment penetration equivalent to a 4" diameter pipe was open at plant conditions other than shutdown. Many of the violations found involved leakage or opening of both airlock doors. However, because the airlocks were alarmed, these violations were generally of very short duration. Incidents in which unmonitored penetrations were open and penetrations caused by plant personnel inadvertently drilling holes in the steel liner did occur. However, the inadvertent drilling penetrations, some of which remained undiscovered until an integrated leak test was performed, were not included as failure contributors because they did not meet the 4" diameter equivalent hole criterion. Thus, the major component of the undetected open penetration contributor to CL was from an incident involving an unmonitored system penetration. This single incident was the largest contributor to containment leakage of atmospheric containments during the time period examined. Assuming such occurrences are equally likely at all plants, this failure mode, estimated at $7x10^{-3}$, was the dominant contributor to the 'CL' probability.

---

1. Nuclear Power Plant Operating Experience - 1978, NUREG-0618.

The contribution to the 'CL' probability of failure to isolate the containment purge lines was also considered. Conversations with plant personnel indicate that the Oconee Unit 3 containment was open via the purge valves approximately two percent of the time the plant was at full power in 1978 (the last year of available data). However, plant personnel also indicate the series purge valves on each line now isolate on redundant signals (ESPS channels 1 and 2, high containment pressure, low reactor coolant system level) so that this was judged to be a significantly smaller contributor to the 'CL' probability than the undetected open penetration. The failure of such passive components as welds, gaskets, pipe caps, over plates and flanges was assumed to be slightly greater than for Surry because of the slightly greater number of penetrations. In the RSS, the contributions to the CL probability from failure of passive components was estimated at approximately 1.0×10^{-4} per reactor year. A slightly greater contribution (3.0×10^{-4}) for passive failures was assigned for Oconee. This leads to a total CL probability of

$$P(CL) = 7.3 \times 10^{-3} \text{ per reactor year.}$$

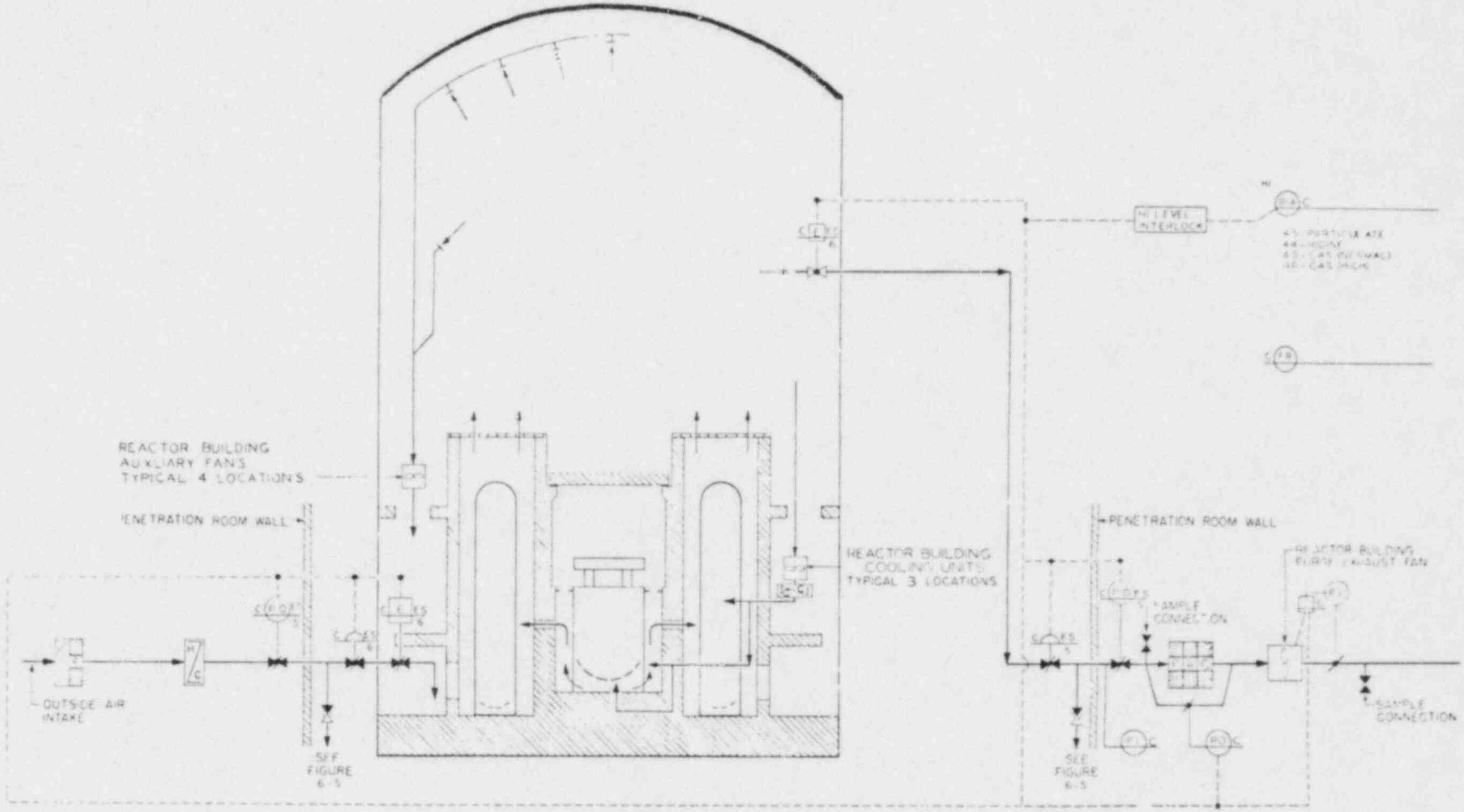


Figure B4-1. Oconee Reactor Building Ventilation Schematic

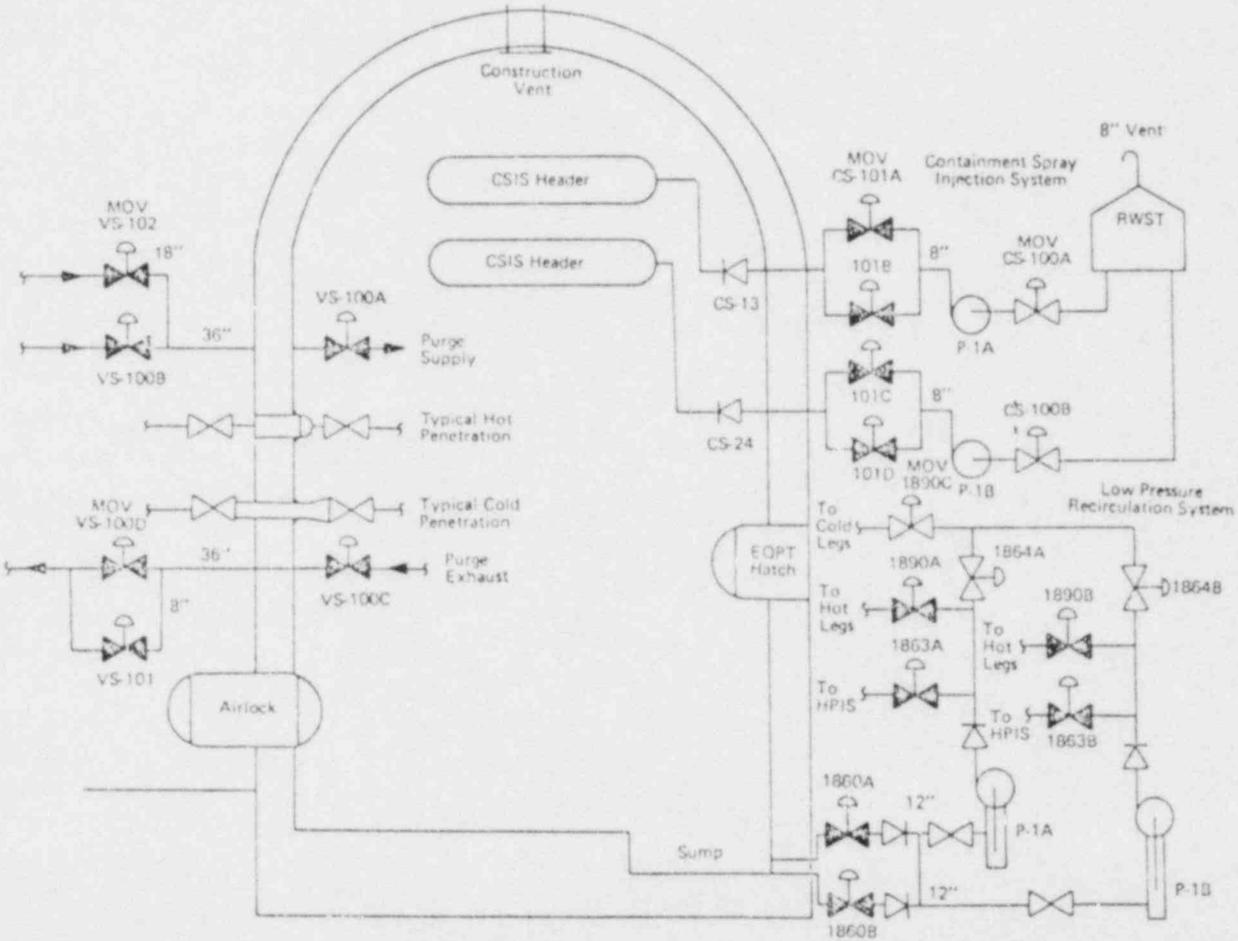


Figure B4-2. Surry Containment Leakage Schematic

APPENDIX B5

SURVEY AND ANALYSIS

CORE FLOODING SYSTEM (CFS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Core Flooding System was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The CFS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two core flooding systems is given in Section 4. CFS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate CFS failures into the Oconee accident sequences and a point estimate of the CFS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE CFS DESCRIPTION

2.1 System Description

The CFS along with the High Pressure Injection System and Low Pressure Injection System are designed to form collectively on overall Emergency Core Cooling System (ECCS), which is designed to prevent core damage over the entire spectrum of LOCA break sizes. Figure B5-1 shows the ECCS for one reactor unit.

The CFS is a passive self-contained, self-actuating system. It is designed to flood the reactor core when the reactor coolant system pressure drops below 600 psig in the event of a large LOCA.

The system consists of two separate and independent trains. Each train consists of a nitrogen pressurized (core flooding) tank, containing borated water, two check valves and a normally open motor operated isolation valve in series, and associated piping. The borated water is discharged directly into the reactor vessel under the driving force of the pressurized nitrogen in the tanks.

The core flooding tank, constructed of carbon steel lined with stainless steel with a total volume of 1410 ft^3, has a normal inventory of 1040 ft^3 of borated water (7000 gallons of H_2O at 2270 ppm boron). The tank design pressure is 700 psig and its operating pressure is 600 psig. A relief valve is installed directly on the tank to protect against overpressurization.

The two 14 inch series check valves, made from type 316 stainless steel and rated at 2500 psig, prevent high pressure coolant from entering the accumulators during normal plant operation. The isolation valve at the tank outlet is fully open during normal plant operation and its position is indicated in the control room.

Each tank includes provisions for adding both borated water and nitrogen during reactor power operation in order to maintain the proper water level and pressure. Redundant pressure and water level indicators and alarms are provided in the control room for each tank.

2.2 System Operation

During normal operation the reactor coolant system is isolated from the tanks bythe two series check valves thereby preventing reactor coolant from entering the accumulators. When the reactor coolant system pressure drops below 600 psig, due to a LOCA, the stored borated water, driven by the pressurized nitrogen, opens the two series check valves and is injected into the reactor vessel to flood the core.

To assure that the isolation valves CF-1 and CF-2 will not be accidently closed during reactor power operation and thus inhibit water injection into the core in the event of a LOCA, the following provisions are included in the CFS design:

- The circuit breaker supplying power to the tank isolation valves will be open and tagged out under administrative control whenever the reactor is at power. Power to the actuation circuitry comes from this same circuit breaker through a control transformer and will also be disconnected when the circuit breaker is open.
- Lights are provided in the control room to indicate valve position (open or closed). These lights have a power supply separate from the circuit breaker serving the isolation valves and are operated from limit switches on the valve operator.
- Another limit switch on the valve operator will cause an annunciator alarm in the control room anytime an isolation valve is away from the wide open position. The annunciator system has a power supply separate from that used to operate the valve or the indicating lights.
- The unit computer also alarms and documents the position (open or closed) of the isolation valve. The computer has a power supply separate from that used to operate the valve or the indicating lights.

3.0 SURRY CFS DESCRIPTION

The Surry Cold Leg Injection Accumulator System (CLAS) (equivalent to CFS) provides for core protection for intermediate and large reactor coolant system pipe failures by automatically flooding the core with borated water. The system, which is passive and self-actuating, includes three independent trains for injecting borated water into the cold legs of the reactor coolant system (Figure B5-2).

Each train consists of a nitrogen pressurized tank, containing borated water, two check valves and a normally open, motor operated isolation valve in series, and the associated piping for interconnecting the tank with the cold leg. The tank is pressurized to 650 psig. When the pressure in the cold leg drops below 650 psig, the check valves will open and the borated water will be forced into the reactor coolant system. If the isolation valve is closed and a LOCA occurs, a safety injection control system (SICS) signal will apply power to the motor operator to open the alve.

Water level and N_2 pressure in each accumulator is monitored and alarmed by redundant level and pressure instrumentation. A relief valve provides overpressure protection for each accumulator. The accumulators are isolated from all other systems and accumulator support systems by closed valves.

Successful operation of the CLAS in the event of an intermediate or large LOCA requires that the contents of at least 2 of the 3 accumulators be injected into the reactor coolant system cold legs. If a LOCA occurs in a cold leg, the contents of the associated accumulator will be lost out of the break thereby requireing both of the remaining 2 accumulators to successfully discharge their contents into the reactor coolant system.

4.0 COMPARISON OF OCONEE AND SURRY CFS

Three major design differences between the Oconee CFS and Surry CLAS designs were disclosed in this analysis. The Surry design employs three identical trains for delivery of the borated water to the reactor coolant system whereas the Oconee design employs two identical trains. Surry injects water into the reactor coolant system cold legs whereas, Oconee injects the water directly into the reactor vessel. If an isolation valve in the Surry system is inadvertently left closed, it will be opened via the safety injection signal which will apply power to the valve motor. No such provisions are present in the Oconee system isolation valves; instead, valve position is monitored and alarmed.

An additional important difference is the technical specification requirement for CFS availability. At Surry one core flood tank is allowed to be out of service for 4 hours before the reactor is to be shut down. At Oconee both coreflood tanks must always be available. This difference adds a significant test and maintenance contribution to the Surry CLAS unavailability which does not exist at Oconee.

The RSS estimated a 9.5×10^{-4} unavailability for the Surry accumulator system. This is somewhat higher than the 6×10^{-4} calculated for Oconee's system.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The CFS is one of a group of three systems which provide Emergency Coolant Injection (ECI) to prevent core damage for various break sizes. The remaining two systems include (1) the High Pressure Injection System and (2) the Low Pressure Injection System.

Failure of CFS contributes to Event D (ECI) on the large (breaks >13.5") LOCA event tree. Failure of the CFS to deliver the contents of both tanks to the reactor core, in the event of a large LOCA, constitutes system failure.

5.2 CFS Model Description

5.2.1 CFS Boolean Equation

The following Boolean equation was developed as the model for CFS failure:

$$\text{CFS (1 of 2 Fail)} = (H + J) + (I + K) \quad . \qquad \text{Eq. B5-1}$$

Table B5-1 relates each term in the above equation to the component in Figure B5-1. Table B5-2 lists total component unavailabilities and each of the failures that contribute to the component unavailability. These failures are comprised only of hardware faults since no important human or test and maintenance faults were identified. There is no significant test and maintenance contribution since the only testing or maintenance that occurs is when the system is down for refueling or the RCS is below 800 psig, as the technical specification operating requirements. No common mode failures were identified.

5.2.2 CFS Unavailability

Using the Boolean equation given in the last section and the term unavailabilities given in Table B5-1, an independent CFS point estimate unavailability can be calculated. This is found to be:

$$\text{CFS (1 of 2 fail)} = 6 \times 10^{-4}/\text{reactor year} .$$

A quantitative ranking of the Boolean terms for the CFS is given in Table B5-3. As can be noted, each term is a significant contributor to the system unavailability.

The reader should be cautioned that these are unavailabilities for Oconee's CFS if the system is considered independent of all others. In general, the CFS unavailability will depend on what other system success or failures have occurred, i.e., the unavailability used for the CFS in the sequence analysis calculations must be a conditional unavailability.

Table B5-1. Boolean Equation Term Descriptions[1]

Boolean Term	Term Definition	Term Unavailability
H	CF-2 + CF-13	2×10^{-4}
I	CF-1 + CF-11	2×10^{-4}
J	CF-12	1×10^{-4}
K	CF-14	1×10^{-4}

1. Refer to Figure B5-1.

Table B5-2. Component Unavailabilities

Component Description	Fault Identifiers	Contributors	Q(per component)
Check Valve	CF-11 CF-12 CF-13 CF-14	Hardware	1×10^{-4}
		Q	1×10^{-4}
Motor Operated Valve (Normally Open)	CF-1 CF-2	Plugged	1×10^{-4}
		Q	1×10^{-4}

Table B5-3. Quantitative Ranking of Terms in CFS Boolean Equation.

H	2×10^{-4}
I	2×10^{-4}
J	1×10^{-4}
K	1×10^{-4}
	6×10^{-4}

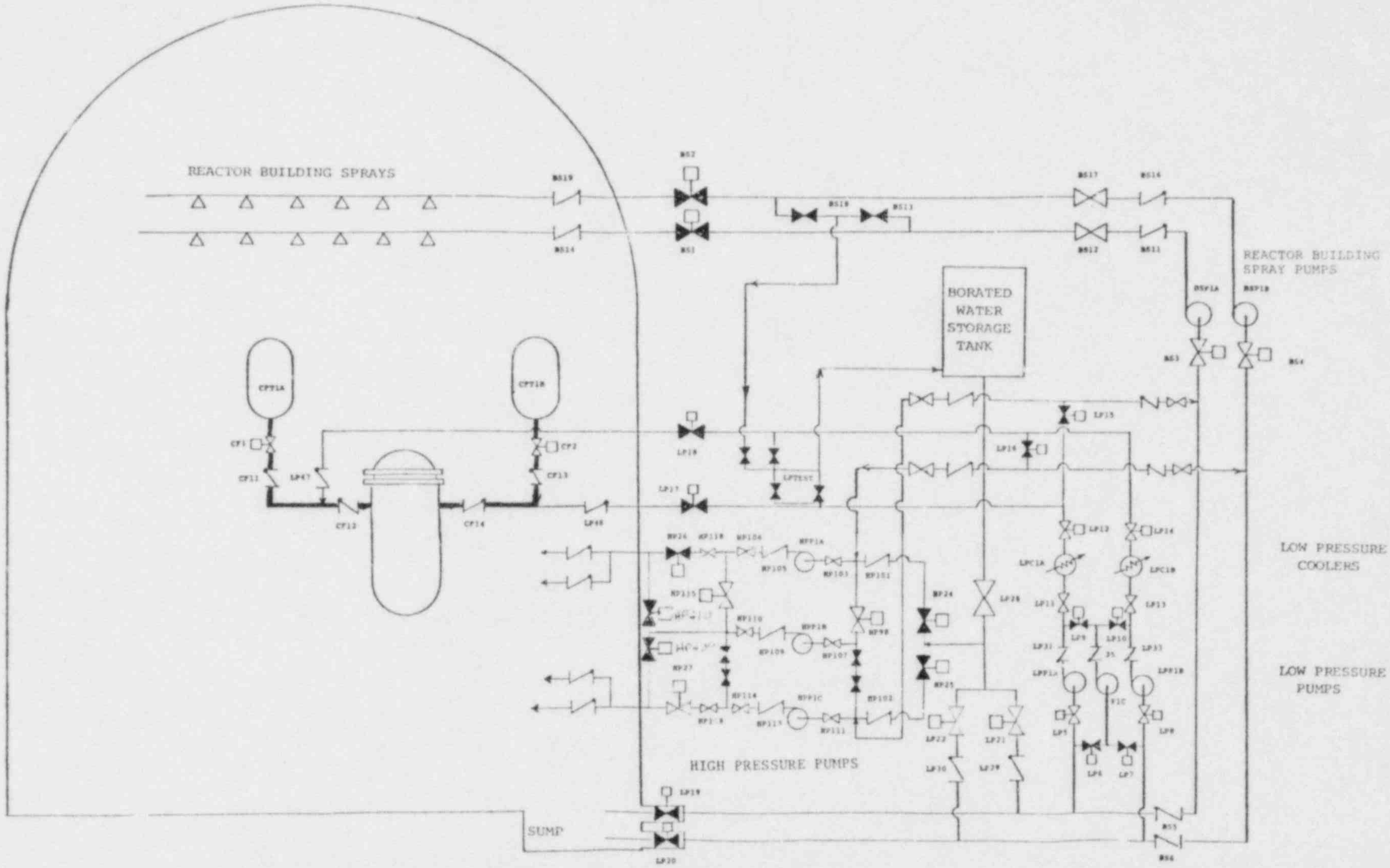


Figure B5-1. Oconee ECCS Schematic (CFS Highlighted).

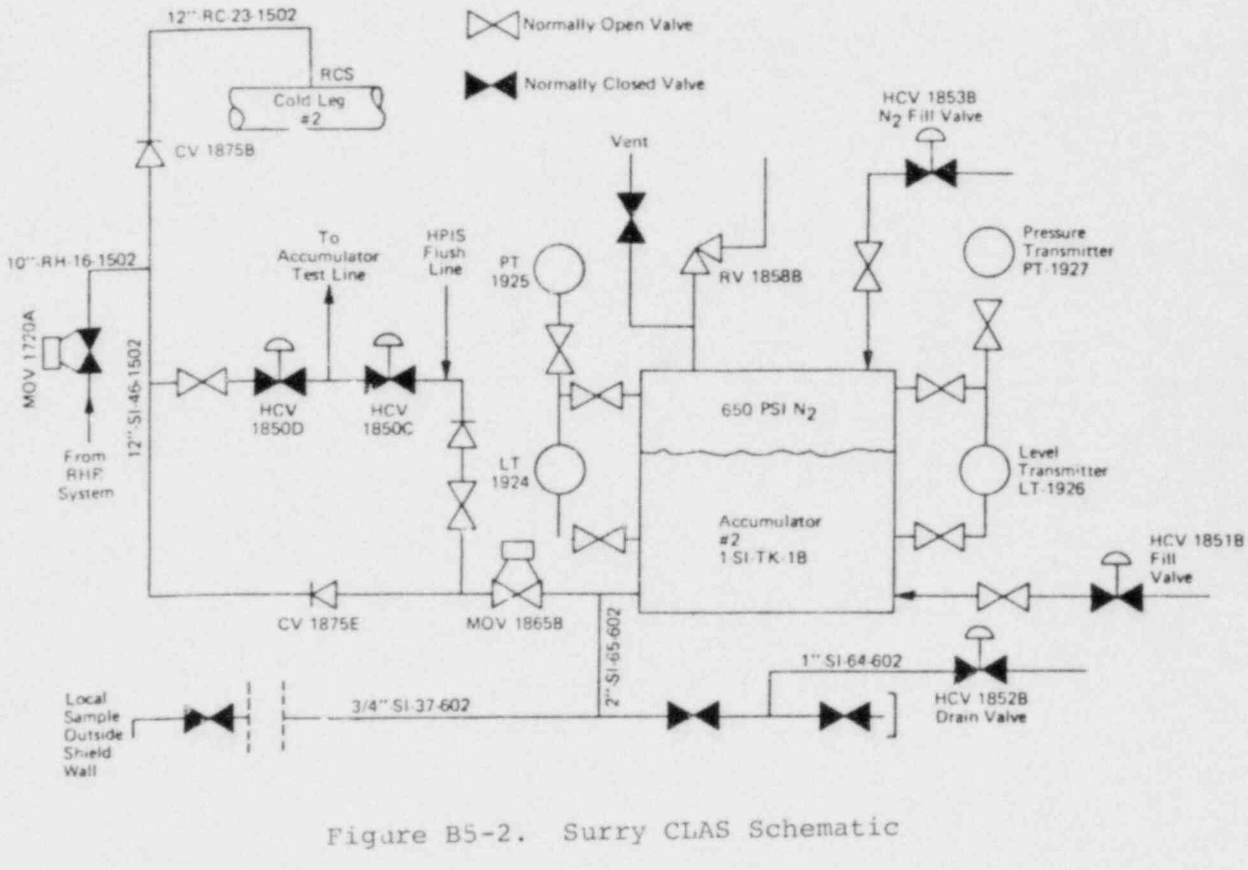


Figure B5-2. Surry CLAS Schematic

APPENDIX B6

SURVEY AND ANALYSIS

LOW PRESSURE INJECTION SYSTEM (LPIS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Low Pressure Injection System (LPIS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The LPIS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two low pressure injection systems is given in Section 4. LPIS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate LPIS failures into the Oconee accident sequences and a point estimate of the LPIS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE LPIS DESCRIPTION

2.1 System Description

The Emergency Core Cooling System (ECCS), which is designed to prevent core damage over the entire spectrum of RCS break sizes, is combined of the LPIS, the High Pressure Injection System (HPIS), and the Core Flooding System. Figure B6-1 shows the ECCS for one reactor unit.

As highlighted in Figure B6-1, the LPIS is a system which provides two flow paths for delivering borated water to the RCS following a LOCA. Water is drawn through a single suction header from the BWST, which has a total capacity of 388,000 gallons containing 2200 ppm boron, and pumped directly into the reactor vessel through two core flooding nozzles located on the opposite sides of the vessel. Each flow path delivers the borated water to the reactor vessel at a flow rate of 3000 gpm.

The BWST is isolated from the LPIS pumps during normal plant operations by two parallel, normally closed, motor operated valves (LP-21, LP-22). The LPIS is isolated from the RCS pressure by two check valves and a normally closed motor operated valve arranged in series in each flow path. Check valves LP-48 and CF-14 and MOV LP-17 provide RCS isolation for one flow path while check valves LP-47 and CF-12 and MOV LP-18 provide RCS isolation for the other flow path. Note that valves CF-12 and CF-14 also provide RCS isolation for the core flooding tanks.

The LPIS includes three electric driven pumps, each with a flow rate of 3000 gpm (LP-P1A, LP-P1B, LP-P1C). Normal low pressure injection is accomplished by pumps LP-P1A and LP-P1B with pump LP-P1C valved out via normally closed MOV's LP-7, LP-8, LP-9 and LP-10. Miniflow by-pass lines are employed to prevent pump overheating and loss of suction (not shown on Figure). Check valves LP-31, LP-33 and LP-35 are included at the output of the low pressure injection pumps LP-P1A, B, and C respectively to prevent back flow of coolant through idle pumps.

Each flow path includes a shell and tube type heat exchanger (LP-C1A, LP-C1B) through which the borated water is pumped prior to injection into the reactor vessel. These heat exchangers are employed during the recirculation mode for cooling water drawn from the reactor building sump.

2.2 System Operation

Automatic initiation of the LPIS is initiated by Channels 3 and 4 of the Engineered Safeguards Protective System (ESPS) when the RCS pressure falls to 500 psig or the reactor building pressure rises to

4 psig. An ESPS signal resulting from either of these conditions causes:

a) Low pressure injection pumps LP-P1A and LP-P1B to start.

b) Valves LP-17 and LP-18 in the low pressure inlet lines to open.

c) All low pressure service water pumps to start.

d) Service water valves from low pressure injection coolers to open (LPSW-4, LPSW-5).

The injection mode continues until the BWST is approximately 94% empty at which time a low water level alarm is annunciated in the control room. Upon receipt of this alarm, the operator must re-align the LPIS to recirculate water from the reactor building sump through the heat exchangers and core flooding nozzles into the reactor vessel.

3.0 SURRY LPIS DESCRIPTION

The LPIS in the Surry Plant (Figure B6-2) consists of

i) Two pumps (3,000 gpm, 600 psig each), each driven by an electric motor. Each pump shares a common suction header and discharge header.

ii) Refueling Water Storage Tank (RWST) (350,000 gal. of borated water, with 1900 PPM boric acid concentration, chilled to 45°F).

iii) 3 discharge lines, one to each of 3 cold legs of RCS.

iv) 2 check valves in each of the 3 discharge lines, 1 normally open motor operated valve in the common feeder to the 3 discharge lines and 2 normally open motor operated valves, one each in the pump discharge line.

v) piping, isolation valves and instrumentation.

All stop valves between the RWST and the RCS are local and/or remote controlled manual valves and would normally be open. The check valves are installed to preclude backflow from the high pressure (2000 psig) RCS to the LPIS (600 psig).

Pump start-up is initiated by a signal from the Safety Injection Control System (SICS) when the pressure in the RCS falls to 600 psig. Borated water is drawn from the RWST and discharged into each of the 3 RCS cold legs. When the RWST is approximately 93% empty, as indicated by low RWST level alarm, the operator must realign the system to recirculate water from the containment sump to the RCS cold legs.

The LPIS is designed on the following basis:

a) Either pump will provide sufficient flow to the RCS cold legs.

b) Acceptable system performance can be achieved with only one of three cold leg flow paths providing flow into the RCS.

4.0 COMPARISON OF OCONEE AND SURRY LPIS

Both Oconee and Surry employ redundant LPIS trains to deliver borated water to the RCS following a LOCA. Major design differences that cause Oconee's LPIS unavailability to differ from Surry's are the valve configurations between the BWST and the LPIS pumps and between the pump discharge and the reactor vessel. Surry's LPIS suction line contains a manually operated gate valve in series with a motor-operated valve and check valve before the branchoff point to the pumps. There is then a single manually operated valve in each flow line before the pump. The LPIS pump discharge lines at Surry come together outside containment and branch inside containment before connecting with the RCS. Oconee's LPIS has one manually operated valve in the suction line before branching off to the pumps and then has two motor-operated valves and a check valve in series before each pump. Oconee's LPIS discharge lines do not come back together before connecting with the reactor vessel. These design differences were outlined to show the important fact that Surry has more LPIS single failures than Oconee. This results in a RSS value of 4.7×10^{-3} for LPIS failure at Surry compared with a 4.4×10^{-3} value for large LOCAs estimated for Oconee.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The LPIS is one of a group of three systems which provide Emergency Coolant Injection (ECI) to prevent core damage for various break sizes. The other two systems are (1) the High Pressure Injection System (HPIS) and (2) the Core Flooding System (CFS).

The probability of LPIS failure contributes to Event D (ECI) for the large LOCA (breaks >13.5 inches), S_1 LOCA (breaks >10 and <13.5 inches) and S_2 LOCA (breaks 4 to 10 inches). Failure of the LPIS for large and S_2 LOCAs is defined as failure to deliver borated water to the RCS at a flow rate equal or greater than the design output of one LPIS pump. Failure of the LPIS for S_1 LOCAs is failure to deliver borated water at a flow rate equal or greater than the design outout of two LPIS pumps. These failure criteria are given on page 14-57 of the Oconee FSAR.

5.2 OCONEE LPIS MODEL DESCRIPTION

5.2.1 LPIS Boolean Equations

Two Boolean equations of the LPIS were developed. One depicts LPIS failure to provide core flow from at least one loop and is used in the analysis of the large and S_2 LOCAs. The second Boolean equation describes LPIS failure to provide core flow from both LPIS loops and is used in the S_1 LOCA analysis.

The Boolean equation representing failure of both LPIS loops is:

$$\text{LPIS (2 of 2 trains fail)} = A + RCSRBCM + (B + E + J + CH4) \cdot (C + D + K + CH3) + LPISCM + RCSLOCM \cdot RBHICM. \quad \text{(Eq. B6-1)}$$

The Boolean equation representing failure of one LPIS loop is:

$$\text{LPIS (1 of 2 trains fail)} = A + RCSRBCM + B + E + J + CH4 + C + D + K + CH3 + RCSLOCM \cdot RBHICM. \quad \text{(Eq. B6-2)}$$

Table B6-1 relate each term in the above equations to the components shown in Figure B6-1. Table B6-2 lists total component unavailabilities and each of the contributors to the component unavailability. Component unavailabilities were comprised of hardware, human, and maintenance faults.

Testing of LPIS valves was found to negligibly add to the component unavailability when compared to other contributions and was therefore not included.

Only two LPIS pumps were included in the analysis (LP-P1A and LP-P1B). The third pump is manually valved out and was not expected to be available. No maintenance contributions were included in the pump unavailability numbers, however, since it was assumed the third pump would be realigned to provide the redundant flow path. For maintenance contributions and unavailability from other system components, technical specifications state that maintenance is allowed during power operation on any component which will not remove more than one train (flow path) of a system from service. Components shall not be removed from service so that the affected LPIS train is inoperable for more than 24 consecutive hours. If one LPIS train is inoperable for more than 24 hours, the reactor must be shut down. The average maintenance interval used in the Reactor Safety Study is 4.5 months, which corresponds to a frequency of 0.22 per month. From the Reactor Safety Study, (Table III 5-3) the lognormal maintenance act duration for components whose range is limited to 24 hours is a mean time of 7 hours. Therefore, the unavailability of one component due to maintenance is estimated to be:

$$\frac{7(.22)}{720} = 2.1 \times 10^{-3}$$

Testing of the LPIS pumps is conducted monthly. The average outage time for pump test is taken from the RSS as 1.4 hours. The unavailability of the pump due to test is therefore:

$$\frac{1.4}{720} = 1.9 \times 10^{-3}$$

Several common mode failures were identified in the LPIS. Both pump trains can be actuated by a reactor low-low pressure signal or a reactor building high pressure signal. Reactor low-low pressure is signaled by sensor group RCSLO (1500 psig trip) employing a 2 out of 3 logic. Similarly, reactor building high pressure is signaled by sensor group RBHI employing 2 out of 3 logic. A 1×10^{-3} common mode unavailability was attributed to sensor groups RCSLO and RBHI due to a possible human error of miscalibrating two or more sensors in a group. These common mode unavailabilities are designated RCSLOCM and RBHICM in the Boolean equations. A common mode failure in which both sensor groups are miscalibrated in a single human error is represented by the term RCSRBCM. For more details concerning ESPS actuation faults and common mode failure, see Appendix B10.

A final common mode failure identified was the possibility of the three LPIS test line valves connecting both LPIS trains to the BWST being inadvertently left open. If they are, LPIS flow will be recirculated back to the BWST and thus divert water from going into the core. This common mode is represented by the term LPISCM in the Boolean equations for the 2 of 2 train failure case. For the case where only 1 of 2 trains fail, these test line valve failures are incorporated into the Boolean terms D and E.

5.2.2 LPIS Unavailability

Using the Boolean equations given in the last section and the term unavailabilities given in Table B6-1, independent LPIS point estimate unavailabilities per reactor year can be calculated. These are found to be:

$$Q\ (\text{LPIS}) = 4.4 \times 10^{-3}\ (2 \text{ of } 2 \text{ trains fail})$$

and

$$Q\ (\text{LPIS}) = 6.6 \times 10^{-2}\ (1 \text{ of } 2 \text{ trains fail})$$

Double test or maintenance contributions, i.e. components of both trains being deliberately removed from service for maintenance, were removed from these unavailabilities since this condition is not allowed by Technical Specifications.

A quantitative ranking of the Boolean terms for the 1 of 2 LPIS case is given in Table B6-3. As can be noted, approximately 50% of the system unavailability is due to single failures LPISCM and A.

A quantitative ranking of the Boolean terms for the 2 of 2 LPIS case is given in Table B6-4. As can be noted, approximately 98% of the system unavailability is due to the first six single failures.

The reader should be cautioned that these are unavailabilities for Oconee's LPIS if the system is considered independent of all others. In general, the LPIS unavailability will depend on what other system successes or failures have occurred.

Table B6-1. Boolean Equation Term Descriptions[1]

Boolean Term	Term Definition	Term Unavailability
A	LP-28	4×10^{-4}
B	LP-22 + LP-30	3.3×10^{-3}
C	LP-21 + LP-29	3.3×10^{-3}
D	LP-5 + LP-P1A+ LP-31 + LP-11 + LP-12 + LP-15 + LP-17 + LP-48 + TEST A	2.3×10^{-2}
E	LP-8 + LP-P1B + LP-13 + LP-14 + LP-16 + LP-18 + LP-33 + LP-47 + TEST B	2.3×10^{-2}
J	CF - 12	1×10^{-4}
K	CF - 14	1×10^{-4}
CH3[2]	ESPS Actuation Train (Channel 3)	5×10^{-3}
CH4[2]	ESPS Actuation Train (Channel 4)	5×10^{-3}
RCSLOCM[2]	Sensor Group RCSLO Common Mode	1×10^{-3}
RBHICM[2]	Sensor Group RBHI Common Mode	1×10^{-3}
RCSRBCM[2]	Common Mode Failure Between RCSLO and RBHI	3.2×10^{-5}
LPISCM[1]	Common Mode Due to Incorrect Test Valve Position LP TEST	3.0×10^{-3}

1. Refer to Figure B6-1.
2. Refer to Appendix B10.

Table B6-2. Component Unavailabilities

Component Description	Fault Identifiers	Failure Contributors	Q/Component
Check Valve	CF - 12		
	CF - 14		
	LP - 29		
	LP - 30		
	LP - 31		
	LP - 33		
	LP - 47		
	LP - 48	Hardware	1×10^{-4}
		Q Total	1×10^{-4}
Pump		Hardware	1×10^{-3}
	LP - P1A	Control Circuitry	1.8×10^{-3}
	LP - P1B	Test	1.9×10^{-3}
		Q Total	4.7×10^{-3}
Motor Operated Valve (Normally Closed)		Hardware	1×10^{-3}
		Plugged	1×10^{-4}
	LP - 18	Control Circuitry	6.4×10^{-3}
	LP - 17	Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}
Motor Operated Valve (Normally Open)	LP - 5		
	LP - 8		
	LP - 12		
	LP - 14	Operator Error	1×10^{-3}
	LP - 21	Plugged	1×10^{-4}
	LP - 22	Maintenance	2.1×10^{-3}
		Q Total	3.2×10^{-3}
Manual Valve (Normally Closed)	LP - 15		
	LP - 16	Operator Error	1×10^{-3}
		Q Total	1×10^{-3}
Manual Valve (Normally Open)	LP - 11	Plugged	1×10^{-4}
	LP - 13	Operator Error	1×10^{-4}
		Q Total	2×10^{-4}
BWST Manual Isolation Valve		Plugged	1×10^{-4}
	LP - 28	Operator Error	3×10^{-4}
		Q Total	4×10^{-4}
Test Lin Valves Inadverte tly Open	TEST A		
	TEST B	Human Error	1×10^{-3}
		Q Total	1×10^{-3}

Table B6-3. Quantitative Ranking of Terms in Two of Two Trains Fail LPIS Boolean Equation

LPISCM	3.0×10^{-3}
E·D	5.3×10^{-4}
A	4×10^{-4}
E·CH3	1.2×10^{-4}
CH4·D	1.2×10^{-4}
B·D	7.6×10^{-5}
E·C	7.6×10^{-5}
RCSRBCM	3.2×10^{-5}
CH4·CH3	2.5×10^{-5}
CH4·C	1.7×10^{-5}
B·CH3	1.7×10^{-5}
B·C	1.1×10^{-5}
E·K	2.3×10^{-6}
J·D	2.3×10^{-6}
RCSLOCM·RBHICM	1×10^{-6}
J·CH3	5×10^{-7}
CH4·K	5×10^{-7}
J·C	3.3×10^{-7}
B·K	3.3×10^{-7}
J·K	1×10^{-8}
	4.4×10^{-3}

Table B6-4. Quantitative Ranking of Terms in One of Two Trains Fail LPIS Boolean Equation

E	2.3×10^{-2}
D	2.3×10^{-2}
CH4	5×10^{-3}
CH3	5×10^{-3}
B	3.3×10^{-3}
C	3.3×10^{-3}
LPISCM	3.0×10^{-3}
A	4×10^{-4}
J	1×10^{-4}
K	1×10^{-4}
RCSRBCM	3.2×10^{-5}
RCSLOCM·RBHICM	1×10^{-6}
	6.6×10^{-2}

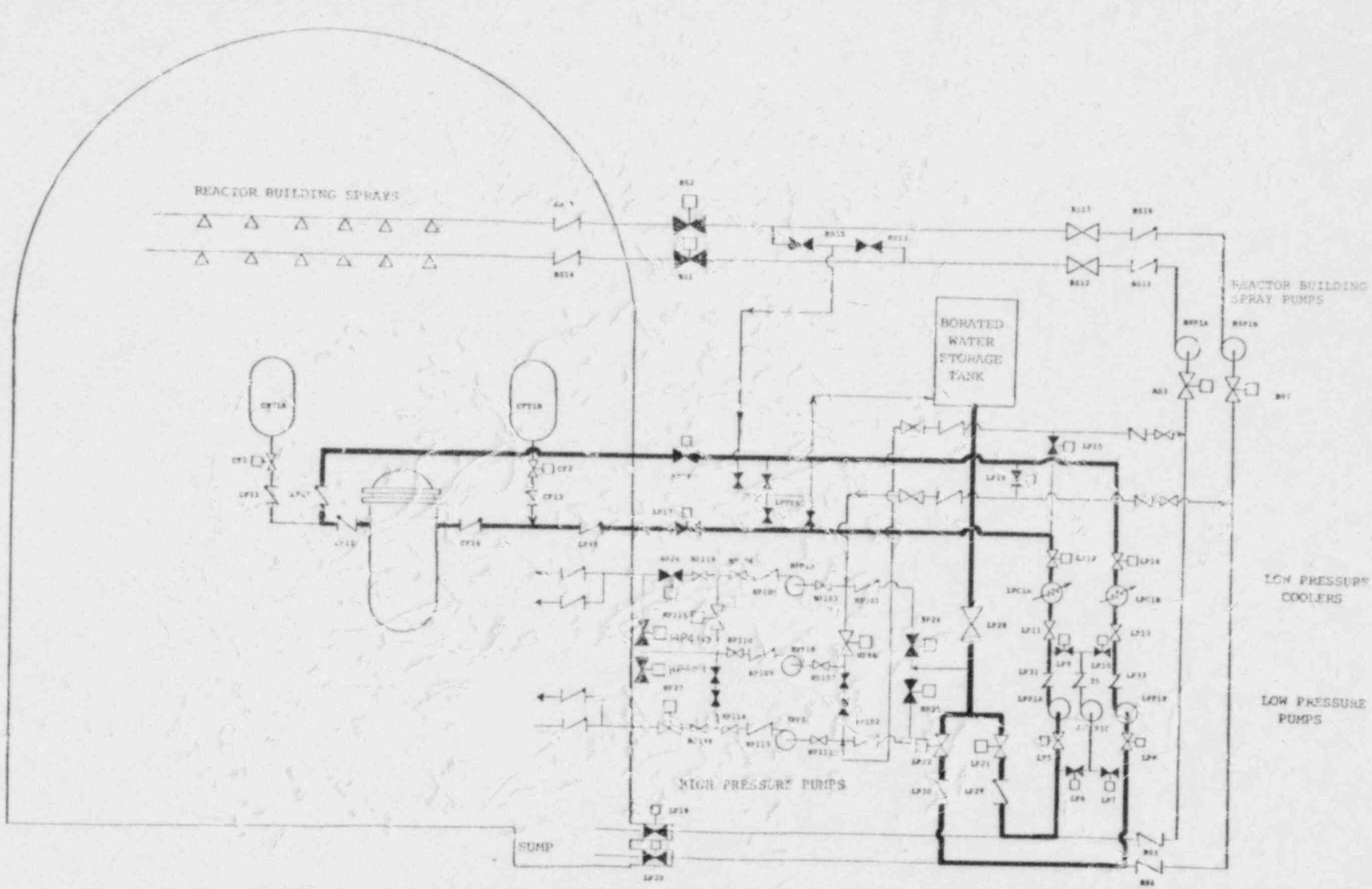


Figure B6-1. Oconee ECCS Schematic (LPIS Highlighted)

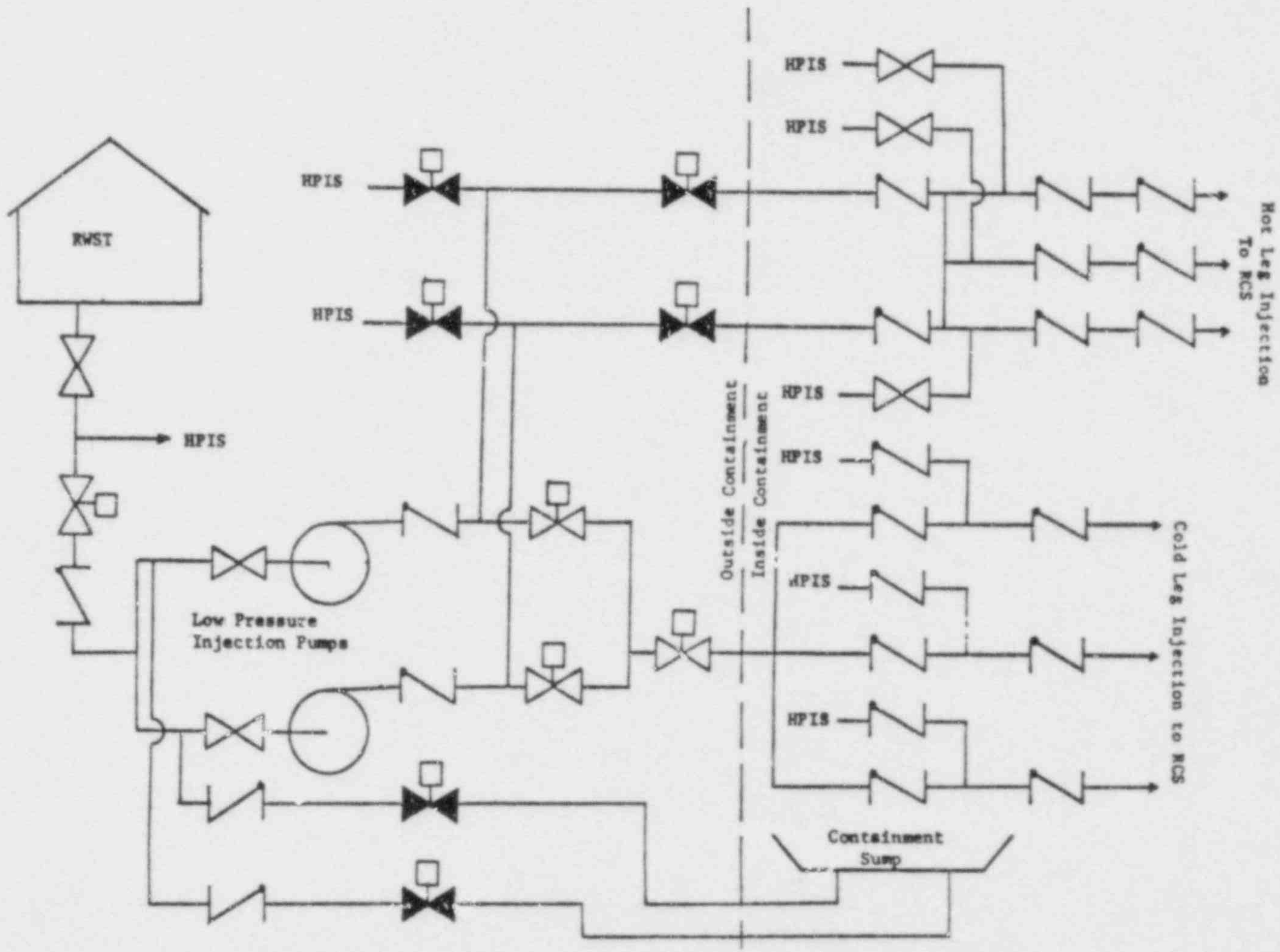


Figure B6-2. Surry LPIS Schematic (Normal Operation)

APPENDIX B7

SURVEY AND ANALYSIS

LOW PRESSURE RECIRCULATION SYSTEM (LRPS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Low Pressure Recirculation System (LPRS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The LPRS designs for Oconee and Surry are described in Sections 2 and 3 of this report, respectively. A comparison of the two low pressure recirculation systems is given in Section 4. LPRS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate LPRS failures into the Oconee accident sequences and a point estimate of the LPRS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE LPRS DESCRIPTION

2.1 System Description

The LPRS (Figure B7-1) is a system which provides two separate flow paths for recirculating water from the containment sump to the reactor vessel. Flow enters the reactor vessel through two core flooding nozzles located on opposite sides of the vessel. Each flowpath of the LPRS includes an electric pump with 3000 gpm flow rate, a shell and tube heat exchanger, and associated piping and valves. Comparison of Figure B6-1 and B7-1 reveals that the LPRS pumps and many valves are shared with the Low Pressure Injection System.

Long term core cooling by the LPRS is achieved by rejecting the core decay heat contained within the LPRS water to the Low Pressure Service Water (LPSW) System via the heat exchangers (see Appendix B14 for analysis of the LPSW system). A third spare pump, which is normally valved out, can be put in either flow path as required. Passive miniflow by-pass lines are employed to prevent pump overheating and loss of suction.

2.2 System Operation

As stated in Section 2.1, the majority of the equipment used in the LPRS is first used by the LPIS (see Appendix B6). When the borated water storage tank is approximately 94% empty a low water alarm is annunciated in the control room. Upon receipt of this alarm the operator must realign certain valves to recirculate water from the reactor building sump to the reactor. Specifically, the two valves from the sump (LP-19 and LP-20) must be opened and the two valves from the borated water storage tank (LP-21 and LP-22) must be closed.

3.0 SURRY LPRS DESCRIPTION

The LPRS in the Surry plant shown in Figure B7-2 includes the containment sump, two pumps in parallel (each capable of delivering 3000 gpm at a 225 foot head), and associated valves and piping. There are 3 discharge lines, one to each of 3 cold legs of the RCS. Each discharge line has 2 check valves. There is one normally open motor operated valve in the common feeder line to the three discharge lines and two normally open motor operated valves in each pump discharge line. When the RWST is approximately 86% empty, as indicated by a low RWST level alarm, the operator must realign the LPIS to recirculate water from the containment sump to the RCS cold legs. After 24 hours for large pipe break accidents, the operator must realign the LPRS to recirculate water to the 3 RCS hot legs. Individual headers provide water from the containment sump to each LP pump. Either pump will provide sufficient flow into the RCS. Flow through any one cold leg or any one hot leg (after 24 hours) is sufficient.

4.0 COMPARISON OF OCONEE AND SURRY LPRS

The Oconee and Surry LPRS are similar in that they employ redundant trains to deliver water to the RCS from the sump following a LOCA. Both systems use the same pumps as in their LPIS and both require operator action to realign the pump suction from the BWST or RWST to the containment sump at the start of the recirculation phase. The Surry system also requires operator action after 24 hours to realign LPRS flow from RCS cold legs to the hot legs. This later realignment is not necessary for the Oconee system. Failure to perform any of the above realignments constitutes a common mode failure of the system due to human error. The contribution to system unavailability due to common mode failures is greater for Surry than for Oconee. This results in an RSS value of 1.3×10^{-2} for Surry compared to a 4.0×10^{-3} value estimated for Oconee.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The LPRS is one of two systems providing Emergency Coolant Recirculation (ECR), event H on the LOCA event trees, to prevent core damage for various break sizes. The other system is the High Pressure Recirculation System (HPRS). Successful ECR requires the operation of one of two LPRS trains for A, S_1, and S_2 LOCAs. For S_3 and transient induced LOCAs, ECR requires one of three HPRS trains as well as a corresponding LPRS train (see Appendix B9).

5.2 LPRS Model Description

5.2.1 LPRS Boolean Equation

The following Boolean equation was developed to model LPRS failure:

$$LPRS = (B + J + CH4 + E + E' + X) \cdot (C + K + CH3 + D + D' + W) + WXCM \quad \text{(Eq. B7-1)}$$

Each term in the above equation except for E', X, D', W and WXCM is described in Section 5.2 of the LPIS Appendix B6. Tables B7-1 and B7-2 list descriptions of the remaining terms and component unavailability estimates. These unavailabilities are comprised of hardware, human, and maintenance faults. Testing of the LPRS valves was found to negligibly add to the valve unavailability when compared to other contributions and was therefore not included. It should be noted that the primed events E' and D' represent failure of the low pressure pumps during the recirculation phase.

Maintenance unavailabilities previously not discussed in the LPRS appendix are due to the sump MOVs LP-19 and LP-20. The technical specifications state that maintenance is allowed during power operation on any component which will not remove more than one train (flow path) of a system from service. The component shall not be removed from service so that the affected train is inoperable for more than 24 consecutive hours. The average maintenance interval used in the RSS is 4.5 months, which corresponds to a frequency of 0.22 per month. From the Reactor Safety Study (Table III T-3), the log normal maintenance act duration for components whose range is limited to 24 hours is 7 hours. The unavailability of valves LP-19 and LP-20 due to a maintenance outage is therefore estimated to be:

$$\frac{7(.22)}{720} = 2.1 \times 10^{-3} \quad .$$

A common mode failure of the LPRS was identified. When the BWST is 93% empty a control room alarm notifies the operator to realign the low pressure pump suction from the BWST to the sump. To do this, the operator stops the pumps, opens LP-19 and LP-20, closes LP-21 and LP-22 and restarts the pumps. Failure to realign to the sump would fail the pumps upon emptying the BWST. This common mode failure due to operator error was assessed as 3×10^{-3} and is designated WCXM.

5.2.2 LPRS Unavailability

Using the Boolean equation given in the last section and the term unavailabilities given in Table B6-1 and B7-1 an independent LPRS point estimate unavailability can be calculated. This is found to be:

$$\text{LPRS} = 4.0 \times 10^{-3}/\text{reactor year} \quad .$$

"Double" test and maintenance contributions, i.e. a deliberate action specifying both trains to be tested or maintenanced simulataneously, were not included in this unavailability estimate because such an action would violate technical specifications. Further, it can be seen that reduction of the Boolean equation describing the LPRS results in 37 terms. Examination of these terms shows that 16 depict "double injection" failures of the LPRS, i.e. LPRS failure due to failure of redundant components during low pressure injection which describe the low pressure injection system. These failures were not included in the calculations of the independent LPRS unavailability above since the LPIS must have succeeded (at least one train) to demand LPRS.

For calculation of the unavailability as used in the accident sequence analysis, double injection failures and other physically inconsistent failure contributors were eliminated according to the Boolean reduction process where the equations describing each of the systems involved in the sequence were condensed together.

A quantitative ranking of the Boolean terms is given in Table B7-3. As can be noted approximately 75% of the system unavailability is due to WXCM.

The reader should be cautioned that these are unavailabilities for Oconee's LPRS if the system is considered independent of all others. In general, the LPRS unavailability will depend on what other system successes or failures have occurred, i.e. the unavailability used for the LPRS in the sequence analysis calculation must be a conditional unavailability.

Table B7-1: Boolean Equation Term Description

Boolean Term	Term Definition	Term Unavailability
D'	LP-P1A	3.5×10^{-3}
E'	LP-P1B	3.5×10^{-3}
W	LP-19	9.6×10^{-3}
X	LP-20	9.6×10^{-3}
WXCM	Common Mode - Due to the failure of the Operator to realign for recirculation (Open LP-19, LP-20 and close LP-21, LP-22 and restart pumps)	3×10^{-3}

Table B7-2: Component Unavailabilities

Component Description	Fault Identifier	Failure Contributors	Q/Component
Pump	LP-P1A LP-P1B	Hardware (Fails to restart)	1×10^{-3}
		Control Circuitry	1.8×10^{-3}
		Fails to operate 24 hrs (3×10^{-5}/hr)	7.2×10^{-4}
		Q Total	3.5×10^{-3}
Motor Operated Valve (Normally Closed)	LP-19 LP-20	Hardware	1×10^{-3}
		Plugged	1×10^{-4}
		Control Circuitry	6.4×10^{-3}
		Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}

Table B7-3. Quantitative Ranking in Terms in LPRS Boolean Equation

WXCM	3.0×10^{-3}
D·X	2.2×10^{-4}
W·E	2.2×10^{-4}
W·X	9.2×10^{-5}
D'·E	8.1×10^{-5}
D·E'	8.1×10^{-5}
W·CH4	4.8×10^{-5}
CH3·X	4.8×10^{-5}
C·X	3.2×10^{-5}
W·B	3.2×10^{-5}
D'·X	3.4×10^{-5}
W·E'	3.4×10^{-5}
D'·CH4	1.8×10^{-5}
CH3·E'	1.8×10^{-5}
D'·E'	1.2×10^{-5}
C·E'	1.2×10^{-5}
D'·B	1.2×10^{-5}
W·J	9.6×10^{-7}
K·X	9.6×10^{-7}
K·E'	3.5×10^{-7}
D'·J	3.5×10^{-7}
	4.0×10^{-3}

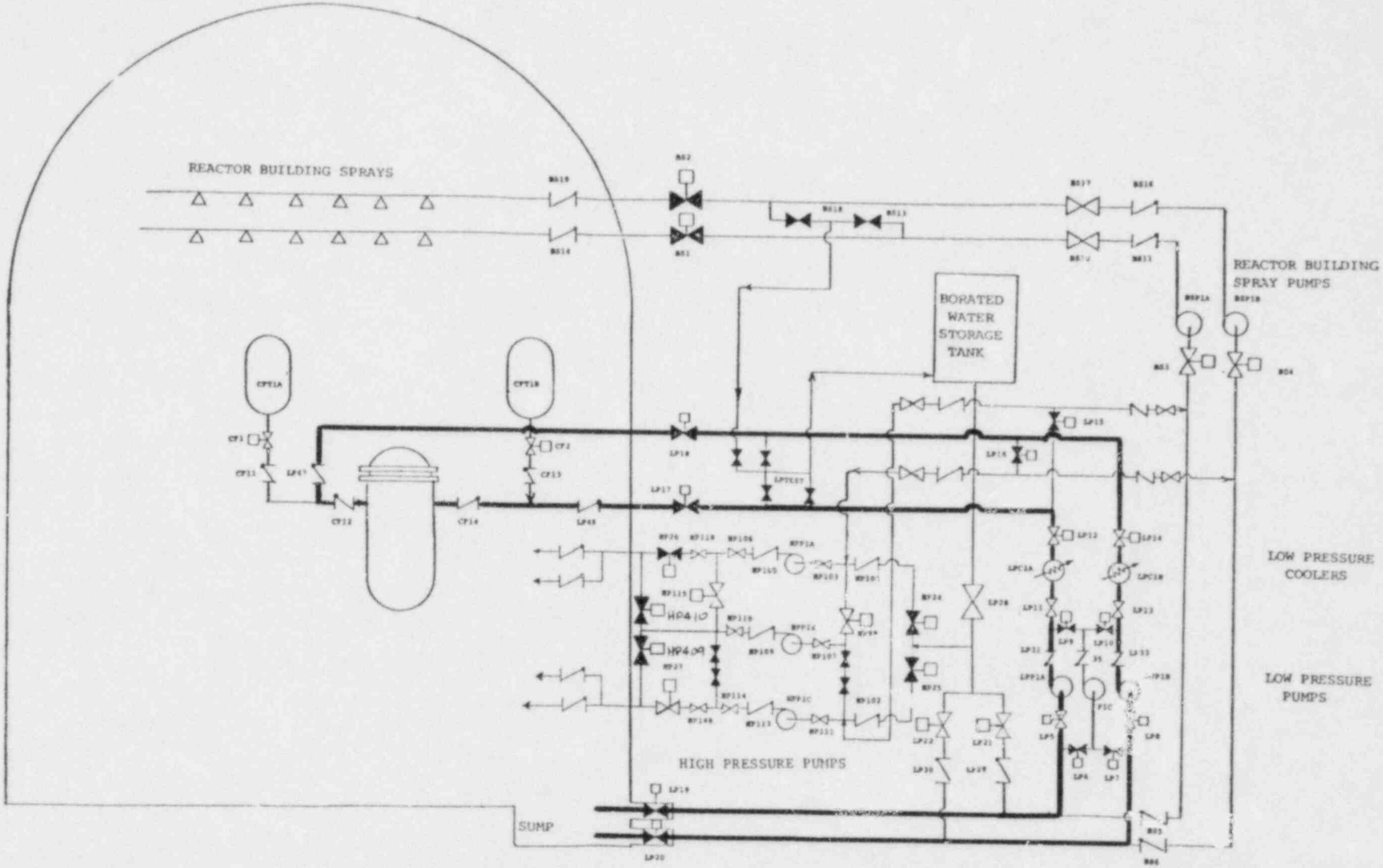


Figure B7-1. Oconee ECCS Schematic (LPRS Highlighted)

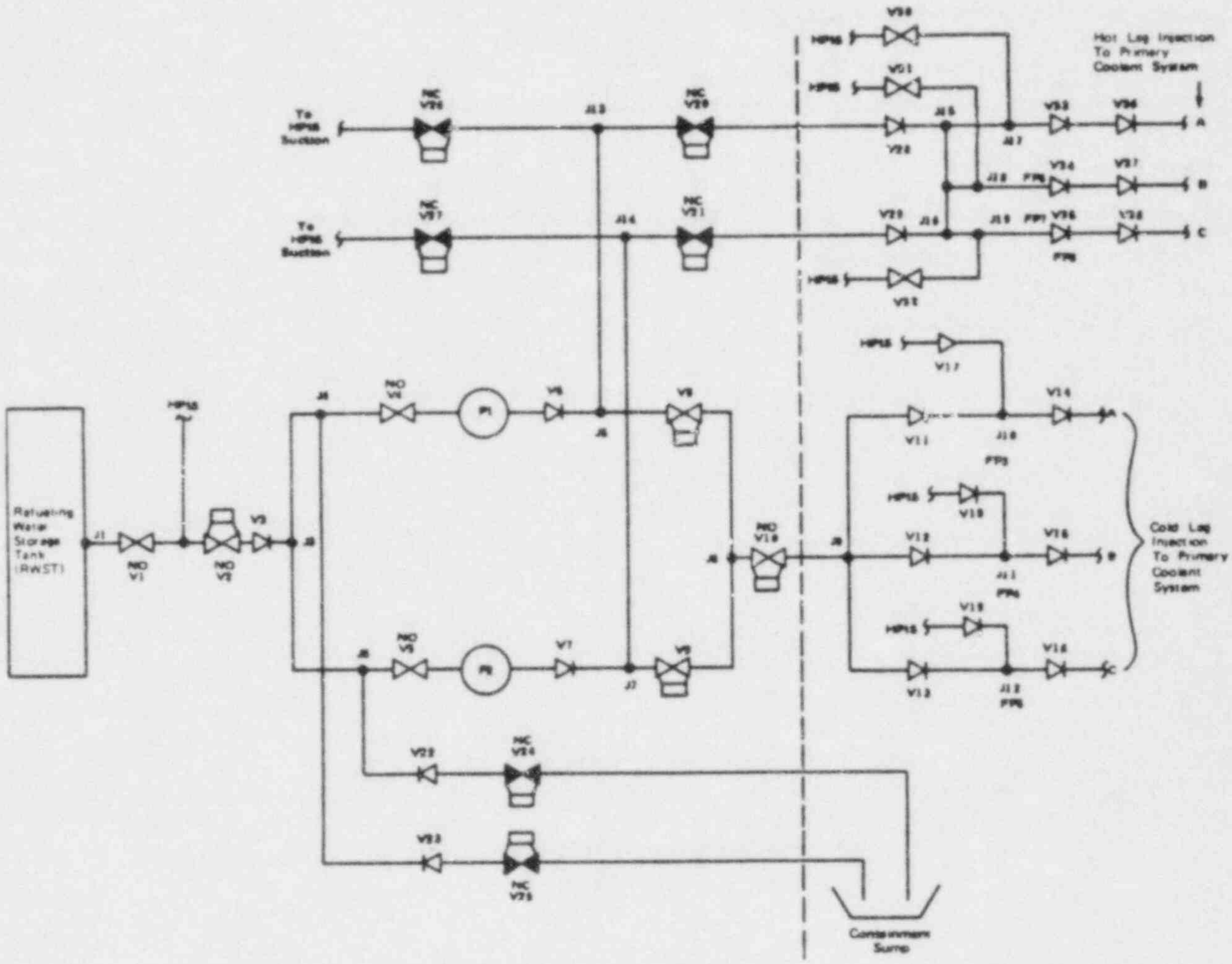


Figure B7-2. Surry LPRS

APPENDIX B8

SURVEY AND ANALYSIS

HIGH PRESSURE INJECTION SYSTEM (HPIS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 High Pressure Injection System (HPIS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The HPIS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two high pressure injection systems is given in Section 4. HPIS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate HPIS failures into the Oconee accident sequences and a point estimate of the HPIS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE HPIS DESCRIPTION

2.1 System Description

The High Pressure Injection System along with the Low Pressure Injection System (LPIS) and the Core Flooding System (CFS) form collectively the overall Emergency Core Cooling System (ECCS), which is designed to prevent core damage over the entire spectrum of RCS LOCA sizes. Figure B8-1 shows the ECCS for one reactor unit. High pressure injection is necessary to prevent uncovering of the core for small LOCAs, where high system pressure is maintained, and to delay uncovering of the core for intermediate-sized LOCAs. The HPIS can also be used to cool the core following a non-LOCA reactor shutdown (e.g., transient). This mode of HPIS operation would be utilized only if normal and emergency secondary heat removal via the steam generators cannot be achieved.

The HPIS is arranged so that three pumps are available for emergency use to inject borated water from the Borated Water Storage Tank (BWST) to the RCS. During normal operation, the HPIS recirculates reactor coolant for purification and for supply of seal water to the reactor coolant circulating pumps. One of the three high pressure injection pumps is normally in operation and a positive static head of water assures that all pipes are filled with water.

Each high pressure injection pump can deliver 450 gpm at 1700 psig reactor vessel pressure. Water is drawn through a single suction header from the BWST and pumped through injection lines which enter the reactor building on opposite sides. Each injection line splits into two lines inside the reactor building, but outside the secondary missile shield, to provide four injection paths to the four RCS cold legs. The four connections to the RCS are located between the reactor coolant pump discharge and the reactor inlet nozzles.

Successful operation of the HPIS pumps requires lubrication oil cooling and pump seal cooling. Charging pump cooling is accomplished via the Low Pressure Service Water (LPSW) System where heat generated in the pump lubricating oil and seals is removed via heat exchangers and transferred to the ultimate heat sink.

Electric power is supplied to the three HPIS pumps by three independent 4160 V buses.

2.2 System Operation

The HPIS is initiated at:

1. a low RCS pressure of 1500 psig or,
2. a reactor building pressure of 4 psig.

Automatic actuation of the valves and pumps by the Engineered Safeguards Protective System (ESPS) channels 1 and 2 switches the system from its normal operating mode to the emergency operating mode to deliver water from the BWST into the reactor vessel through the reactor coolant inlet lines. The following automatic actions occur on receipt of an ESPS signal:

a. The isolation valves (HP-3, 4 and 5) in the purification letdown line and valves (HP-20, 21) in the seal return lines close (not shown in Figure B8-1).

b. All high pressure injection pumps start.

c. The inlet valve HP-26 opens.

d. The valves (HP-24, 25) in the lines connecting to the BWST outlet header open.

After receiving an actuation signal, the HPIS valves will reach full open within 6 seconds. Operation of the HPIS in the emergency mode will continue until system operation is manually terminated. The pumps are designed so that periodic testing may be performed to assure operability and ready availability.

The HPIS may also be started manually from the control room. This mode of HPIS actuation would be used if the system is required following a non-LOCA caused reactor shutdown in which all heat removal capability through the steam generators is lost. This capability is useful for conditions in which the RCS is losing inventory, but the RCS pressure is being maintained above the low pressure actuation set point. In this mode of operation the operator could cool the core by injecting HPI water and allowing it to boil off through the pressurizer relief valves.

3.0 SURRY HPIS DESCRIPTION

The Surry High Pressure Injection System provides a high pressure source of emergency cooling water to the RCS in the event of of a LOCA. Figure B8-2 is a simplified system diagram of the HPIS.

The HPIS uses the high pressure charging pumps to draw water through a single suction header from the Refueling Water Storage Tank (RWST) and injects the water through a single discharge header into the cold legs. Another function of the HPIS is to push the 12 weight percent boric acid solution in the 900 gallon Boron Injection Tank (BIT) into the RCS in order to provide fast injection of boron to the reactor core for reactivity suppression. The injection of the 12 weight percent boron from the BIT was concluded not to be a critical requirement for HPIS success in response to a LOCA.

During normal plant operation, one operating charging pump draws water from the Volume Control Tank (VCT) and discharges it as makeup to the normal charging line and seal coolant to the pump seal injection line. Actuation of the Safety Injection Control

System (SICS) will:

a. Open parallel RWST supply valves 1115B and D to provide the RWST emergency water for HPIS pump (charging pump) suction;

b. Start the standy charging pumps;

c. Close the VCT isolation valves LCV-1115C and E (in series) to prevent draining the VCT;

d. Close the normal charging line isolation valves 1289A and B (in series);

e. Open the parallel BIT isolation valves 1867A and B, at the BIT inlet, and 1867C and D at the BIT outlet;

f. Close the boric acid recirculation line trip valves 1884A, B and C, to terminate low pressure recirculation of 12 weight percent boric acid solution between the Boric Acid Tanks (BAT) and the BIT:

g. Close the charging system mini-flow valves.

After the SICS changes the HPIS valve positions, all operable charging pumps will pump water from the RWST to discharge header CH-80, through HPIS line SI-57 through the BIT, and to the RCS cold legs through lines common with the LPIS. The actuation of the HPIS for injection is entirely automatic.

The 12 weight percent boric acid solution is normally recirculated between the Boric Acid Tank (BAT) and the BIT by one of two redundant boric acid transfer pumps. The boric acid recirculation serves to assure that the BIT is full and to help prevent boron precipitation by keeping the solution mixed.

Boron precipitation in the 12 weight percent boric acid solution will occur at a temperature below 130°F. The contents of the BIT and those sections of HPIS piping isolated by the BIT isolation valves are maintained above the precipitation temperature by strip heaters on the BIT and heat tracing on the piping and valves, including the boric acid recirculation piping. Temperature alarms and backup heaters are provided should any of the heaters or heat tracing circuits fail. Transfer to the backup heaters for heat tracing is manual. Undetected heat tracing failure will result in precipitation of boric acid solution within 4 to 5 hours and will fail the HPIS.

Successful longterm operation of the charging pumps requires lubrication oil cooling and pump seal cooling. Plant personnel estimate that the charging pumps can operate for 30 to 45 minutes without lubricating oil or seal cooling.

4.0 COMPARISON OF OCONEE AND SURRY HPIS

The Oconee HPIS is similar to the Surry HPIS in that each have three high pressure pumps which take suction from a 350,000 gallon borated water supply (~2000 ppm boron). Both systems have a single header which connects this borated water supply to the charging pumps.

The three high pressure pumps of Surry are all completely interconnected by normally open motor operated valves, whereas Oconee has two manually operated normally closed valves in the pump suction and discharge header.

A design difference that gives rise to a change in the Oconee's HPIS unavailability is the valve configuration between the pump discharge and the reactor vessel. The pump discharge in the Surry HPIS feeds a common header which contains the BIT.

The operation of Surry's BIT is necessary for successful HPIS operation. Failure of the BIT due to precipitation of the twelve 12 percent boric acid solution contained in the BIT and its associated piping can plug the valves or lines of the HPIS. This failure mode does not apply to the Oconee HPIS since Oconee has separate discharge headers and does not have the equivalent of a BIT. The Surry system therefore has more single failures.

Another major difference between the systems is the type of pumps used. The Oconee HPIS pumps deliver adequate flow at normal RCS operating pressure to cool the core if heat removal via the steam generators fails. The Surry pumps, however, do not have the capability to deliver adequate flow at RCS pressures to cool the core. This makes the requirement for heat removal via the steam generators more critical at the Surry reactor.

These differences are reflected in the different system unavailabilities. The RSS estimated a 8.6×10^{-3} HPIS unavailability for Surry while the Oconee unavailability for LOCAs was estimated at 1.4×10^{-3}.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The HPIS is one of the three subsystems of the ECCS which provide injection of coolant to the core to prevent damage for various break sizes. The remaining two subsystems are the LPIS and the CFS.

Failure of the HPIS contributes to event D (ECI) on the A (>13.5" break), S_1 (10"-13.5" break), the S_2 (4"-10" break), the S_3 (0-4" break), and the transient induced LOCA event trees. The HPIS also contributes to event U (Primary System Makeup) on the transient event trees. Failure to deliver water to the reactor core at a flow rate of less than the design output of one high pressure pump at full head constitues HPIS failure.

5.2 HPIS Model Description

5.2.1 HPIS Boolean Equations

The general form of the HPIS Boolean equation representing failure of the HPIS system considering one of the trains is required for success is:

$$\begin{aligned} HPIS = & (A1 + CH1 + D1 \cdot E1 + C1) \cdot (B1 + CH2) + A \\ & + RCSRBCM + RCSLOCM \cdot RBHICM + LPSW + HPMAN \\ & + LOPNRE \qquad \text{(Eq. B8-1)} \end{aligned}$$

The above equation, except for the last two terms, was used in the analysis of all LOCA sequences (A, S_1, S_2, S_3) and the analysis of transient induced LOCA sequences where AC power is available (T_1Q, T_2Q, and T_3Q). Equation B8-1 without the last two terms is referred to as Eq. B8-1(a) in the main report chapters. Equation B8-1, without the last term, was used to analyze all normal transients except the station blackout transient ($T_1(B_3)$) and is referred to as Equation B8-1(b) in the main report. For $T_1(B_3)$ sequences, all of Eq. B8-1 was used. For $T_1(B_3)Q$ sequences, where there is a stuck-open relief valve and a station blackout, HPIS failure is assessed to be unity. This is because, under these circumstances, core damage is assumed to begin quickly and recovery of offsite power is not assumed to occur in the short time interval.[1]

Table B8-1 relates each term in the above equation to the components shown in Figure B8-1. Table B8-2 lists total component unavailabilities and each of the contributors to the component unavailability.

The unavailabilities listed in Table B8-2 are comprised of hardware, human and maintenance faults. Testing of HPIS valves and pumps was found to negligibly add to the valve and pump unavailability when compared to other contributions and was therefore not included.

Two high pressure injection pumps shall be maintained operable to provide redundant and independent flow paths. Maintenance shall be allowed during power operation on any component which will not remove more than one train (flow path) of a system from service. Components shall not be removed from service so that the affected system is inoperable for more than 24 consecutive hours after which it will be shutdown. The average maintenance interval used in the Reactor Safety Study is 4.5 months, which corresponds to a frequency of 0.22 per month. From the Reactor Safety Study, Table III 5-3, the log-normal maintenance act duration for components whose range is limited to 24 hours is a mean time of 7 hours. The unavailability of one component due to maintenance is estimated to be:

$$\frac{7(.22)}{720} = 2.1 \times 10^{-3}$$

---

[1] This assumption is consistent with the WASH-1400 treatment of the S_2B sequence. A detailed analysis of this sequence may indicate that core damage begins at a time significantly later than that assumed.

Several common mode failures were identified in the HPIS. Both pump trains can be actuated by a reactor low-low pressure signal or a reactor building high pressure signal. Reactor low-low pressure is signaled by sensor group RCSLO employing a 2 out of 3 logic. Similarly, reactor building high pressure is signaled by sensor group RBHI employing 2 out of 3 logic. A 1×10^{-3} common mode unavailability was attributed to sensor groups RCSLO and RBHI as the dominant failure contributor due to a possible human error of miscalibrating two or more sensors in a group. These common mode unavailabilities are designated RCSLOCM and RBHICM in the Boolean equation. A common mode failure in which both sensor groups are miscalibrated in a single human error is represented by the term RCSRBCM. For more details concerning ESPS actuation faults and common mode failure, see Appendix B10.

5.2.2 HPIS Unavailability

Using the Boolean equations given in the last section and the term unavailabilities given in Table B8-1, independent HPIS point estimate unavailabilities can be calculated. These are found to be:

Q (HPIS) = 1.4×10^{-3}	(Applies to A, S_1, S_2, S_3 and transient induced LOCAs)
Q (HPIS) = 1.6×10^{-2}	(Applies to transients with AC power available)
Q (HPIS) = 2.2×10^{-1}	(Applies to transients with no AC power initially available)

Double maintenance contributions were removed from these unavailabilities since both trains being out for maintenance at the same time is not allowed by Technical Specifications.

A quantitative ranking of the Boolean terms for the 1 of 3 HPIS case in response to LOCAs with AC power available is given in Table B8-3. As can be noted, approximately 90% of the system unavailability is due to the first 4 terms. For the case in which the HPIS is asked to respond to a transient with AC power available the unavailability is dominated by the Boolean term HPMAN. For transients without AC power, the unavailability is dominated by the term LOPNRE.

The reader should be cautioned that these are unavailabilities for Oconee's HPIS if the system is considered independent of all others. In general, the HPIS unavailability will depend on what other system successes or failures have occured. Further, when calculating sequence probabilities, possible common mode failures among systems must be considered if the systems are not independent. An example of this is valve LP-28 which contributes to both HPIS and LPIS unavailability.

Table B8-1. Boolean Equation Term Descriptions

Boolean Term	Term Definitions	Term Unavailability
A	LP-28	4×10^{-4}
B1	HP-27 + HP-148 + HP-114 + HP-113 + HP-P1C + HP-111 + HP-102 + HP-25	3.5×10^{-2}
A1	HP-26 + HP-118	9.8×10^{-3}
C1	HP-101 + HP-24	9.8×10^{-3}
E1	HP-98 + HP-107 + HP-P1B + HP-109 + HP-110	* (running in makeup mode)
D1	HP-103 + HP-P1A + HP-105 + HP-106	1.6×10^{-2}
**CH1	ESPS Actuation Train (Channel 1)	5×10^{-3}
**CH2	ESPS Actuation Train (Channel 2)	5×10^{-3}
**RCSLOCM	Sensor Group RCSLO Common Mode	1×10^{-3}
**RBHICM	Sensor Group RBHI Common Mode	1×10^{-3}
**RCSRBCM	Common Mode Failure Between RCSLO and RBHI	3.2×10^{-5}
***LPSW	Low Pressure Service Water Pump Cooling	2.7×10^{-5}
HPMAN	Operator Fails to Start System (Event U Only)	1.5×10^{-2} (see footnote 4)
LOPNRE	Offsite Power Not Restored Within 1/2-1 Hr. (Applies to Loss of all AC Power Only)	2×10^{-1}

*Refer to Appendix B1
**Refer to Appendix B10
***Refer to Appendix B14
****$1.5 \times 10^{-2} = (3 \times 10^{-3}) \times 5$; where 10^{-3} is the basic human error of commission. This value is increased by a factor of 5 to reflect a moderately high stress situation (reference NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications).

Table B8-2. Component Unavailabilities

Component Description	Fault Identifiers	Failure Contributors	Q/Component
Check Valve	HP-101 HP-102 HP-105 HP-113	Hardware	1×10^{-4}
		Q Total	1×10^{-4}
Pump	HP-P1A HP-P1C	Hardware	1×10^{-3}
		Control Circuitry	1.2×10^{-3}
		Lube Oil to Viscous	1×10^{-2}
		Service Water Not Valved In	1×10^{-3}
		Maintenance	2.1×10^{-3}
		Test	1.9×10^{-3}
		Q Total	1.7×10^{-2}
Motor Operated Valve (Normally Closed)	HP-26 HP-27 HP-24 HP-25	Hardware	1×10^{-3}
		Plugged	1×10^{-4}
		Control Circuitry	6.4×10^{-3}
		Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}
Manual Valve (Normally Open)	HP-118 HP-106 HP-103 HP-148 HP-114 HP-111	Plugged	1×10^{-4}
		Operator Error	1×10^{-4}
		Q Total	2×10^{-4}
BWST Manual Isolation Valve	LP-28	Plugged	1×10^{-4}
		Operator Error	3×10^{-4}
		Q Total	4×10^{-4}

Table B8-3. Quantitative Ranking of Boolean Equation Terms

A	4×10^{-4}
C1·B1	3.4×10^{-4}
A1·B1	3.4×10^{-4}
CH1·B1	1.8×10^{-4}
A1·CH2	4.9×10^{-5}
C1·CH2	4.9×10^{-5}
RCSRBCM	3.2×10^{-5}
LPSW	2.7×10^{-5}
CH1·CH2	2.5×10^{-5}
RCSLOCM·RBHICM	1×10^{-6}
D1·E1·B1	ϵ
D1·E1·CH2	ϵ
	1.4×10^{-3}

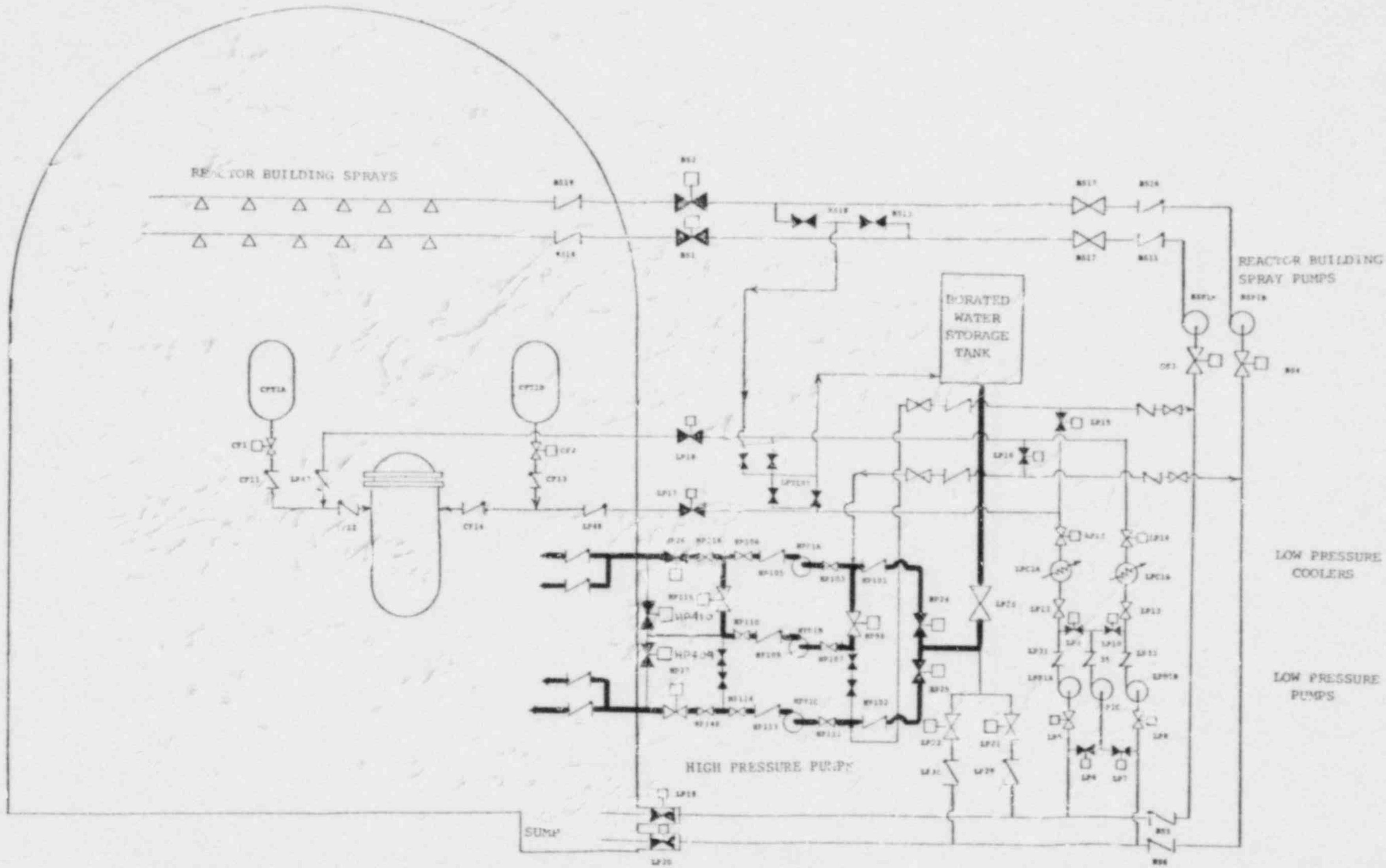


Figure B8-1. Oconee ECCS Schematic (HPIS Highlighted)

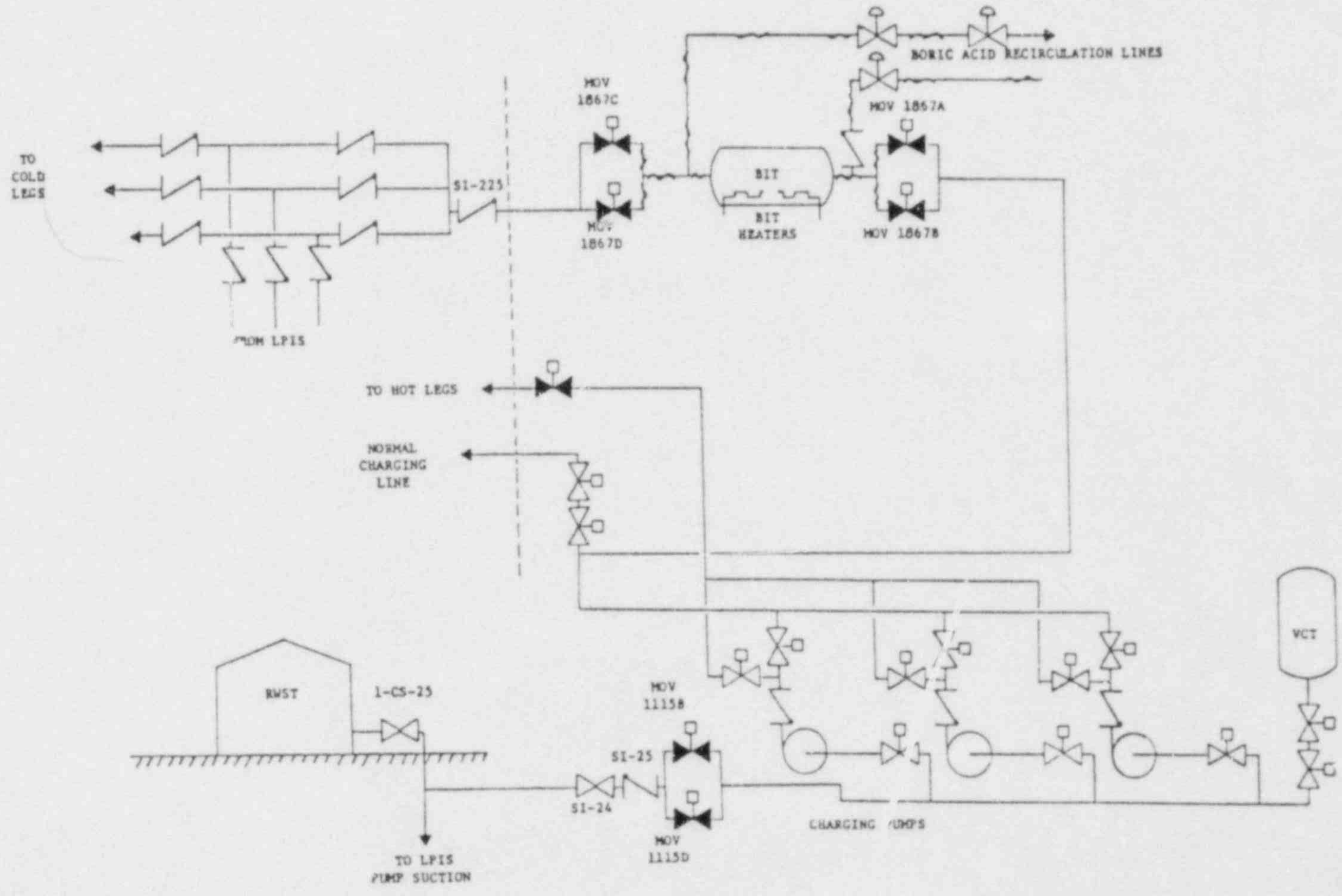


Figure B8-2. Surry HPIS Schematic (Normal Operation)

APPENDIX B9

SURVEY AND ANALYSIS

HIGH PRESSURE RECIRCULATION SYSTEM (HPRS) - OCONEE PLANT

TABLE OF CONTENTS

1. INTRODUCTION

The Oconee Unit 3 High Pressure Recirculation System (HPRS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The HPRS designs for Oconee and Surry are described in Sections 2 and 3 of this report, respectively. A comparison of the two high pressure recirculation systems is given in Section 4. HPRS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate HPRS failures into the Oconee accident sequences and a point estimate of the HPRS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE HPRS DESCRIPTION

2.1 System Description

The HPRS is one of two systems designed for long-term core cooling following a LOCA. The other system is the Low Pressure Recirculation System (LPRS). After exhaustion of the BWST, the LPRS and HPRS are used to recirculate water from the containment sump to the RCS. If the LOCA is large enough, the RCS will be at a low enough pressure so that only the LPRS would be required. If the LOCA is small, however, the RCS will be at a pressure above the shutoff head of the LPRS pumps and the HPRS would be required. As can be seen in Figure B9-1, for these LOCAs, the HPRS and the LPRS are both required, since the HPRS takes its suction from the discharge of the LPRS.

As discussed in Appendix B-7, the LPRS must be realigned by the operator for sump suction and discharge directly into the reactor vessel. The HPRS serves the same function as the LPRS, except that it delivers water into the RCS cold legs at high pressure and takes its suction from the LPRS discharge. The HPRS, highlighted in Figure B9-1, consists of three pumps and associated pipes all designed for high pressure operation. Following exhaustion of the BWST, a portion of the LPRS pump discharge is diverted through the HPRS for recirculation into the RCS cold legs. (The remaining portion is diverted to the containment spray headers.) There are two separate flow paths from the LPRS to the HPRS pump suction header which is common to all three pumps.

Flow through any one pump is capable of preventing core damage for those smaller leak sizes which do not allow the RCS pressure to decrease rapidly enough to the point where only the LPRS is required. One high pressure line can deliver 450 gpm at 1800 psig reactor vessel pressure. One of the three high pressure pumps is normally in operation and a positive static head of water assures that all pipe lines are filled with coolant. The high pressure lines contain thermal sleeves at their connections into the reactor coolant pipint to prevent over stressing the pipe juncture.

All three pumps have self-contained lubrication systems and mechanical seal coolant systems tied in with the Low Pressure Service Water System (LPSW). RCS decay heat is removed through the Low Pressure Injection System coolers to the Condenser Circulating Water System (CCW). Under a loss of AC power situation, the emergency discharge line will automatically open and the

CCW system will continue to operate as an unassisted siphon system supplying sufficient water to the condenser for decay heat removal and emergency cooling requirements. One low pressure injection cooler is located in each of the two separate LPRS discharge lines to remove the decay heat from the circulated reactor coolant.

Electric power is supplied to the three HPIS pumps by three independent 4160 V buses.

2.2 System Operation

The equipment used in the HPRS operates in three modes:

(1) During normal operation of the RCS, one high pressure injection pump continuously supplies high pressure water from the letdown storage tank to the seals of each of the reactor coolant pumps and to a make-up line connected to one of the reactor inlet lines (Normal Mode).

(2) Immediately following an accident, the high pressure pumps deliver water from the borated water storage tank to the cold legs of the RCS. (Injection mode - see Appendix B8.)

(3) Following exhaustion of the BWST, water is drawn from the LPRS discharge for recirculation into the RCS cold legs (Recirculation Mode).

The high pressure recirculation mode is initiated by the following operator actions:

(1) BWST supply line values HP-24, HP-25, LP-21 and LP-22 are closed when BWST low level alarm notifies operator. All high and low pressure ECCS pumps are also shut off at this point.

(2) Containment sump valves LP-19 and LP-20 are opened and the low pressure pumps LPP1A and LPP1B are restarted.

(3) Valves LP-15 and LP-16 are opened in order to divert a portion of the LPRS flow to the high pressure pumps which are also restarted.

After initiating the HPRS, the operator continues to control the system. To aid the operator, the following system conditions are monitored and displayed in the control room: the reactor building sump level, the temperature of water in the line from the sump to the low pressure pumps, the low pressure pump discharge pressure, the flows in the low pressure and high pressure supply lines to the reactor vessel, the level in the BWST and all motor operated valve positions.

3.0 SURRY HPRS DESCRIPTION

The primary function of the Surry HPRS serves basically the same functions as the Oconee HPRS. The HPRS is required to supply high pressure water to the RCS following a small LOCA where there is no rapid depressurization of the RCS. The HPRS can also serve as an alternate discharge path for the LPRS at low pressures (see Figure B9-2).

The HPRS consists of three charging pumps, each with a 150 gpm capacity at a 2750 psig discharge pressure. The required flow for successful HPRS operation is 150 gpm at full head or the flow of one charging pump. This includes consideration for the loss of flow of a rupture in the flow path to a cold leg. The source of water for the HPRS pumps comes from the discharge of the LPRS pumps through motor operated valves 1863A-B. The LPRS draws flow from the containment sump.

Initially, when in the HPIS mode, the system is aligned to draw water from the Refueling Water Storage Tank (RWST) and deliver it to the cold legs of the RCS. The HPRS mode is manually initiated when the level of the RWST reaches 87% empty by the operator who opens the suction valves from the LPRS discharge, MOV 1863A and MOV 1863B, and closes the RWST supply valve. It is assumed that the charging pumps are already operating from the HPIS mode and that the LPRS and sump systems are operable.

The discharge of the HPRS is directed to either the RCS cold legs or hot legs with initial recirculation passing through the Boron Injection Tank (BIT) to the cold legs. An alternate path to the cold legs which bypasses the BIT is available if flow is found to be deficient. This is done by opening MOV-1842. During the first day of operation recirculation is injected to the cold legs. If necessary, flow is then directed to the hot legs to prevent the accumulation of boron, residue, and debris in the core which would result from continuous boiling.

It should be noted that all valve manipulations required for emergency recirculation are directed or remotely operator controlled. Thus, a valve in the wrong position will not be activated to the proper position automatically.

Successful charging pump cooling depends on a closed charging pump cooling water system to provide cooling water for the pump seals and a once through charging pump service water system to cool the lubrication oil coolers and to remove heat from the charging pump cooling water system through intermediate seal heat exchangers. The 600 HP charging pump motors also require cooling by air drawn into the hoods over the motors into the auxiliary building central air ventilation system. Failure of pump lubricating oil or seal cooling or failure of air flow through the auxiliary building central area ventilation system, which prevents overheating of the pump motors during HPRS operation, is assumed to fail the charging pumps.

4.0 COMPARISON OF OCONEE AND SURRY HPRS

The HPRS at both Oconee and Surry are similar in that each has three high pressure pumps which take their suction from two independent flow paths at the discharge of the LPRS pumps. Both systems require the successful operation of their respective LPRS and require operator action to valve in the HPRS pump discharge. Failure of the LPRS or of the appropriate operator action are the main contributors to HPRS unavailability at both plants.

At the Surry reactor, HPRS flow must be manually realigned from the cold legs to the hot legs within 24 hours. This additional important contributor to the Surry system availability does not apply to the Oconee HPRS.

The HPRS unavailability for Oconee was calculated to be somewhat higher than that calculated for Surry (1.1×10^{-2} compared to 9.0×10^{-3}).

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

Failure of the HPRS contributes the Emergency Coolant Recirculation (ECR) event, Event H, for the S_3 LOCA (breaks < 4") and transient induced LOCAs. The ECR event also includes failure of the LPRS. As stated previously, the HPRS is clearly dependent on the LPRS because the high pressure pumps take suction from the low pressure pump discharge during the recirculation mode. This interaction was accounted for in the sequence analysis by including an ECR common mode failure in the Boolean equations. Other common mode failures such as failure to remove heat via the heat exchangers in the LPRS were also considered. Considering the success criteria stated in the FSAR, Event H for S_3 LOCA sequences is defined as failure to recirculate water into the reactor vessel from at least one of two low pressure pumps and the corresponding one of three high pressure pumps.

5.2 HPRS Model Description

5.2.1 HPRS Boolean Equations

The following Boolean equation was developed to model HPRS failure considering one high pressure pump is required for success:

$$HPRS = HPRSCM + LPRS + LPISCM \quad . \qquad \text{(Eq. B9-1)}$$

The term LPRS represents the LPRS Boolean equation given in Appendix B7. The term HPRSCM represents the common mode failure of the operator to realign the high pressure pump suction to the low pressure pump discharge (failure to open valves LP-15 and LP-16 and close valves HP-24 and HP-25). This failure has an assessed probability of 3×10^{-3}. The term LPISCM represents system failure due to the human error of inadvertently leaving the LPIS test valves in the open position (see also Appendix B6). If they are left in this position following a test, LPRS flow will be recirculated back to the BWST and thus divert water from going to the core. This term must be included in the above equation because the LPIS is not demanded in accident sequences requiring the HPRS and the fault LPISCM would not occur until the LPRS was started by the operator. The term LPISCM was assessed at 3×10^{-3}.

Other terms which model continued operation of the high pressure pump trains could have been added to the above equation, but they are not important contributors to system failure and were therefore not included.

5.2.2 HPRS Unavailability

The Boolean equation presented in Section 5.2.1 of the LPRS Appendix B7 models both injection and recirculation failure modes of the low pressure trains. If the LPRS is to be used following a success of the LPIS, then double injection failures must be removed from the unavailability estimate of the LPRS (refer to discussion in Section 5.2.2 of that appendix). However, in the case of small LOCAs, the LPIS is not required during the injection phase, since only the HPIS is required. Since the LPIS is not demanded prior to the start of the recirculation phase, the unavailability estimate for the LPRS following small LOCAs must include all injection failure combinations.

Referring to the Boolean equation for the LPRS and including double injection failure yields

$$LPRS = 5.0 \times 10^{-3} .$$

"Double" test and maintenance contributions, i.e., a deliberate action specifying both low pressure trains to be tested or maintenanced simultaneously, were not included in this unavailability estimate because such an action would violate technical specifications.

Substitution of the term unavailabilities into the HPRS equation yields

$$HPRS = 1.1 \times 10^{-2}$$

Forty-six percent of this unavailability is due to LPRS, 27% is due to HPRSCM and 27% is due to LPISCM.

The reader should be cautioned that this is the unavailability for Oconee's HPRS if the system is considered independent of all others. In general, the HPRS unavailability will depend on what other system successes or failure have occurred, i.e., the unavailability used for the HPRS in the sequence analysis calculabion must be a conditional unavailability.

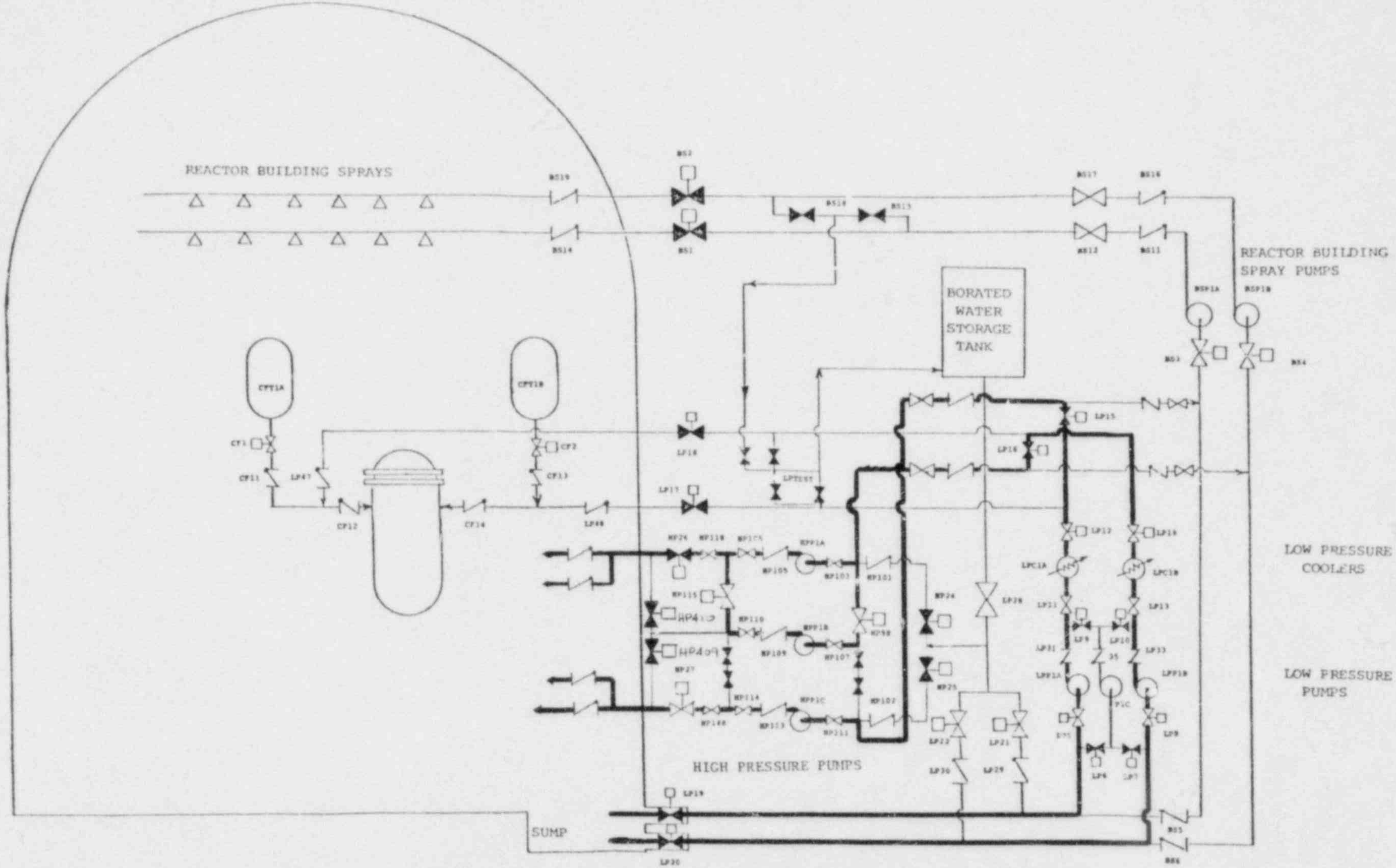


Figure B9-1. Oconee ECCS Schedmatic (HPRS Highlighted)

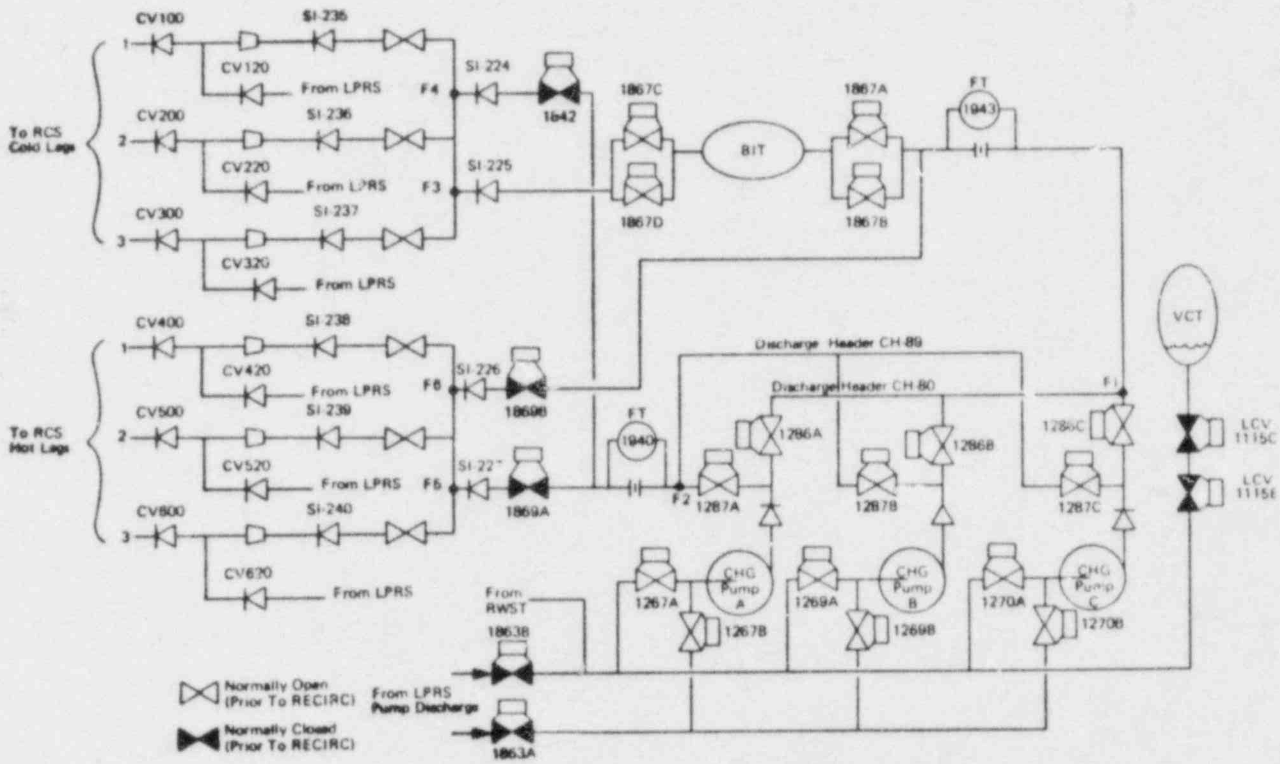


Figure B9-2. Surry HPRS Simplified System Diagram (Shown in Cold Leg Recirculation Mode)

APPENDIX B10

SURVEY AND ANALYSIS

ENGINEERED SAFEGUARDS PROTECTIVE SYSTEM (ESPS)

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Engineered Safeguards Protective System (ESPS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The ESPS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two engineered safeguards protective systems is given in Section 4. ESPS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model and point estimate unavailabilities used to incorporate ESPS failures into the Oconee accident sequence.

2.0 OCONEE ESPS DESCRIPTION

2.1 System Description

The ESPS monitors reactor building pressure and RCS pressure to detect the failure of the RCS. The ESPS provides initiation signals to the high and low pressure injection systems, containment isolation systems, the reactor building cooling system, and the containment spray injection system. In addition, an ESPS signal is used to start the emergency power system and initiate a transfer to that system. The conditions that will actuate engineered safeguards are listed in Table B10-1.

The ESPS is a basic 2-out-of-3 coincidence logic system. Each pressure input is measured three times, the three redundant signals terminate in three bistables as shown in Figure B10-1. Specifically, the system consists of eight 2-out-of-3 coincidence logic networks for initiating four safeguards actions. The equipment required for these safeguards actions is initiated by two

2-out-of-3 logic networks, each referred to as an ESPS channel. Each safeguards system is therefore actuated by either of two redundant coincident logic or protective channels. Refer to Table B10-2 for a list of engineered safeguards actuated devices.

The output of the protective channel coincidence logic is connected to the channel's unit control (UC) modules There is one UC module for every item (pump, valve, etc.) controlled by the protective channel. A protective channel's UC modules are connected in parallel with the output of the coincidence logic (e.g., one channel may signal 4 valves or pumps simultaneously). The output of the coincidence logic follows a normally closed path in each UC module, finally terminating in an output relay with each module.

2.2 System Operation

When the RCS pressure falls to 1500 psig following a LOCA, the three bistable devices associated with this trip set point will initiate signals which will energize two, redundant, 2 out of 3 logic networks (ESPS channels 1 and 2) for actuation of the reactor building isolation system (RBIS), HPIS, and EPS. These networks will, in turn, energize the output relay in each unit control module associated with safeguard equipment for the RBIS, HPIS and EPS. Closure of the normally open contacts of the output relay energizes the control relay in the controller of the equipment required to be actuated. A further decrease in RCS pressure to 500 psig results in the same actions by ESPS channels 3 and 4 for actuation of the LPIS and LPSW.

Similarly, a reactor building (RB) pressure rise of 4 psig results in actuation of the Reactor Building Cooling System by ESPS channels 5 and 6. This 4 psig signal also provides input to channels 1 and 2 for actuation of the RBIS, HPIS and LPIS. A further increase of RB pressure to 10 psig causes two redundant coincident logic networks, ESPS channels 7 and 8, to energize, which, in turn, provides a signal to control electronics for actuation of the CSIS.

Loss of vital bus power to instrument string will, with the exception of the CSIS, initiate a trip of that portion of the logic associated with the affected string. Loss of vital bus power to the system will not initiate system actuation. The devices actuated by the system are listed in Table B10-2.

3.0 SURRY ESPS DESCRIPTION

The Surry ESPS as described in WASH-1400 was split into two systems; namely, the Consequence Limiting Control System (CLCS) and the Safety Injection Control System (SICS).

3.1 Surry CLCS Description

The Surry CLCS is designed to detect out-of-tolerance conditions within the containment, by measuring containment pressure, and to initiate operation of equipment and systems designed to limit and counteract these conditions (see Figure B10-2).

The devices which are activated by the CLCS are initiated at one of two pressure levels. A containment pressure rise to 1.5 psig initiates the "HI" containment pressure phase of the CLCS. In this phase, the containment vacuum pumps are tripped, certain containment isolation valves are closed and back-up signals are sent to the Safety Injection Control

System (SICS) which monitors RCS pressurizer pressure to activate core cooling systems. A further rise in containment pressure to 10.3 psig initiates the "HI-HI" containment pressure phase of the CLCS. In this phase, the CSIS and the Containment Spray Recirculation System (CSRS) are initiated, the remaining containment isolation valves are closed, the emergency diesel generators (No. 1 and No. 3) are started, and service water is diverted to the containment spray heat exchangers by energizing the appropriate motor operated valves.

The CLCS consists of four independent measurement channels and two logic trains for each pressure level. Each logic train trips when 3 of the 4 measurement channels sense a trip pressure. The logic trains and measurement channels are designed to trip on loss of power for HI actuation but are prevented from tripping HI-HI on loss of power (redundant power precludes disabling HI-HI by one failure). Manual initiation of the HI trains is accomplished by depressing one push button while manual initiation of the HI-HI trains is accomplished by simultaneously depressing two push buttons.

Placing a measurement in the test mode causes it to send a trip signal to all four logic trains. Thus, only two of the three remaining channels must trip to initate the logic trains. A logic train, which is in test, will be automatically pulled out of test if the train not being tested trips.

3.2 Surry SICS Description

The Surry actuation system, the Safety Injection Control System (SICS), provides initiating signals to other systems such as the LPIS, HPIS, and the Reactor Protection System (RPS). The SICS consists of two redundant trains, each of which includes analog instrumentation to energize seven output relay coils which provide for electrical control of the HPIS, LPIS, accumulators and containment valves. The circuitry in both trains is identical and redundant. Each train is fed by a separate DC bus and is located in a separate cabinet. Both trains are fed from different bistable relays which in turn are fed by the same comparators, i.e., relay PC 455 in train A and relay PC 455 in train B are both fed by comparator 455 (see Figure B10-3). Thus, train redundancy is lost but is replaced by channel redundancy at this point.

The SICS is automatically activated when any of the following conditions exists:

a) Low pressurizer pressure coincident with low pressurizer water level.

b) High containment pressure.

c) High differential pressure between any two steam lines.

d) High steam line flow coincident with low steam line pressure or low T_{AVG} across the core.

The logic diagram for one channel of the dual channel SICS appears in Figure B10-3.

4.0 COMPARISON OF OCONEE AND SURRY ESPS

The Oconee and Surry designs employ comparable degrees of redundancy in processing sensor data and initiating engineered safeguards actuation when required. Both designs actuate similar types of systems and utilize dual logic trains which derive their signals from a sensor group common to both trains. At both plants the HPIS and LPIS, in addition to their normal trip signals, receive backup signals from a high reactor building pressure trip. There are several differences between the systems, however.

One difference between the two designs is that the Oconee design monitors RCS pressure only, whereas the Surry SIAS monitors RCS pressurizer pressure and level. Another difference is that the Oconee ESPS employs 3 pressure sensors for generating a HI reactor building pressure signal and 6 pressure switches, arranged in 2 groups of 3 switches, for generating a HI-HI signal. The Surry CLCS employs 4 pressure sensors for generating both the HI and HI-HI signals. The Oconee design employs 2-out-of-3 trip logic while the Surry design employs 3-out-of-4 trip logic. The Surry CLCS provides for automatically initiating, through delay circuits, the CSRS with manual initiation as backup. The Oconee CSRS is initiated when the operator realigns the LPIS to the recirculation mode. And finally, the Surry SICS will actuate all of its associated safeguard systems whenever any of the required trip conditions are met. The Oconee design has the capability of actuating only the HPIS (at RCS pressure of 1500 psig) providing RCS pressure does not fall to 500 psig or reactor building pressure does not rise to 4 psig. This is accomplished in the analog channels which include separate bistables for RCS pressure (1500 psig and 500 psig) and RB pressure (4 psig).

Based on a qualitative comparison between the two designs, it was concluded that the unavailability of the Oconee ESPS is similar to that estimated for the Surry SICS and CLCS.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The ESPS does not appear as an explicit event on the event trees. The ESPS, however, does contribute to several events since it actuates many of the plant ESF systems. A list of the systems the ESPS actuates and the corresponding event tree events is given below.

	System	Event
1)	HPIS	LOCA event D
2)	LPIS	LOCA event D
3)	LPRS	LOCA event H, event G
4)	CSIS	LOCA event C
5)	CSRS	LOCA event F
6)	RBCS	LOCA event Y, event Z, Transient event O
7)	LPSW	LOCA events Y,D,Z,G, Transient events L,U,O

5.2 ESPS Model Description

A comparison was made of the Surry SIAS and CLCS and the Oconee ESPS which identified actuation logic trains (or channels) and sensor groups that perform similar functions. The unavailability of an Oconee channel or sensor group was then assumed to be the same as the equivalent Surry channel or sensor group. Common mode failures which applied to the Surry actuation system were also assumed to apply to the Oconee system. Results of this comparison are given in Table B10-3.

The faults depicted in Table B10-3 were substituted into the LPIS, LPRS, HPIS, CSIS, CSRS, LPSW and RBCS Boolean equations as appropriate (see Appendices B6, B7, B8, B11, B12, B14 and B15). These faults appear in these equations according to the Boolean identifier given in Table B10-3.

The common modes listed in Table B10-3 are all due to sensor/comparitor miscalibrations. For instance, the Surry CLCS HI and HI-HI common mode error assessment was based on the possibility of repetitive human errors during the containment pressure sensor comparator calibration and test procedures. This fault could occur on all comparitors for which similar actions are called for. If this human error were to occur, both logic trains of CLCS HI would fail. In the Surry CLCS analysis it was assumed to be a tightly coupled event where miscalibration of all comparitors was assigned the value of 1×10^{-3}. The similar sensor-comparitor group at Oconee is ESPS HI. If 2 of 3 comparitors are miscalibrated, both channels 5 and 6 would fail. The probability of this occurrence was also assigned to be 1×10^{-3} per reactor year.

Table B10-1. Engineered Safeguards Actuation Conditions

Channel No.	Action	Trip Condition	Steady State Normal Value	Trip Point
1, 2	High-Pressure Injection	Low Reactor Coolant Pressure or	2120-2250 psig	1500 psig
		High Reactor Building Pressure	Atmospheric	4 psig
3, 4	Low-Pressure Injection	Very Low Reactor Coolant Pressure or	2120-2250 psig	500 psig
		High Reactor Building Pressure	Atmospheric	4 psig
5,6	Start Reactor Building Cooling	High Reactor Building Pressure	Atmospheric	4 psig
7,8	Reactor Building Spray	High Reactor Building Pressure	Atmospheric	10 psig

Table B10-2. Engineered Safeguards Actuated Devices

Channel 1	Channel 2	Channels 1&2	Channel 3	Channel 4	Channels 3&4
HP-P1A	HP-P1C	HP-P1B	LP-P1A	LP-P1B	LPSW-P1C[3]
HP-24	HP-25		LP-17	LP-18	
HP-26					
HP-3	HP-5				
HP-4	HP-21		LPSW-4	LPSW-5	
HP-20	KEOWEE START (Channel B)		LPSW-P3B	LPSW-P3A	
KEOWEE START (Channel A)	LOAD SHED & STBY. BKR. 2				
LOAD SHED & STBY. BKR. 1	Standby BUS FEED BKR.2				
Standby BUS FEED BKR.1					

Channel 5	Channel 6	Channels 5&6	Channel 7	Channel 8
RC-5	RC-7	LPSW-15	BS-1	BS-2
RC-6	FDW-106	LPSW-6		
FDW-105	FDW-108	LPSW-21		
FDW-107	CC-8	RBCU-F1B	BS-P1a	BS-P1B
CC-7	LPSW-24			
LPSW-18	RBCU-F1C			
RBCU-F1A	CWD-13			
CWD-12	LWD-2			
LWD-1	CS-6			
CS-5	PR-2			
PR-1	PR-3			
PR-6	PR-4			
PR-E1A	PR-5			
PR-7	PR-E15			
PR-9	PR-3			
	PR-10			
	FDW-103			
	FDW-104			

Table B10-3. Comparison of Surry and Oconee Actuation Faults

Surry Fault Description	Similar Oconee Fault Description	Surry Failure Contributors	Q/Component
CLCS HI Containment Pressure Logic Train	ESPS HI Reactor Building Pressure Channels 5 or 6 (CH5, CH6)[1]	Singles, Doubles	2×10^{-2}
		Test, Maintenance	2.1×10^{-3}
		Q Total	2.2×10^{-2}
CLCS HI-HI Containment Pressure Logic Train	ESPS HI-HI Reactor Building Pressure Channels 7 or 8 (CH7, CH8)[1]	Singles, Doubles	4.8×10^{-3}
		Test, Maintenance	2.1×10^{-3}
		Q Total	6.9×10^{-3}
SIAS Logic Train	ESPS Channels 1,2,3 or 4 (CH1, CH2, CH3, CH4)[1]	Singles, Doubles	2.9×10^{-3}
		Test, Maintenance	2.1×10^{-3}
		Q Total	5×10^{-3}
CLCS HI Containment Pressure Sensor Group Common Mode	ESPS HI Reactor Building Pressure Sensor Group Common Mode (RBHICM)[1]		1×10^{-3}
CLCS HI-HI Containment Pressure Sensor Group Common Mode	ESPS HI-HI Reactor Building Sensor Group Pressure Common Mode (RBHIHICM)[1]		1×10^{-3}
SIAS Common Mode	ESPS Channels 1, 2, 3, and 4 Sensor Group Common Mode (RCSRBCM)[1]		3.2×10^{-5}

1. Term in parenthesis is the Boolean identifier of this fault.

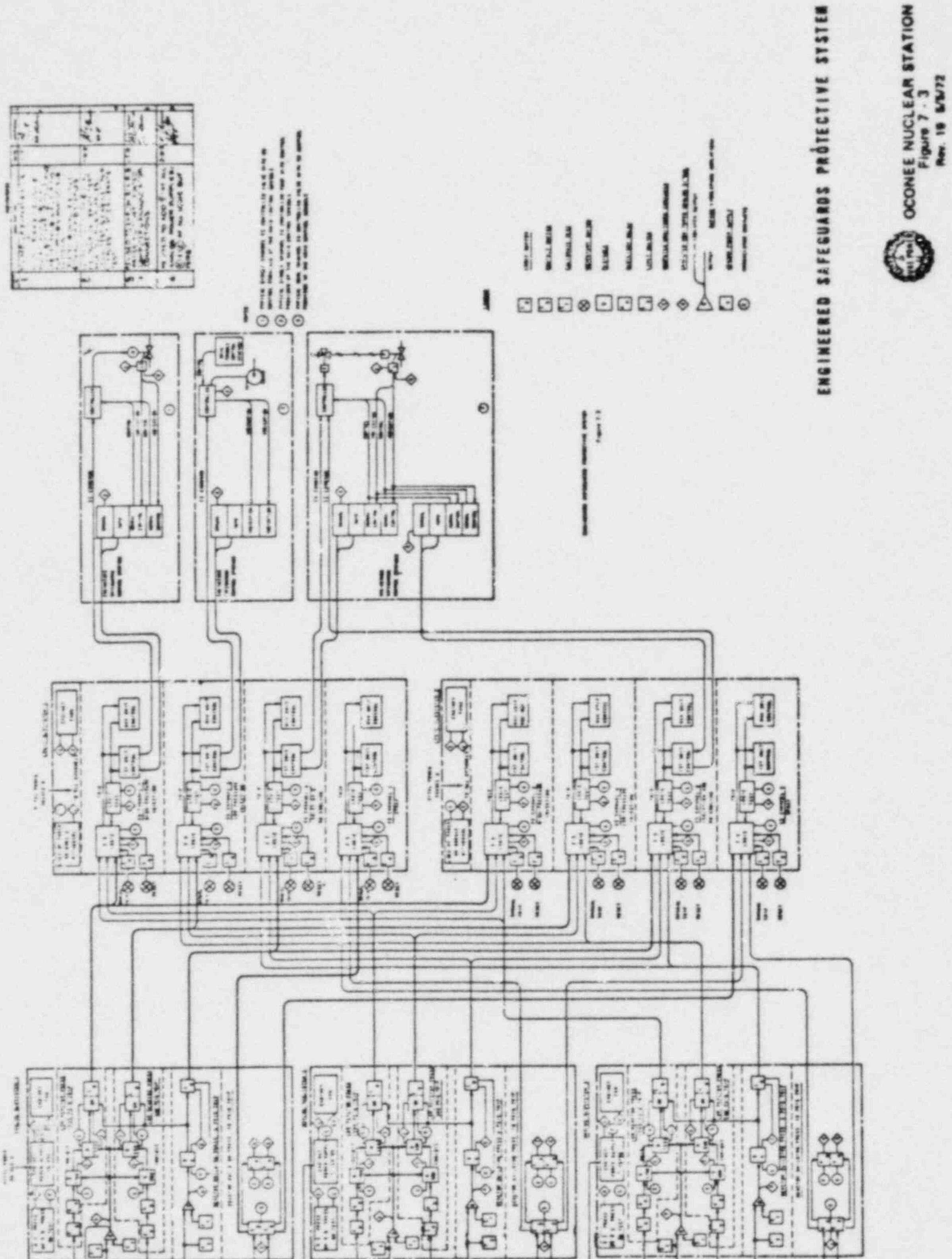


Figure B10-1. Oconee Engineered Safeguards Protective System

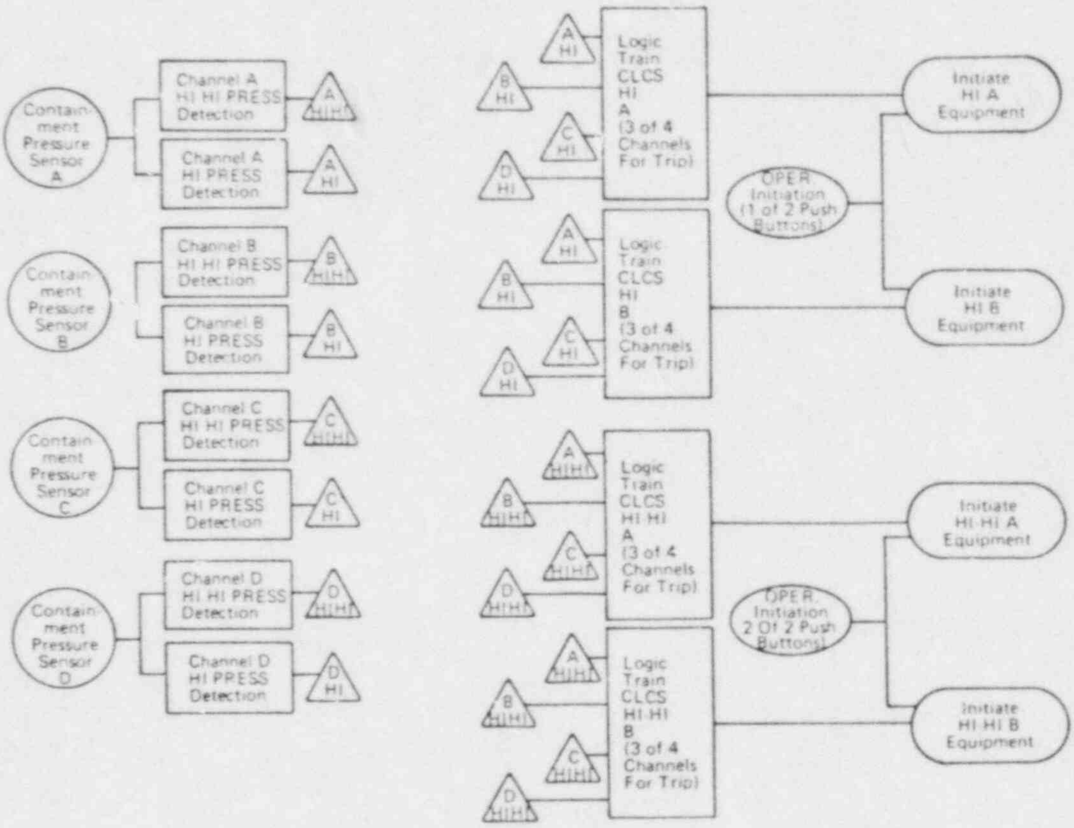


Figure B10-2. Surry CLCS Simplified Diagram

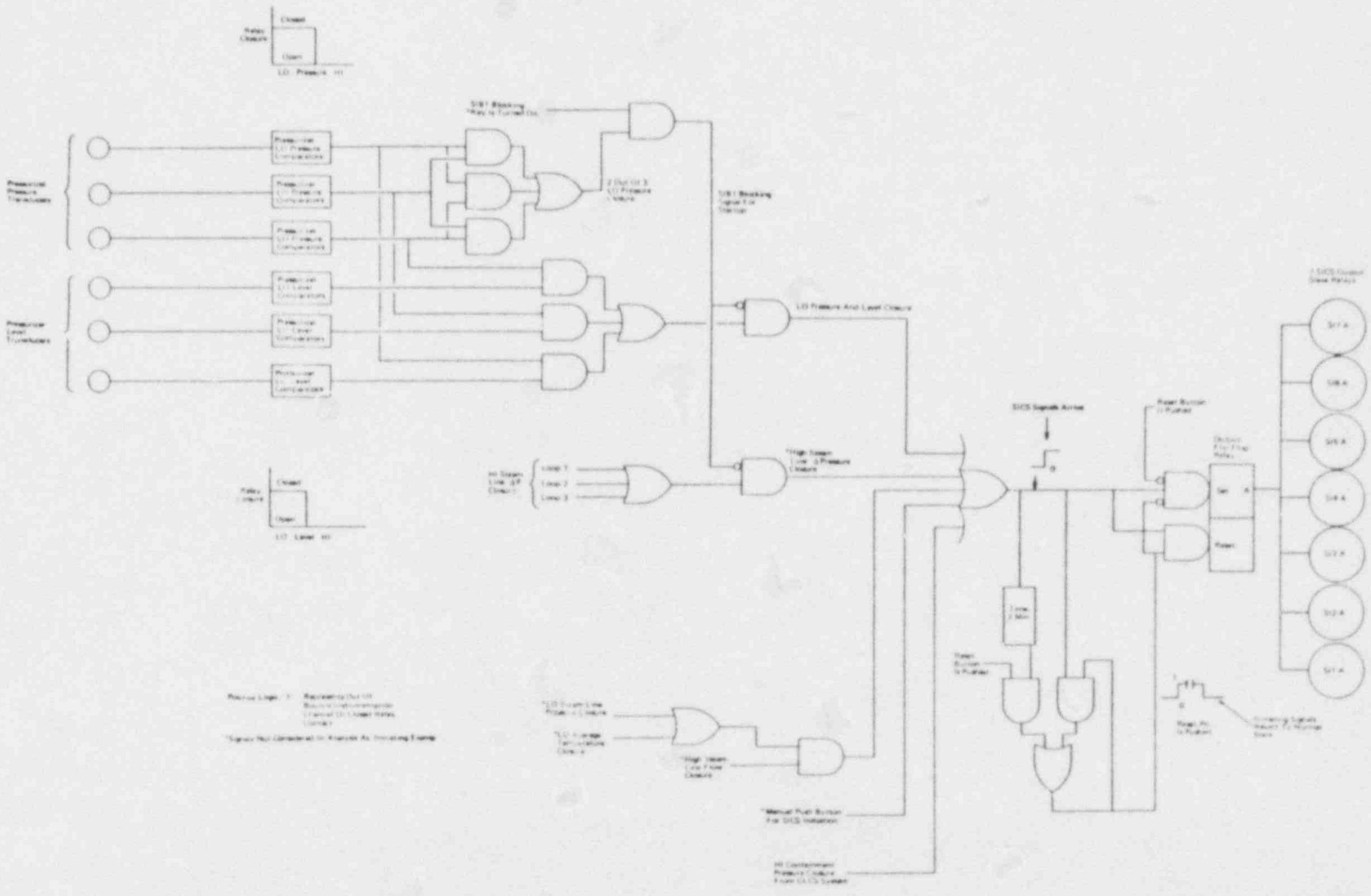


Figure B10-3. Surry Safety Injection Control System

APPENDIX B11

SURVEY AND ANALYSIS

CONTAINMENT SPRAY INJECTION SYSTEM (CSIS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Containment Spray Injection System (CSIS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The CSIS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two containment spray injection systems is given in Section 4. CSIS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate CSIS failures into the Oconee accident sequences and a point estimate of the CSIS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE CSIS DESCRIPTION

2.1 System Description

The CSIS along with the Reactor Building Cooling System (see Appendix B15) provide alternative methods of depressurizing the containment following a LOCA. In addition, the CSIS sprays provide removal of released radioactivity from the post accident containment atmosphere.

The Oconee CSIS consists of two electric motor driven pump trains which draw water from the Borated Water Storage Tank, via a common header, and discharge to the spray headers located in the upper area of the containment. A simplified schematic of the system is shown in Figure B11-1. Each pump is designed to deliver 1500 gpm and the system will provide a minimum of 240×10^6 Btu/hr cooling capacity with both paths in operation. Operation of either train is sufficient to depressurize the post-accident containment pressure excursion and return the pressure to atmospheric. As stated above, the operation of the CSIS sprays also provide removal of core released radioactivity from the containment atmosphere.

2.2 System Operation & Control

The CSIS operation is initiated automatically by a signal from channels 7 and 8 of the Engineered Safeguards Protection System at a reactor building pressure of 10 psig. Initiation provides the following actions:

a) Valves BS-1 and BS-2 open

b) Containment spray injection pumps BS-P1A and BS-P1B start.

The injection mode continues until the BWST is approximately 94% empty at which time a low water level alarm is annunciated in the control room. Upon receipt of this alarm, the operator must realign the CSIS to recirculate water from the building sump.

3.0 SURRY CSIS DESCRIPTION

The Surry CSIS, shown in Figure B11-2, consists of two independent spray subsystems, each containing a pump, filter, spray nozzles, isolation valves and associated piping, plumbing, instrumentation and controls for delivery of 3200 gpm per subsystem of chilled, alkalized borated water from the Refueling Water Storage Tank (RWST) to the containment atmosphere. Each pump is driven by a steam turbine - electric motor dual drive. A mechanical clutch assembly allows only one drive to be effective at a time. The system is automatically placed in emergency service by a 10 psig reactor building pressure signal from the consequence limiting control system which starts the pumps and opens the isolation valves to the containment. Each spray train is designed to deliver sufficient heat removal capacity to provide for successful initial containment response (depressurization of initial pressure excursion and return to sub-atmospheric conditions) until depletion of the RWST. The addition of sodium hydroxide solution to the containment spray serves to improve spray removal of radioactive iodine from the containment atmosphere.

The Surry CSIS operates in conjunction with the Containment Spray Recirculation System (CSRS) during the initial containment response period. Since CSIS water is required for the CSRS suction supply, the systems are dependent. The criterion for containment spray success therefore requires the successful operation of either CSIS train plus successful operation of two of the four CSRS trains.

4.0 COMPARISON OF OCONEE AND SURRY CSIS

Both systems are similar in that each has redundant CSIS trains to deliver water to the containment spray nozzles. They are also susceptable to similar common mode failures. Common mode failure of either system may be caused by mispositioning of valves after pump test and miscalibration of the sensor group which actuates the system. There are, however, some differences.

At Surry each train has an independent header connecting the water tank and the pump suction. At Oconee, however, each train shares a common header. Because of this, the Oconee CSIS has an additional single failure that is not possible at Surry.

The unavailability estimates for the two systems are similar. The estimated value for both Surry and Oconee was approximately 3.3×10^{-3} for LOCAs.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The Oconee CSIS is one of two systems designed to provide immediate cooling of the reactor building atmosphere to limit the post-accident containment pressure excursion and return the containment to atmospheric pressure. The other system is the RBCS which is automatically placed in its emergency operating mode at a reactor building pressure of 4 psig. The CSIS also provides the function of post accident radioactivity removal.

Failure of the CSIS is represented by event C on the LOCA event trees and event O' on the transient event trees. It also contributes to the probability of containment pressure reduction failure, event O, on the transient trees. For all cases, failure of the CSIS is defined as failure to deliver flow to a spray nozzle from at least one pump This criteria for success differs somewhat from the FSAR definition and its basis is discussed more fully in Section 5.1 of Appendix B15.

5.2 CSIS Model Description

5.2.1 CSIS Boolean Equations

The general form of the Boolean equation used to model the CSIS is given below

$$\begin{aligned} \text{CSIS (2 of 2 trains fail)} = \; & A + RBHIHICM + CSISCM \\ & + (F + C + CH7)\cdot(G + B + CH8) \\ & + LOPNRE\cdot LOPNRL \quad . \qquad \text{(Eq. B11-1)} \end{aligned}$$

Table B11-1 relates of each term in the above equations to the components shown in Figure B11-1. Table B11-2 lists total component unavailabilities and each of the contributors to the component unavailability. These unavailabilities are comprised of hardware, human, test and maintenance faults.

The above equation, except for the last term, is referred to as Eq. B11-1(a) in Chapter 4 and was used to model CSIS failure for

LOCAs and transients with AC power available. The entire equation was used for cases in which AC power is not initially available (e.g. loss of offsite power followed by a failure of the emergency hydro AC generators to start, $T_1(B_3)$).

Each spray injection pump is tested monthly to verify proper operation. Table III 5-1 in RSS (Page III 55-56) lists the mean test act duration times for pumps as 1.4 hours. The pump test downtime is therefore:

$$\frac{1.4}{720} = 1.9 \times 10^{-3} \quad .$$

Testing of the CSIS valves was found to negligibly add to the component unavailability when compared to other contributors and was therefore not included.

Scheduled pump and valve maintenance is on a one to twelve month interval with a log normal mean of 4.5 months. The duration is from .5 hours to 24 hours with a log normal mean of 7 hrs. The unavailability of one component due to maintenance is therefore:

$$\frac{7}{720 \times 4.5} = 2.1 \times 10^{-3} \quad .$$

Several common mode failures were identified in the CSIS. Both pump trains are actuated by a reactor building hi-hi pressure signal. This signal is generated by sensor group RBHIHI employing a 2 out of 3 logic. A 1×10^{-3} common mode unavailability was attributed to sensor group RBHIHI due to a possible human error of miscalibrating two or more sensors. This common mode is designated RBHIHICM in the Boolean equation. (For more detail concerning ESPS actuation faults and common mode failure, see Appendix B10.) Another common mode, CSISCM, assessed at 1×10^{-3} was caused by a human failure to reclose the CSIS valves BS-18, BS-13 and BS-21 after a system test. If these valves are left open, CSIS flow will be recirculated back to the BWST and thus diverted from reaching the spray nozzles.

5.2.2 CSIS Unavailability

Using the Boolean equations given in the last section and the term unavailabilities given in Table B6-1, independent CSIS point estimate unavailabilities can be calculated. These are found to be:

$$CSIS = 3.3 \times 10^{-3}$$ (Applies to LOCAs and transients with AC power initially available)

and

$$CSIS = 6.3 \times 10^{-3}$$ (Applies to situations with AC power initially unavailable) .

Double test or maintenance contributions which would violate the system technical specification were removed from these unavailabilities. For example, simultaneous maintenance of both containment spray trains were removed from the probability calculations.

A quantitative ranking of the Boolean terms which describe the failure modes of the CSIS following LOCAs and transients with AC power available is given in Table B11-3. As can be noted, greater than 50% of the system unavailability is due to terms CSISCM and RBHIHICM. For situations with AC power initially lost approximately 44% of the CSIS unavailability is due to the failure to restore off-site power within 40 minutes and the failure of the operator to notify the Lee Steam Station.

The reader should be cautioned that these are unavailabilities for Oconee's CSIS if the system is considered independent of all others. In general, the CSIS unavailability will depend on what other system successes or failures have occurred, i.e. the unavailability for the CSIS used in the sequence calculation must be a conditional unavailability.

Table B11-1. Boolean Equation Term Descriptions

Boolean Term	Term Definition	Term Unavailability
A	LP-28	4×10^{-4}
F	Spray Nozzles A + BS-1 + BS-12 + BS-11 + BS-P1A + BS-3 + BS-5 + BS-14	2.0×10^{-2}
G	Spray Nozzles B + BS-19 + BS-2 + BS-17 + BS-16 + BS-P1B + BS-4 + BS-6	2.0×10^{-2}
C	LP-21 + LP-29	3.3×10^{-3}
B	LP-22 + LP-30	3.3×10^{-3}
CH7[1]	ESPS Actuation Train (Channel 7)	6.9×10^{-3}
CH8[2]	ESPS Actuation Train (Channel 8)	6.9×10^{-3}
CSISCM	Valves BS-18, BS-13, and BS-21 in recirculation line to BWST inadvertently left open	1×10^{-3}
RBHIHICM[1]	Sensor Group RBHIHI Common Mode	1×10^{-3}
LOPNRE[2]	Offsite power not recovered within 1/2-1 hour (applies to loss of all AC only)	2×10^{-1}
LOPNRL[2]	Offsite power not recovered within 1-3 hours (applies to loss of all AC only)	5×10^{-1}

---

[1]Refer to Appendix B10.
[2]Refer to Appendix B1.

Table B11-2. Component Unavailabilities

Component Description	Fault Identifier	Failure Contributors	Q/Component
	BS-19		
	BS-14		
Check Valve	BS-16		
	BS-11		
	BS-5		
	BS-6		
	LP-[illegible]9		
	[illegible]	Hardware	1×10^{-4}
		Q Total	1×10^{-4}
Pump	BS-P1A	Hardware	1×10^{-3}
	BS-P1B	Control Circuitry	1×10^{-3}
		Maintenance	2.1×10^{-3}
		Test	1.9×10^{-3}
		Q Total	6×10^{-3}
Motor Operated	BS-2		
Valve	BS-1	Hardware	1×10^{-3}
(Normally Closed)		Control Circuitry	6.4×10^{-3}
		Plugged	1×10^{-4}
		Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}
Motor Operated	BS-3	Operator Error	1×10^{-3}
Valve	BS-4	Plugged	1×10^{-4}
(Normally Open)	LP-21	Maintenance	2.1×10^{-3}
	LP-22		
		Q Total	3.2×10^{-3}
Manual Valve	BS-17	Plugged	1×10^{-4}
(Normally Open)	BS-12	Operator Error	1×10^{-4}
		Q Total	2×10^{-4}
BWST Manual	LP-28	Plugged	1×10^{-4}
Isolation Valve		Operator Error	3×10^{-4}
		Q Total	4×10^{-4}
Spray Nozzles A			
Spray Nozzles B		Plugged	1.3×10^{-4}
		Q Total	1.3×10^{-4}

Table B11-3. Quantitative Ranking of Terms in CSIS Boolean Equation

CSISCM	1.0×10^{-3}
RBHIHICM	1.0×10^{-3}
F·G	4.0×10^{-4}
A	4.0×10^{-4}
F·CH8	1.4×10^{-4}
CH7·G	1.4×10^{-4}
F·B	6.6×10^{-5}
C·G	6.6×10^{-5}
CH7·CH8	2.5×10^{-5}
C·CH8	2.3×10^{-5}
CH7·B	2.3×10^{-5}
C·B	1×10^{-5}
	3.3×10^{-3}

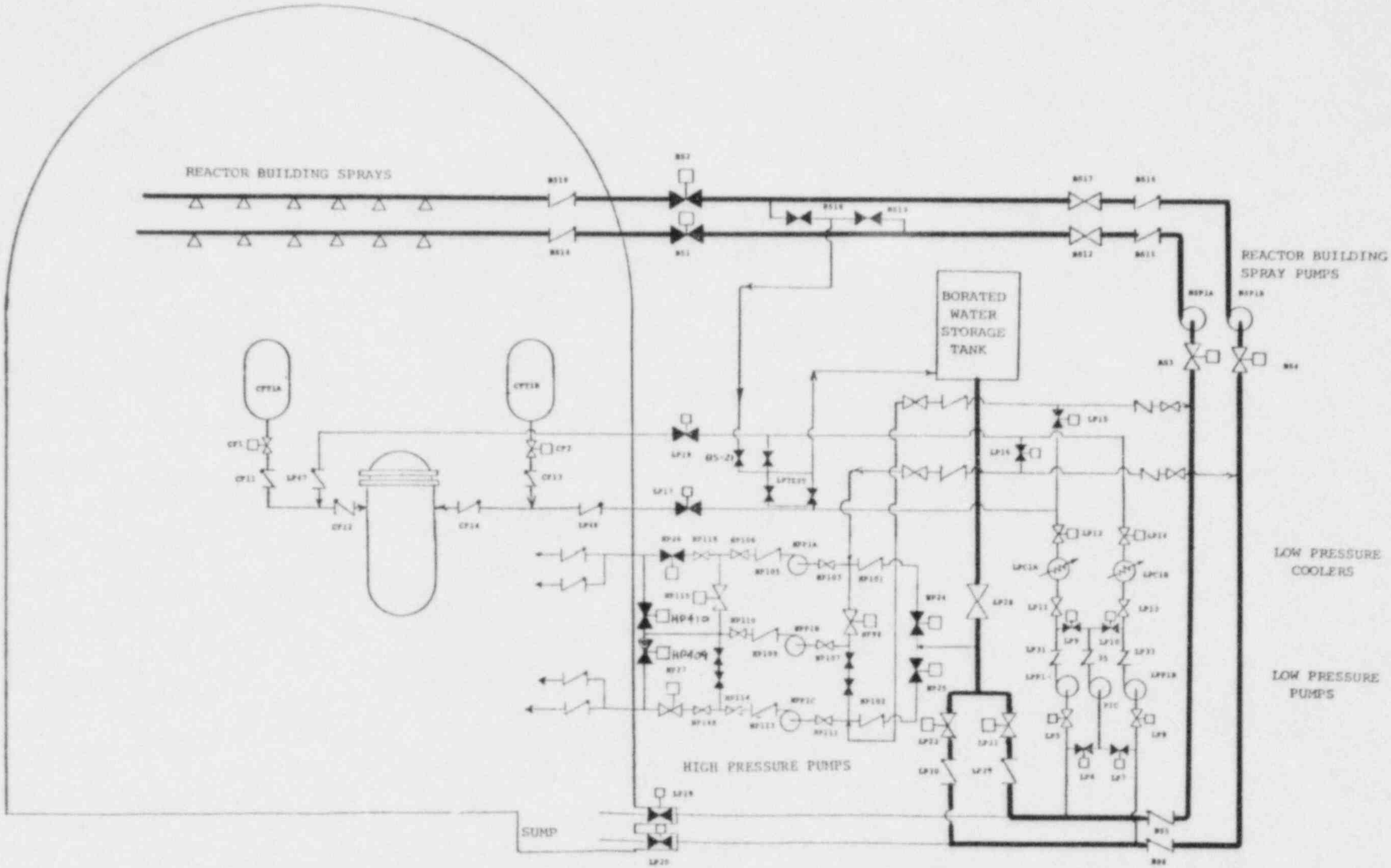


Figure B11-1. Oconee ECCS Schematic (CSIS Highlighted)

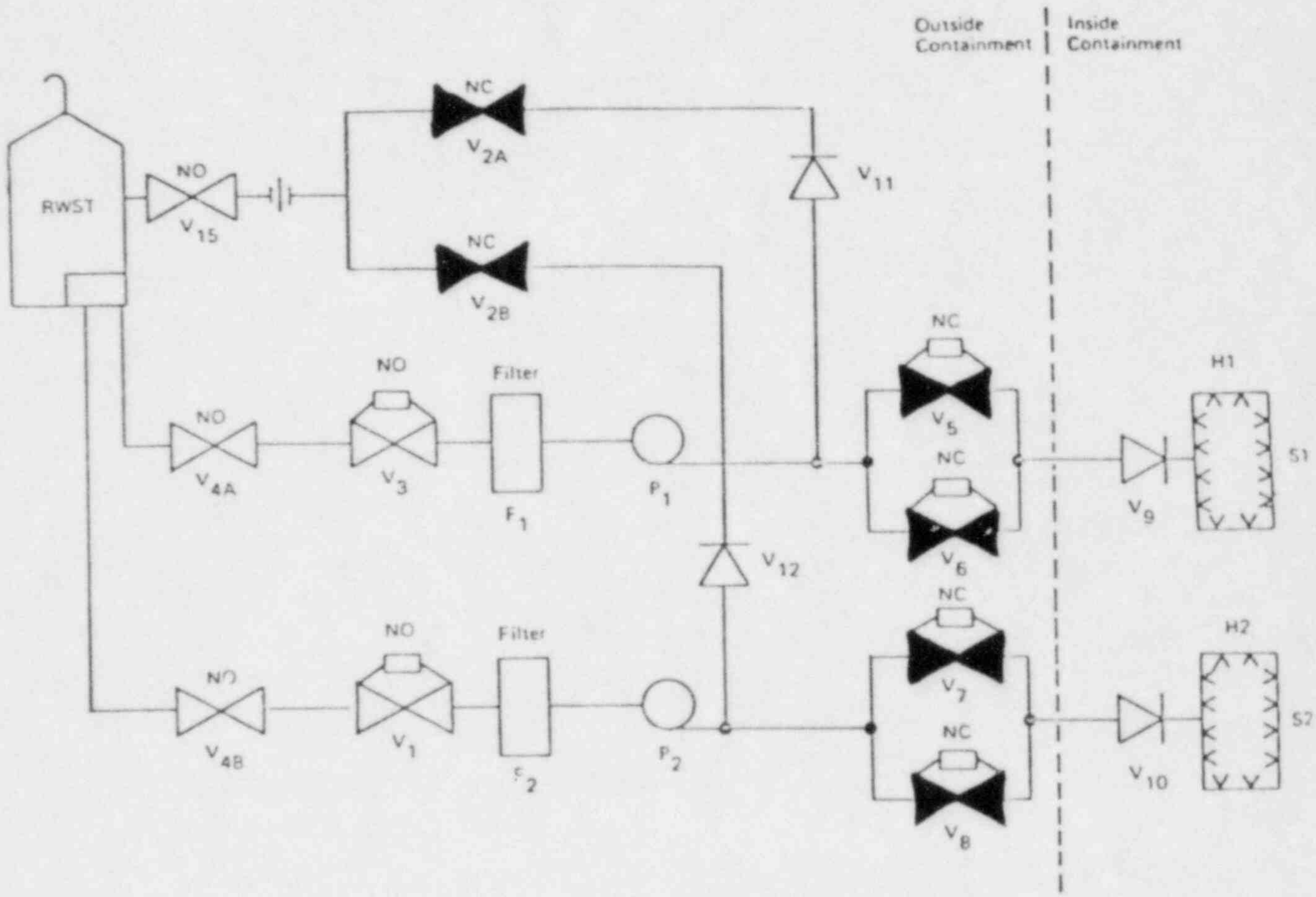


Figure B11-2. Surry CSIS Simplified Flow Diagram

APPENDIX B12

SURVEY AND ANALYSIS

CONTAINMENT SPRAY RECIRCULATION SYSTEM (CSRS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Containment Spray Recirculaton System (CSRS) was reviewed and compared with the similar PWR design (Surry) evaluated in the WASH-1400 study. The CSRS designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. A comparison of the two containment spray recirculation systems is given in Section 4. CSRS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate CSRS failures into the Oconee accident sequences and a point estimate of the CSRS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE CSRS DESCRIPTION

2.1 System Description

The CSRS provides for long term cooling of the reactor building atmosphere to limit the containment system pressure to below the design limit. It also provides for long term scrubbing of the atmosphere to remove radioactive materials.

Each of two spray paths includes an electric pump, a spray header containing 120 nozzles, and associated piping and valves (see Figure B12-1). The pumps which are located outside the containment, are rated at 1500 gpm but deliver water at 1000 gpm during the recirculation mode. This system is initially aligned to draw water from the borated water storage tank. During the recirculation mode, water is drawn from the reactor building emergency sump. The sump water is cooled by the LPRS which pumps the water through heat exchangers, for heat removal via the service water system, prior to injection into the reactor vessel.

Provisions are included for testing the pumps, spray headers, and associated piping and valves. The pumps are tested by drawing water from the borated water storage tank and discharging it through test lines. Low pressure fog or air is blown through the spray nozzles to verify that flow paths are open, valve operation and seal integrity in piping and valves is observed during these tests.

2.2 System Operation

Initially, following a LOCA, the containment spray system is aligned to deliver water from the borated water storage tank to the reactor building at a flow rate of 1500 gpm per pump. Realignment to take suction from the reactor building emergency sump requires operator action. Specifically, upon receipt of an alarm indicating low water level in the borated water storage tank (~ 94% empty), the operator opens two motor operated valves in the emergency sump suction lines (LP-19 and LP-20) and closes the two motor operated valves in the borated water storage tank suction lines (LP-21 and LP-22). This action places both the spray system and the LPIS in the recirculation mode. At this time, the operator also must throttle each of the spray pumps from the 1500 gpm flow to a 1000 gpm flow in order to maintain adequate NPSH. Operation in this mode continues until terminated by operator action.

3.0 SURRY CSRS DESCRIPTION

The CSRS provides for recirculation of the containment sump water through the heat exchangers of the Containment Heat Removal System (CHRS) to spray headers inside the containment for pressure control, fission product removal and long-term energy removal in the event of a LOCA.

The CSRS, which is independent of the CSIS, consists of four trains, each of which includes a pump, heat exchanger, spray header and associated piping and valves (see Figure B12-2). Each pump has a rated flow of 3500 gpm. Two of the pumps are located inside the containment and have a rated head of 230 feet. The remaining two pumps, which are located outside the containment, have a rated head of 249 feet.

All stop valves in the flow path from the containment sump to the spray headers are normally open. Therefore, initiation of flow is accomplished by turning on the four pumps (P1A, P1B, P2A and P2B) via a signal from the Consequence Limiting Control System (CLCS) when a LOCA occurs. Start-up of the pumps located inside the containment (P1A and P1B) is delayed for two minutes and start-up of the pumps located outside the containment (P2A and P2B) is delayed for five minutes after receipt of the CLCS HI-HI signals by the associated pump control circuits. The motor operated valves V_1, V_2, V_3 and V_4 are automatically opened by the CLCS signals if they are inadvertently left closed. Pumps 2A and 2B can be manually stopped by the operator action at any time while pumps 1A and 1B cannot be stopped until the CLCS is reset following a return of containment pressure to subatmospheric.

The CSRS is designed on the following basis:

Pumping by two of the four trains during the first twenty-four hours following a large pipe break accident and by one of the four pump trains after twenty-four hours will provide sufficient flow for system success.

4.0 COMPARISON OF OCONEE AND SURRY CSRS

The CSRS systems for Oconee and Surry are considerably different in both design and mode of operation. One important difference is that the Surry system is independent of its CSIS whereas the Oconee CSRS uses much the same equipment as its CSIS. The success criteria for Surry is two of four pumps. The success criteria for Oconee is one of two pumps.

The Surry CSRS is automatically activated whereas Oconee must be manually activated by having the operator realign the pump suction from the BWST to the containment sump. The Oconee system also requires the operator to throttle the pump flow rate to provide an adequate net positive suction head so that pump cavitation failure will not occur. If these operator actions are not performed, common mode failure of the Oconee CSRS will result. These important common modes do not apply to the Surry system. This results in a CSRS unavailability of 6.9×10^{-3} for Oconee as compared with the RSS value of 1.0×10^{-4} for Surry.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The CSRS is one of two systems designed to provide long term cooling of the reactor building atmosphere to limit containment pressure. The other system is the reactor building cooling system (see Appendix B15) which includes three separate cooling units. Either of these systems provides sufficient cooling to limit and maintain containment pressure to below the design pressure. The CSRS also provides for long term scrubbing of the containment atmosphere to remove radioactive materials.

The probability of failure of the CSRS is represented by Event F on the LOCA event trees. Failure of the system requires the failure of both CSRS trains to deliver water to the spray nozzles from the sump at a flow rate equal or greater than the design output of one pump.

5.2 CSRS Model Description

5.2.1 Boolean Equation

The following Boolean equation was developed to model CSRS failure:

$$CSRS = (F + C + CH7 + F' + W) \bullet (G + B + CH8 + G' + X) + WXCM + CSRSCM \quad \text{(Eq. B12-1)}$$

Each term in the above equation except for F', X, G', W, WXCM and CSRSCM is described in Section 5.2 of the CSIS Appendix B11. Tables B12-1 and B12-2 list the remaining terms and component unavailability estimates. These unavailabilities are comprised of hardware, human, and maintenance faults. Testing of the CSRS valves was found to negligibly add to the valve unavailability when compared to other contributions and was therefore not included. It should be noted that the primed events F' and G' represent failure of the pumps to operate in the recirculation phase.

Maintenance unavailabilities previously not discussed in the CSIS appendix are due to the sump MOVs LP-19 and LP-20. The technical specifications state that maintenance is allowed during power operation on any component which will not remove more than one train (flow path) of a system from service. The component shall not be removed from service so that the affected train is inoperable for more than 24 consecutive hours. The average maintenance interval used in the RSS is 4.5

months, which corresponds to a frequency of 0.22 per month. From the Reactor Safety Study (Table III 5-3), the log normal maintenance act duration for components whose range is limited to 24 hours is 7 hours. The unavailability of values LP-19 and LP-20 due to a maintenance outage is estimated to be:

$$\frac{7(.22)}{720} = 2.1 \times 10^{-3}$$

Two common mode failures of the CSRS were identified. When the BWST is 93% empty a control room alarm notifies the operator to realign the low pressure pump suction from the BWST to the sump. To do this, the operator stops the pumps, opens LP-19 and LP-20, closes LP-21 and LP-22 and restarts the pumps. Failure to realign to the sump would fail the pumps upon emptying the BWST. This common mode failure due to operator error has an assessed probability of 3×10^{-3} and is designated WXCM. After realigning to the sump, the operator is then required to throttle the system flow rate so that each pump train delivers 1000 gpm. During the injection phase each pump delivers 1500 gpm. Throttleing of the flow is required to ensure an adequate net positive suction head to prevent pump cavitation failure. This common mode failure due to operator error has an assessed probability of 3×10^{-3} and is designated CSRSCM.

5.2.2 CSRS Unavailability

Using the Boolean equation given in the last section and the term unavailabilities given in Table B11-1 and B12-1 an independent CSRS point estimate unavailability can be calculated. This is found to be:

$$CSRS = 6.9 \times 10^{-3} .$$

Double test and maintenance contributions, i.e., a deliberate action specifying both trains to be tested or maintenanced simultaneously, were not included in this unavailability estimate because such an action would violate technical specifications. Further, it can be seen that reduction of the Boolean equation describing the CSRS results in 27 terms. Examination of these terms shows that nine depict "double injection" failures of the CSRS, i.e., CSRS failure due to failure of redundant components during low pressure injection which describe the low pressure injection system. These failures were not included in the calculations of the independent CSRS unavailability above, since the CSIS must have succeeded (at least one train) to demand CSRS.

For calculation of the CSRS unavailability as used in the accident sequence analysis, double injection failures and other physically inconsistant failure contributors were eliminated according to the Boolean reduction process where the equations describing each of the systems involved in the sequence were condensed together.

A quantitative ranking of the Boolean terms is given in Table B12-3. As can be noted, approximately 85% of the system unavailability is due to CSRSCM and WXCM.

The reader should be cautioned that these are unavailabilities for Oconee's CSRS if the system is considered independent of all others. In general, the CSRS unavailability will depend on what other system successes or failures have occurred; i.e., the unavailability used for the CSRS in the sequence analysis calculation must be a conditional unavailability.

Table B12-1. Boolean Equation Term Description

Boolean Term	Term Definition	Term Unavailbility
F'	BS-P1A	3.5×10^{-3}
G'	BS-P1B	3.5×10^{-3}
W	LP-19	9.6×10^{-3}
X	LP-20	9.6×10^{-3}
WXCM	Common Mode Due to the failure of the Operator to Realign for Recirculation (open LP-19, LP-20 and close LP-21, LP-22 and restart pumps)	3×10^{-3}
CSRSCM	Common Mode Due to the Failure of the Operator to Throttle CSRS Pumps	3×10^{-3}

Table B12-2. Component Unavailabilities

Component Description	Fault Identifier	Failure Contributors	Q/Component
Pump	BS-P1A BS-P1B	Hardware (Fails to restart)	1.0×10^{-3}
		Con[illegible] Circuitry	1.8×10^{-3}
		Fails to Operate 24 hrs (3×10^{-5}hr)	7.2×10^{-4}
		Q Total	3.5×10^{-3}
Motor Operated Valve (Normally Closed)	LP-19 LP-20	Hardware	1×10^{-3}
		Plugged	1×10^{-4}
		Control Circuitry	6.4×10^{-3}
		Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}

Table B12-3. Quantitative Ranking of Terms in CSRS Boolean Equation

CSRSCM	3.0×10^{-3}
WXCM	3.0×10^{-3}
G·W	1.9×10^{-4}
X·F	1.9×10^{-4}
X·W	9.2×10^{-5}
G'·F	7.0×10^{-5}
G·F'	7.0×10^{-5}
X·CH7	6.6×10^{-5}
CH8·W	6.6×10^{-5}
G'·W	3.4×10^{-5}
X·F	3.4×10^{-5}
X·C	3.2×10^{-5}
B·W	3.2×10^{-5}
G'·CH7	2.4×10^{-5}
CH8·F'	2.4×10^{-5}
G'·F'	1.2×10^{-5}
B·F'	1.2×10^{-5}
G'·C	1.2×10^{-5}
	6.9×10^{-3}

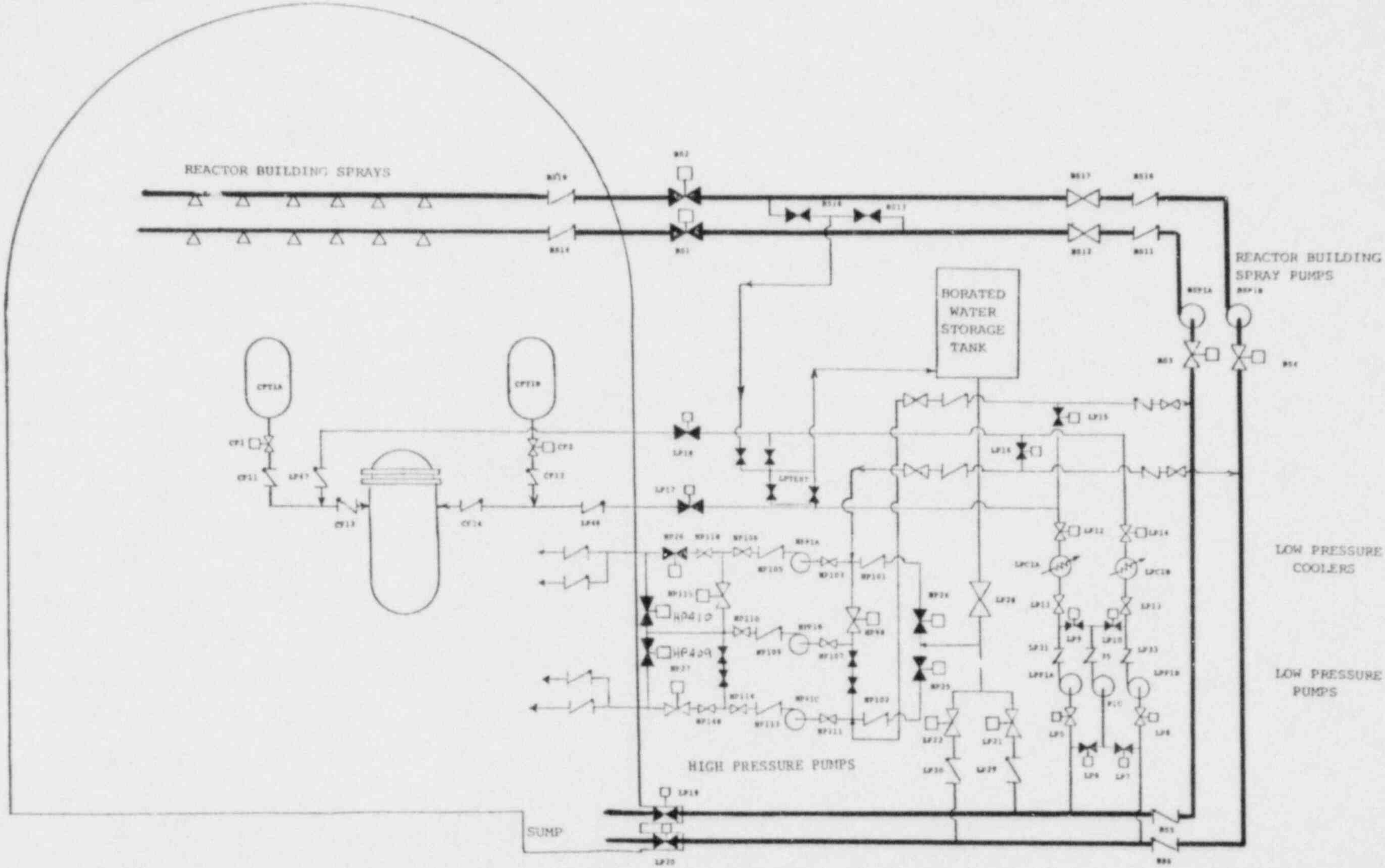


Figure B12-1. Oconee ECCS Schematic (CSRS Highlighted)

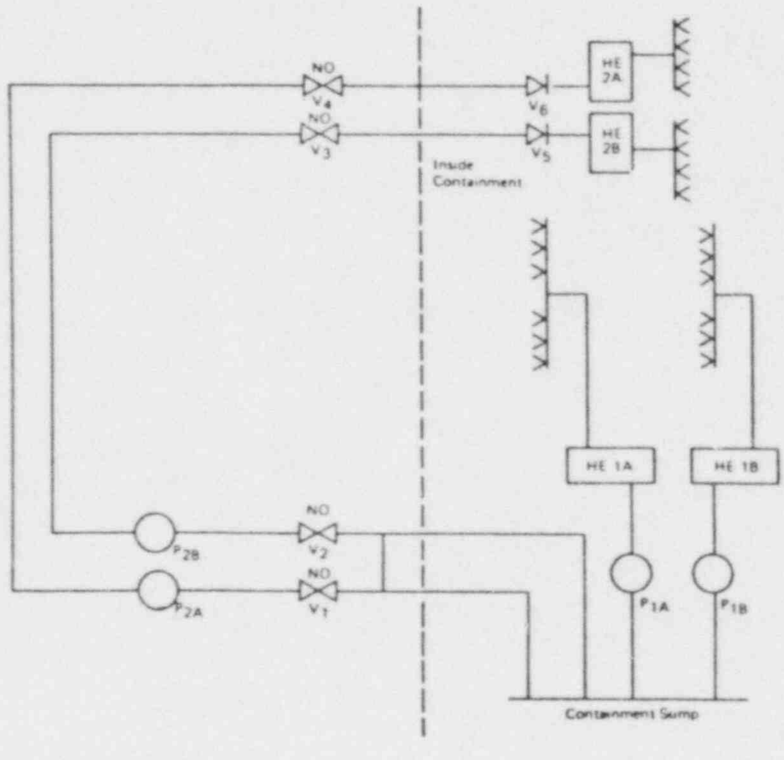


Figure B12-2. Surry Containment Spray Recircuiation System

APPENDIX B13

SURVEY AND ANALYSIS

EMERGENCY FEEDWATER SYSTEM (EFWS) AND HIGH HEAD AUXILIARY SERVICE WATER SYSTEM (HHASWS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Emergency Feedwater System (EFWS) was reviewed and compared with the similar PWR Auxiliary Feedwater System (AFWS) design (Surry) evaluated in the WASH-1400 study. The system designs for Oconee and Surry are described in Sections 2 and 3 of this report respectively. Also included is a brief description of the Oconee High Head Auxiliary Service Water System (HHASWS). There is no comparable system at Surry. This system performs a similar function as the EFWS and is used as a backup to the EFWS. A comparison of the two systems is given in Section 4. EFWS event tree interrelationships are detailed in Section 5. Also incuded in Section 5 is a description of the model used to incorporate EFWS and HHASWS failures into the Oconee accident sequences and a point estimate of the EFWS and HHASWS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE EFWS AND HHASWS DESCRIPTIONS

The purpose of the EFWS is to remove post shutdown decay heat from the Reactor Coolant System (RCS) via the steam generators for those shutdowns in which the main feedwater system is unavailable. If for some reason the EFWS is unavailable, the HHASWS, which performs a similar function as the EFWS, may also be utilized (based on discussions with plant personnel, the HHASWS is currently planned to be utilized if all onsite and offsite AC is unavailable). Successful steam generator cooling can be accomplished by a flow of 500 gpm from either system.

2.1 EFWS Description

A diagram of the Oconee Unit 3 EFWS is presented in Figure B13-1. The EFWS is capable of feeding to either or both steam generators under automatic or manual initiation and control. The system consists of separate feed trains supplied by two motor-driven pumps and/or one turbine driven pump, and a combined suction source.

Two primary reserves of water are continuously available for EFWS use: The condensor hotwell, a 142,000 gallon tank normally containing more than 100,000 gallons; and the two compartments of the upper surge tank, UST "A" and UST "B", two 36,000 gallon tanks which normally contain 25,000 gallons each and which are cross-connected with normally-open motor operated valves. Upon loss of main feedwater, the upper surge tanks may be automatically replenished from the condensor hotwell. The hotwell pumps are normally running. Detection of low suction flow to the main feedwater pumps causes hotwell pump discharge to be recirculated to the upper surge tank dome.

The turbine-driven pump takes suction from the upper surge tank via an 8-inch line containing normally open valves. This pump can also be connected to the condensor hotwell by opening the normally-closed motor-operated valve C-391. The motor-driven pumps have a common suction header which is supplied from both the condensor hotwell and the upper surge tanks.

Emergency feedwater is supplied to the feed trains by either a turbine-driven emergency feedwater pump, which is rated at 1080 gpm, and/or both motor-driven emergency feedwater pumps, each rated at 500 gpm.

Recirculation for the motor-driven pumps is provided by special check valves (FDW-370 and 380) which operate at low flow conditions to recirculate less than 10 gpm per pump to the upper surge tank. A recirculation flow of 100 gpm (nominal) is provided for the turbine-driven pump by valve FDW-89.

Of importance to system reliability is the 6-inch test line containing valve FDW-88. This line is used to perform periodic tests of the turbine-driven pump and is capable of diverting full flow of the turbine pump to the upper surge tanks.

Steam is normally supplied to the EFWS turbine from either steam generator via normally open motor-operated valves MS-82 and MS-84. An alternate source of steam is the startup and auxiliary steam header via valve AS-38. This steam supply is interconnected with other Oconee Units.

Steam availability is controlled by a series of valves. The first in this series is the air-operated steam admission valve, MS-93. On turbine initiation, a solenoid valve is de-energized, venting the air supply to MS-93 and causing it to open. The next valve, MS-94, is a mechanically operated turbine overspeed stop valve. This valve trips automatically on turbine overspeed and must be reset locally. Turbine speed is controlled by the final valve, MS-95, the turbine governor. Exhaust from the turbine is vented directly to the atmosphere.

Figure B13-2 shows the support system dependence of the EFWS turbine and pump. As indicated in the figure, the turbine depends on auxiliary systems to circulate and cool oil for bearing lubrication. Primary oil circulation is provided by a turbine shaft-driven oil pump. However, until the turbine reaches a speed sufficient to drive this pump, the oil is circulated by a

DC motor-operated auxiliary oil pump. The turbine governor valve is connected to the bearing oil supply and will not admit steam to the turbine until a sufficient bearing oil pressure exists.

Oil cooling is accomplished with an oil cooler through which water is circulated by an AC motor-operated pump. Because of the size of the oil reservoir, it is estimated that the turbine can be operated without adverse consequences for up to 45 minutes in the absence of cooling water flow to the oil cooler.[1]

There are no external lube oil dependencies for the motor-driven pumps and motors.

Cooling water must be supplied to the cooling jackets of both the turbine-driven and motor-driven EFWS pumps.

Cooling for the turbine-driven pump jacket is shown in Figure B13-3. Cooling water is supplied from either the Low Pressure Service Water (LPSW) pumps or by gravity flow from the High Pressure Service Water (HPSW) elevated tank. In either case, AC operated valve LPSW-137 (or an associated manual valve) must be opened to permit cooling water flow. It is estimated that the pump can operate only 12 to 15 minutes without cooling water.[1]

Cooling for the motor-driven pump jackets is shown in Figure B13-3. Cooling water for these pumps is also supplied by the LPSW system. This water flows through normally-open, air-operated valves downstream of the pump jackets. If these valves are inadvertently closed prior to an accident, flow would be

---

1. It should be noted that Duke Power has committed to remove this turbine pump AC dependency in the near future.

assured by valve open signals (to de-energize solenoid valves) which accompany motor-driven initiation.

The Low Pressure Service Water (LPSW) pumps also supply water to the turbine-driven pump lube oil cooler.[1] One of these pumps is kept running at all times (see Appendix B14).

Motor-driven pumps "A" and "B" normally supply feedwater to steam generators A and B, respectively. The turbine-driven pump feeds both generators through a common discharge header. Two paths are available for the flow of emergency feedwater to each steam generator from the discharge of the motor-driven pump feeding that generator.

The primary flow path to each generator contains an air-operated flow control valve, FDW-315 or FDW-316; flow to these valves is supplied via normally-open valves and check valves.

An alternate path for emergency feedwater flow to each steam generator is available using part of the normal startup feedwater flow path. This discharge path is available to the motor-driven pumps by opening normally-closed motor-operated valves FDW-374 or FDW-384. Flow through this alternate path is controlled by DC motor-operated valves FDW-38 or FDW-47.

Crosstie connections between the motor-driven pumps discharges contain locked closed manual valves (FDW 313 and 314); these cross connnections were considered unavailable for the purposes of this study.

2.2 EFWS Operation

The EFWS is automatically initiated by either low Main Feedwater (MFW) discharge pressure from both MFW pumps or pump

---

1. It should be noted that Duke Power has committed to remove this turbine pump AC dependency in the near future.

trip signals from both pumps. When either of these conditions exist the following action takes place:

1) Motor driven pumps are both signaled to start.
2) Normally open motor driven pump cooling jacket valves LPSW-516, LPSW-525 are signaled open.
3) Steam admission valve MS-93 is signaled open. Limit switches on MS-93 change state, allowing the auxiliary lube oil pump to start; when sufficient oil pressure is attained, the turbine governor valve will open starting the turbine pump.
4) Normally closed turbine driven pump cooling jacket valve LPSW-137 is signaled open.
5) Turbine driven pump lube oil cooling water motor signaled to start.
6) Steam generator level control is initiated by automatic control of flow control valves FDW-315 and FDW-316. Steam generator level control is provided by level control instrumentation and analog circuits are on battery-backed power and which are separate and independent from the Integrated Control System (ICS).

To aid the operator in monitoring EFWS operation the following instrumentation is available in the control room.

- EFWS Flow - measured for both discharge paths for both feed trains.
- Discharge Pressures - for all EFW pumps.
- Cooling Water Flow - to the motor-driven pumps cooling jackets.

A loss of offsite power causes the following EFWS components to be load shed from the emergency power buses: normally closed turbine cooling water valve LPSW-137; air supply to flow control valves FDW-315, - 316; normally-open suction valves C-152, -153, -156, and -158: normally-closed suction valves C-160 and -391; steam valves MS-82, -84, -17, -26, -24 and -23; and all three hotwell pump motors. The air supply to the flow control valves is only expected to last a few minutes unless the operator loads the air compressors onto the emergency bus. These valves may also be manually valved into a backup nitrogen supply. The turbine cooling water valve must also be loaded onto emergency power and opened since the pump will only run about 15 minutes without cooling.

2.3 HHASWS Description and Operation

The HHASWS is a subsystem of the Oconee Safe Shutdown System (SSS). Since the SSS is a system important to plant security, a detailed discussion of its design in this document is not appropriate pursuant to 10CFR 2.790.[1]

The HHASWS provides an alternative means of supplying feedwater to the steam generators in the event both the normal and emergency feed-water systems are unavailable (based on discussions with plant personnel, the HHASWS is currently only planned to be utilized if all onsite and offsite AC power is unavailable). It consists of a single 2250 gpm motor driven pump which has the capacity of providing adequate shutdown cooling to the steam generators of all three Oconee units simultaneously. The source of AC and DC power required to operate the SSS can be generated by the SSS power system which does not rely on other power systems utilized at the Oconee station. Remote manual initiation is required for the HHASWS.

1. This a new system which is scheduled to be installed in 1981.

3.0 SURRY AUXILIARY FEEDWATER SYSTEM

A simplified flow diagram for the Surry AFWS is shown in Figure B13-4 (reference WASH 1400 II 5-11). The AFWS consists of two 350 gpm electric-driven pumps and one 700 gpm turbine-driven pump along with associated piping, valves, and controls. All pumps can be started either automatically or manually. The system delivers feedwater via separate suction lines from a 110,000 gallon condensate storage tank to the secondary side of three steam generators through two headers. Each steam generator can draw from either header.

The electric pumps are started automatically when: 1) a Safety Injection Control System (SICS) signal is present; 2) loss of off-site power is detected; 3) main feedwater pumps shut off; or 4) low water level is detected in a steam generator. The turbine pump is automatically started for detection of low water in a steam generator or loss of off-site power.

After about eight hours the condensate storage tank is exhausted and water must be drawn from the fire main (400000 gallons with 400 gpm replacement) or from another condensate storage tank (300000 gallons). Switching to these water supplies requires manual valve operation. Successful operation requires flow of the equivalent of one electric driven pump to any one steam generator.

4.0 COMPARISON OF OCONEE EFWS AND HHASWS AND SURRY AFWS

The Oconee EFWS and Surry AFWS are similar in that each system consists of two electric and one turbine driven pump train. Though many piping differences exist between the systems, successful system operation requires the flow equivalent of one pump to one steam generator at both plants.

Given a loss of offsite power the Oconee system requires operator action to engage important EFWS components to the emergency power buses. If this is not accomplished, system flow control and operation of the turbine driven pump will be lost (due to loss of pump cooling) in a short time. Similar operator actions were not identified for the Surry AFWS.

Given a loss of all AC power (both normal and emergency) the Oconee EFWS will fail in a short time due to loss of turbine pump cooling. The Surry turbine pump was not identified to have this cooling dependency and could therefore operate given a loss of all AC power.

The HHASWS at Oconee has no comparable Surry system. This system can provide backup to any EFWS demand and is especially important following a total loss of all AC power. Since the HHASWS has its own power system, this system is not affected and can successfully provide post shutdown cooling.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The EFWS and HHASWS provide the function of emergency secondary heat removal (along with recovery of the main feedwater system) and therefore appear as part of Event L on the transient event trees.

Successful EFWS operation requires the attainment of flow from turbine driven pump to at least one steam generator or from one motor driven pump to its associated steam generator. For cases when the main and EFWS are unavailable, the secondary heat removal must be provided by the single HHASWS pump delivering 500 gpm flow to one of two steam generators. Since the HHASWS is only expected to be used if all onsit ınd offsite power is unavailable (i.e., $T_1(B_3)$ transients disc... ed in Appendix B1, Section 5.1), credit is not gi n to this system for T_1, T_2, or T_3 transients in which either offsite or ...e AC power is available.

5.2 EFWS and HHASWS Model Description

5.2.1 EFWS and HHASWS Boolean Equations

Three Boolean equations were developed to model EFWS failure. The first depicts system failure following a transient involving a loss of the main feedwater system caused by other than a loss of offsite power (T_2 and T_3 transients). The second depicts system failure following a loss of offsite power (T_1 transient) induced loss of main feedwater in which the onsite emergency power is operationable. The third depicts failure of the system following a loss of offsite power in which the onsite emergency AC power system also fails ($T_1(B_3)$ transients).

$$EFWS = [A3+E3\cdot(F3+P3)]\cdot[B3+G3\cdot(F3+P3)] + LPSW$$ (Applies to T_2 or T_3 transients)

$$EFWS = [A3+E3]\cdot[B3+G3] + LPSW$$ (Applies to T_1 transients)

$$EFWS = 1.0$$ (Applies to $T_1(B_3)$ transients)

Table 13-1 lists descriptions of each term in the previous equations. Table 13-2 lists componer.t ..ypes in the EFWS, fault identifiers that label specific components and failures that contribute to the component unavailability. These unavailabilities are comprised of hardware, human, and maintenance faults.

The differences between the first two equations is that for T_1 transients the turbine driven pump is assumed to fail (F3 becomes Ω). The turbine pump is assumed to fail due to loss of jacket cooling. This failure has a very high probability since the valve which must open to allow cooling to the jacket is load shed following this transient and there is a loss of valve position and flow indication. To supply turbine jacket cooling requires the operator to open the valve locally. Given a $T_1(B_3)$ type transient, the EFWS will fail due to loss of pump cooling. Pump cooling depends on the LPSWS which will fail in this situation since AC power is required for LPSWS operation.

Testing of EFWS pumps and valves were found to negligibly add to that component's unavailability when compared to other contributions and was therefore not included. For example, during test of the turbine pump, operators are stationed at valves FDW-309 and 310 (closed) and valve FDW-88 (open). In the event the EFWS is required these operators can rapidly return the system to a functional configuration.

Components shall not be removed from service so that the affected EFWS train is inoperable for more than 72 hours, after which the reactor will be shutdown. The average maintenance interval used in the RSS is 4.5 months, which corresponds to a frequency of 0.22 per month. From the RSS, (Table III 5-3) the lognormal maintenance act duration for components whose range is limited to 72 hours is a mean time of 19 hours. The unavailability of one component due to maintenance is estimated to be:

$$\frac{19(.22)}{720} = 5.8 \times 10^{-3}$$

The Boolean equation representing HHASWS failure is

HHASWS = HHMAN

The unavailability of the HHASWS is completely dominated by the term HHMAN which represents failure of the operator to start the system remote manually.

The above Boolean equations can be combined in a form which is convenient for use in the accident sequence analysis. These equations are:

EFWS/PCS Non-Recovery = (CONST1 + LPSW)·PCSNR (Applies to T_2 transients) Eq. B13-1

EFWS = CONST1 + LPSW (Applies to T_3 transients) Eq. B13-2

EFWS = CONST2 + LPSW (Applies to T_1 transients) Eq. B13-3

HHASWS = HHMAN (Applies to $T_1(B_3)$ transients) Eq. B13-4

These equations represent loss of both the EFWS and HHASWS and have lumped several Boolean terms which only apply to the EFWS into terms CONST1 and CONST2. (See Tables B13-3 and B13-4.) As can be noted above, the difference between equations B13-1 and B13-2 is the term PCSNR. This term represents the failure to restore the power conversion system within ~30 minutes following a T_2 transient. Discussions with plant personnel indicate that given a loss of both the EFWS and PCS, primary emphasis would be placed in restoring the EFWS, but that a somewhat parallel effort to restore the PCS would also be conducted. (Recovery of the EFWS is discussed in the following paragraph.) PCS non-recovery, following a T_2 transient, was roughly estimated to be 10^{-1}, based on Oconee data. Discussions with plant personnel also indicated that it was reasonable to assume that the PCS would not be restored within 30 minutes, following a T_1 transient. The term PCSNR is therefore not applicable to equations B13-3 and B13-4. (For more details, refer to the discussion of the PCS in Chapter 3 of the main report.)

It should be noted that the EFWS Boolean equations depict failure to establish core cooling by the EFWS via the normally configured flow paths. It is recognized that alternate core cooling methods (i.e., the HPIS feed and bleed core cooling method described in Appendix B8), EFWS flow paths, and sources of feedwater different from that modeled are available. All alternate core cooling methods, flow paths and sources of feedwater, which include the HPIS core cooling method, require operator action from either the control room or remote manually. This analysis assumes that if the EFWS fails to deliver via its normally configured flow paths, the operator will utilize one of the following methods of establishing core cooling: An alternate EFWS flow path, inter-tie with the unit one or two EFWS, initiate HPIS core cooling, or actuate the HHASWS. Credit is only given to one of these alternatives due to a fairly short time window available for recovery of emergency feedwater (~20 minutes). As a matter of convenience, this analysis has chosen to model the HPIS core cooling method as the backup means of core cooling if the EFWS fails to establish core cooling via its normally configured flow path for T_1, T_2 and T_3 transients with AC power available. For $T_1(B_3)$

transients, since AC power and the HPIS are unavailable, it is assumed that the HHASWS will be used as the backup.

5.2.2 EFWS and HHASWS Unavailability

Using the Boolean equations given in the last section and the term unavailabilities given in Table B13-1, an independent EFWS and HHASWS point estimate unavailablity can be calculated. These are found to be:

EFWS = 2.4×10^{-4} (Applies to T_2 and T_3 transients)

EFWS = 6.5×10^{-4} (Applies to T_1 transients)

EFWS = 1.0 (Applies to $T_1(B_3)$ transients)

HHASWS = 1×10^{-1} (Applies to $T_1(B_3)$ transients only)

"Double" test and maintenance contributions, i.e., a deliberate action specifying both EFWS trains to be tested or maintenanced simultaneously, were not included in this unavailability estimate because such an action would violate technical specifications. A quantitative ranking of the Boolean terms for the EFWS is given in Tables B13-3 and B13-4. The reader should be cautioned that these are unavailabilities for Oconee's EFWS and HHASWS if the systems are considered independent of all others. In reality the EFWS shares the LPSWS with several other systems (see Appendix B14) so that the unavailability used for the EFWS in the sequence analysis calculation must be a conditional unavailability.

Table B13-1. Boolean Equation Term Descriptions

Boolean Term	Term Definition	Term Unavailability
A3	FDW-232 + FDW-317 + FDW-315	1.3×10^{-2}
B3	FDW-233 + FDW-319 + FDW-316	1.3×10^{-2}
E3	C575 + EFP-A + FDW-373 + FDW-370 + FDW-372	1.7×10^{-2}
G3	C576 + EFP-B + FDW-383 + FDW-380 + FDW-382	1.7×10^{-2}
F3	EFP-TD + FDW-88 + C-157 + C-156 + LPSW-137	1.1×10^{-1}
P3	MS-90 + MS-91 + MS-93 + MS-94 + MS-95 + MS-87	3.6×10^{-2}

Table B13-1 (Continued)

Boolean Term	Term Definition	Term Unavailability
LPSW[1]	Low Pressure Service Water Pump Cooling	2.7×10^{-5}
HHMAN	Operator Fails to Start HHASWS Remote Manually	1×10^{-1}
PCSNR	Failure to Restore the PCS Within 30 Minutes Given a T_2 Transient	1×10^{-1}

[1]Refer to Appendix B14.

Table B13-2. Component Unavailabilities

Component Description	Fault Identifiers	Failure Contributors	Q/Component
	FDW-232		
	FDW-317		
	FDW-233		
	FDW-319		
Check Valve	FDW-373		
	FDW-370		
	FDW-383	Hardware	1×10^{-4}
	FDW-380	Q Total	1×10^{-4}
	MS-91		
Electric Pump	EFP-A	Hardware	1×10^{-3}
	EFP-B	Control Circuitry	1.8×10^{-3}
		Maintenance	5.8×10^{-3}
		Fails to Run 24 hrs (3×10^{-5}/hr)	7.2×10^{-4}
		Q Total	9.3×10^{-3}
Air Operated Valve	FDW-315	Hardware	3×10^{-4}
(Normally Closed)	FDW-316	Control Circuitry	6.3×10^{-3}
	MS-93	Maintenance	5.8×10^{-3}
		Plugged	1×10^{-4}
		Q Total	1.3×10^{-2}

Table B13-2 (Continued)

Component Description	Fault Identifiers	Failure Contributors	Q/Component
Air Operated Valve (Normally Open)	MS-87	Operator Error	1×10^{-3}
		Plugged	1×10^{-4}
		Maintenance	5.8×10^{-3}
		Q Total	6.9×10^{-3}
Turbine governor Valve	MS-95	Plugged	1×10^{-4}
		DC oil pump fails	1×10^{-3}
		DC oil pump circuit	2×10^{-3}
		Maintenance	5.8×10^{-3}
		Q Total	8.9×10^{-3}
Turbine overspeed stop valve	MS-94	Plugged	1×10^{-4}
		Operator Error	1×10^{-3}
		Maintenance	5.8×10^{-3}
		Q Total	6.9×10^{-3}
Manual Valve	MS-90	Operator Error	1×10^{-4}
	C-575	Plugged	1×10^{-4}
	C-576		
	C-157		
		Q Total	2×10^{-4}
Manual Test Valve	FDW-88	Operator Error (leaves open after test)	1×10^{-3}
		Q Total	1×10^{-3}

Table B13-2 (Continued)

Component Description	Fault Identifier	Failure Contributors	Q/Component
Motor Operated	FDW-372	Plugged	1×10^{-4}
Valve	FDW-382	Operator Error	1×10^{-3}
(Normally Open)	C-156	Maintenance	5.8×10^{-3}
		Q Total	6.9×10^{-3}
Motor Operated	LPSW-137	Hardware	1×10^{-3}
Valve		Plugged	1×10^{-4}
(Normally Closed)		Control Circuitry	6.4×10^{-3}
		Maintenance	5.8×10^{-3}
		Q Total	1.3×10^{-2}
Turbine Pump	EFP-TD	Hardware[1]	9.1×10^{-2}
		Maintenance	5.8×10^{-3}
		Fails to Run (24 hrs 3×10^{-5}/hr)	8×10^{-4}
		Q Total	9.8×10^{-2}

[1]This unavailability is derived from plant test data for this pump taken from an April 25, 1979 letter from William O. Parker, Jr. (Duke Power) to Harold Denton (NRC).

Table B13-3. Quantitative Ranking of Terms in EFWS Boolean Equation Following T_2 and T_3 Transients

A3·B3	1.4×10^{-4}	
LPSW	2.7×10^{-5}	
E3·F3·G3	1.7×10^{-5}	
A3·G3·F3	1.6×10^{-5}	
E3·F3·B3	1.6×10^{-5}	Σ = CONST1
E3·P3·G3	5.8×10^{-6}	
E3·P3·B3	5.3×10^{-6}	
A3·G3·P3	5.3×10^{-6}	
	2.4×10^{-4}	

Note: Double and triple maintenance contributions have been removed from these terms.

Table B13-4. Quantitative Ranking of Terms in EFWS Boolean Equation Following T_1 Transients

E3·G3	1.7×10^{-4}	
E3·B3	1.6×10^{-4}	
A3·G3	1.6×10^{-4}	Σ = CONST2
A3·B3	1.4×10^{-4}	
LPSW	2.7×10^{-5}	
	6.5×10^{-4}	

Note: Double maintenance contributions have been removed from these terms.

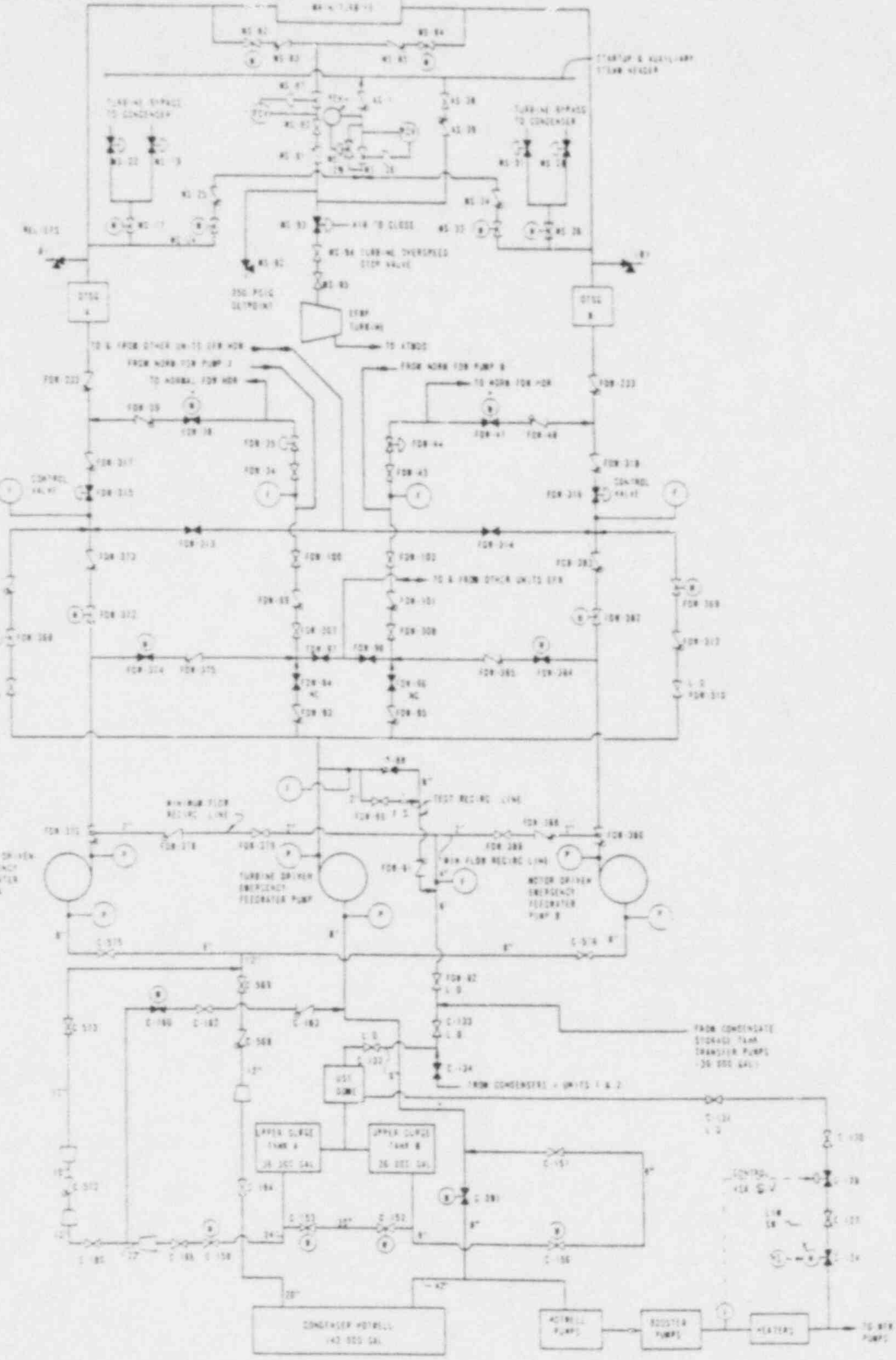


Figure B13-1. Oconee Emergency Feedwater System

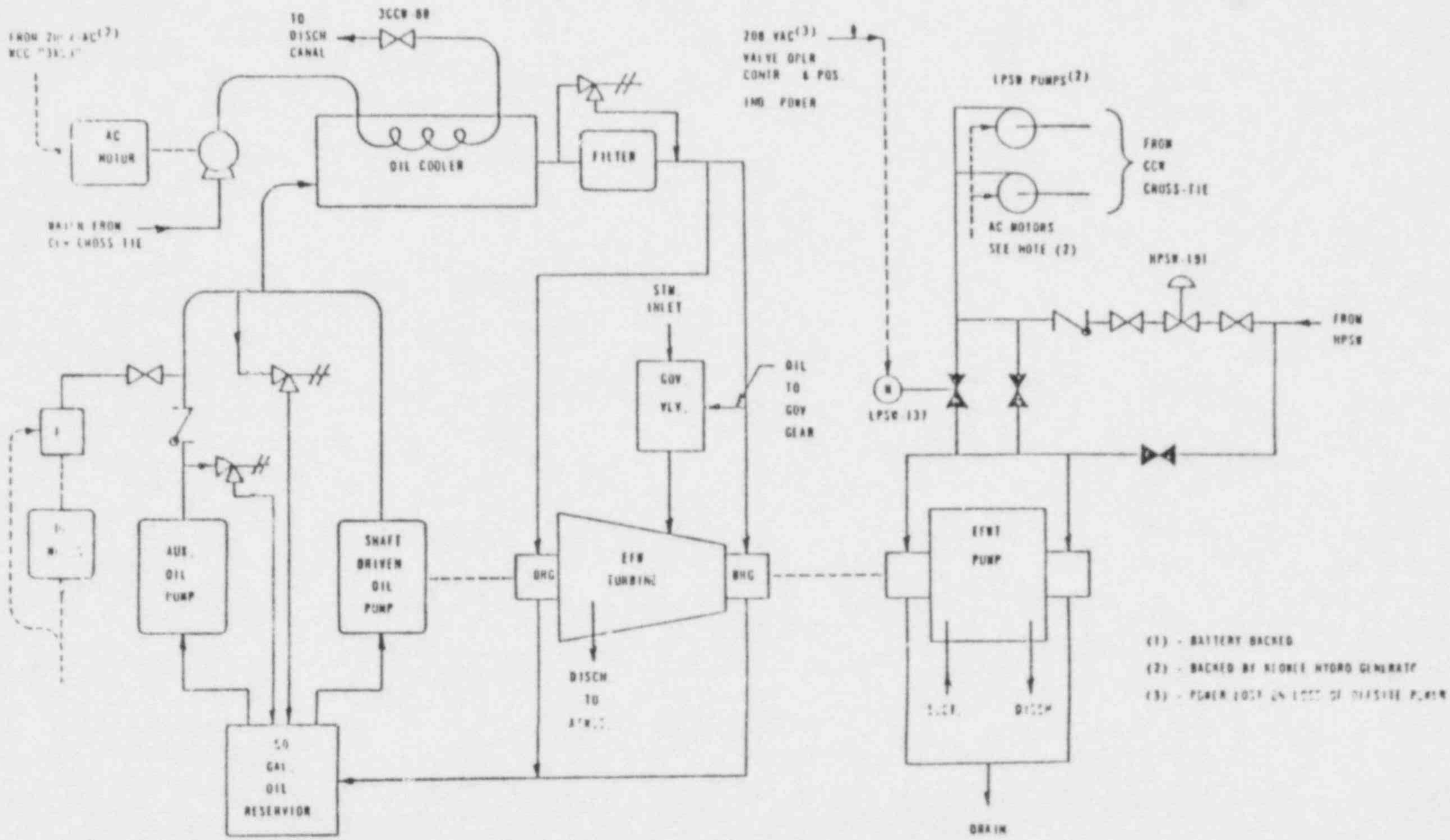


Figure B13-2. Oconee EFWS Turbine and Pump Support Systems

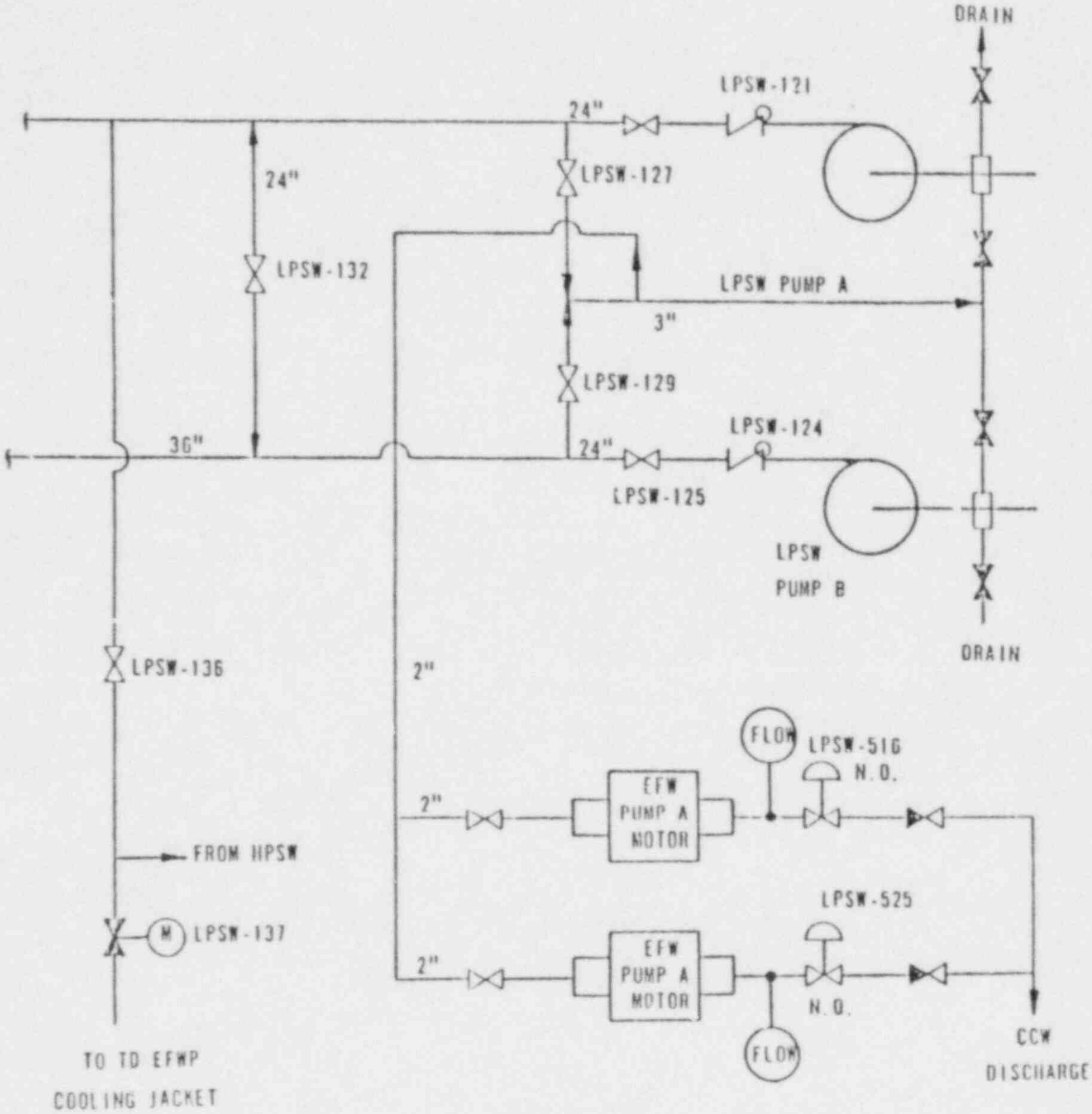


Figure B13-3. Oconee Units-Motor-Driven Emergency Feedwater Pump Motor Cooling Water (Note: Oconee Units 1 & 2 share 3 LPSW pumps; Oconee Unit 3 has 2 LPSW pumps as shown.)

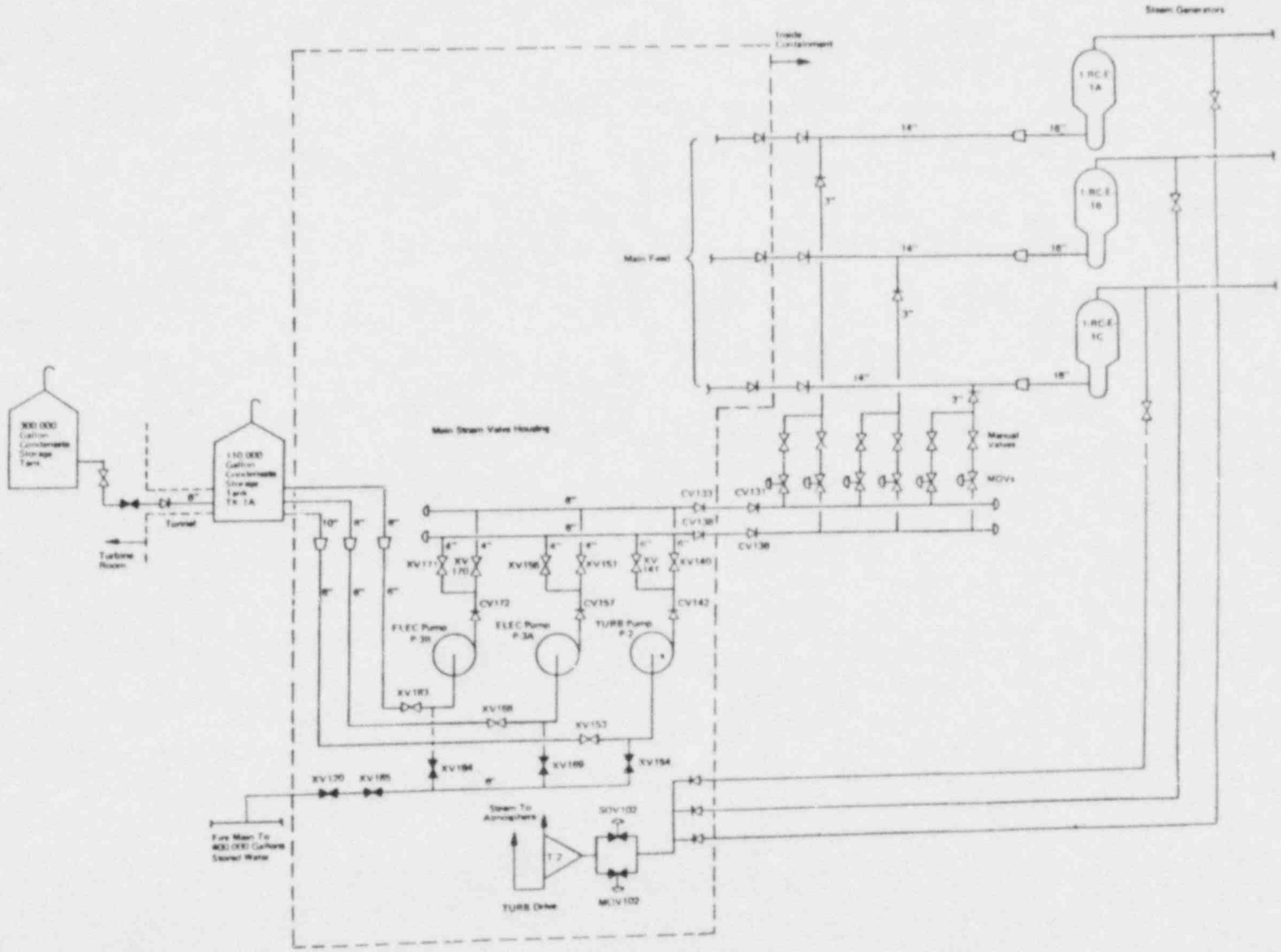


Figure B13-4. Surry Auxiliary Feedwater System Flow Diagram

APPENDIX B14

SURVEY AND ANALYSIS

LOW PRESSURE SERVICE WATER SYSTEM (LPSWS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Low Pressure Service Water System (LPSWS) was reviewed and compared with the similar PWR Containment Heat Removal System (CHRS) design (Surry) evaluated in the WASH-1400 study. The system designs for Oconee and Scurry are described in Sections 2 and 3 of this report, respectively. A comparison of the two systems is given in Section 4. LPSWS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate LPSWS failures into the Oconee accident sequences and a point estimate of the LPSWS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE LPSWS DESCRIPTION

2.1 System Description

The function of the LPSWS is to provide cooling water to components in the turbine, auxiliary, and reactor buildings for normal and emergency services. Engineered Safety Feature components cooled by the LPSWS include the high pressure injection and emergency feedwater pumps. Following a LOCA, the LPSW performs the function of containment heat removal by providing water to cool the reactor building air and the emergency Reactor Building Cooling System (RBCS) sump via the fan cooling units and the LPIS coolers. The LPSWS consists of two 15000 gpm pumps, supply lines and headers, and associated piping, valves, instrumentation and controls (see Figure B14-1).

The source of the cooling water for the LPSW system is the CCW System which draws its water from the Little River arm of Lake Keowee and discharges it into the Keowee River arm of Lake Keowee. Four condenser circulating water pumps, each rated at 177000 gpm, supply water into a common condenser intake via two 11-foot conduits. The water is drawn from the river by a siphon created by plant vacuum pumps at start-up and sustained during operation by continuous priming pumps. The CCW pumps are required only to overcome pipe and condenser friction losses. A 48-inch emergency discharge line to the Keowee hydro tailrace is connected to each of the three condensers of each unit. Under a loss of power condition, the emergency discharge line opens automatically while the vacuum for the siphon is maintained by steam ejectors. The LPSWS pumps take their suction from a 42-inch crossover line between the condenser inlet headers. Cooling water to the RBCS units and the LPIS coolers is provided by the pumps via separate supply lines which can be isolated by remotely operated isolation valves. The return lines from these systems are separate to a point beyond a remotely operated isolation valve. Isolation valves are incorporated in all LPSW lines penetrating the containment. The LPSW is monitored and operated from the control room.

The RBCS coolers are supplied by individual lines from the separate LPSWS supply headers. Each inlet line is provided with a motor operated shutoff valve located outside the containment. Similarly, each discharge line from the coolers is provided with a motor operated valve located outside the containment. This allows each cooler to be isolated individually.

During normal operation, the cooling requirements are supplied via one LPSWS pump and flow through the coolers will be throttled for containment temperature control by the motor operated throttle valves on the discharge of each cooler. These valves open automatically upon engineered safeguards signal to provide full emergency flow through the coolers.

The LPSWS flow to and from each RBCS cooler is measured. The inlet and outlet flow indications are compared and any excessive deviations are annunciated as an indication of cooler leakage. The LPSWS return from the auxiliary building is monitored for radioactivity. Upon any indication of radioactivity in the effluent, the component suspected of leaking may be individually isolated. The LPSWS pumps are connected to the 4160 volt buses which supply power to engineered safeguards equipment. The emergency power supply is designed to operate all LPSW pumps upon a loss of offsite power.

2.2 System Operation

During normal operation, the component cooling requirements are supplied by one LPSWS pump. When the reactor coolant system pressure falls to 500 psig or the reactor building pressure rises to 4 psig, following a LOCA, the Engineered Safeguards Protective System (ESPS) provides signals which initiate the following actions:

1) ESPS Channels 3 and 4 start with LPSWS pumps (LPSW-P3A and LPSW-P3B) and open the discharge valves for the LPIS coolers (i.e., closes LPSW-4 and LPSW-5).

2) ESPS Channels 5 and 6 isolate the reactor coolant pump oil and bearing coolers (LPSW-6 and LPSW-15) and open the discharge valves for the RB cooling unit (LPSW-18, LPSW-21, and LPSW-24).

The low pressure service water is delivered to the RB coolers and the LPIS coolers at a pressure of 65 psig and a temperature ranging between 45° F to 76° F.

3.0 SURRY CHRS DESCRIPTION

The function of the Containment Heat Removal System (CHRS) is to cool the containment sump water being recirculated through the Containment Spray Recirculation System (CSRS). The system includes the cooling water source, the secondary side of four heat exchangers and associated piping and valves (see Figure B14-2).

River water is the source of service for the heat exchangers. The service water is directed through the secondary side of the heat exchangers for heat removal and is discharged into the discharge canal. The water is supplied from the Circulating Water System by gravity flow between the high level intake canal and discharge canal seal pit.

Intake canal water flows under the influence of a 20-foot gravity head through the heat exchangers when the MOV-SW-103 valves are opened via the Consequence Limiting Control System (CLCS) HI-HI signals.

The water flows from the common header through normally open valves (MOV-SW-104), through the heat exchangers, and then through another set of normally open valves (MOV-SW-105) into the discharge canal. The containment sump water is recirculated at a higher pressure than service water; therefore, leakage would be of sump water to the discharge cooling water. A sample of discharge water from each heat exchanger is passed through radiation monitors (RM-SW-114, -115, -116, and -117) which are automatically started by the CLCS HI-HI signals. If activity is detected in one of the discharge lines, the plant procedures require the operator to close the appropriate isolation valves (MOV-SW-105 valves and MOV-SW-104 valves) to isolate the leaking heat exchanger.

Air vents are located at the high point in each of the service water supply and discharge lines (eight in total). Each line is two inches in diameter and includes a (normally open) manual valve and a check valve. The purpose of these vents is to allow air in the heat exchanger system to escape, in order not to impede the start of service water flow.

The level in the intake canal is maintained by eight circulating water pumps which supply water from the river. These pumps are powered by offsite power. If offsite power is lost, water flow into the intake canal from these pumps is stopped and flow from the canal to the two condensers in each unit must be stopped to avoid draining the 25,000,000 gallon intake canal. Upon receipt of a "loss of electric power" signal coincident with a CLCS HI-HI signal in Unit 1, the condenser inlet and outlet valves (MOV-SW-106) and -100) are automatically closed on the Unit 1 condensers. At the same time one valve in each circulating water line to the Unit 2 condenser is closed (MOV-SW-200B, -200D, -206A, -206C). Since the accident has directed the swing diesel (No. 3) to Unit 1, only the No. 2 diesel is available for Unit 2, and hence only four of the eight valves on Unit 2 have power. The operators have the capability of switching the No. 3 diesel generator to Unit 2, from the control room, should such a condition exist.

There are three diesel driven emergency service water pumps of 15000 gpm each, which can supply water to the intake canal from the river and which start upon loss of station power; these are only intended to supply the necessary service water under the assumption that all condenser main coolant lines are closed.

a. The CHRS is designed on the following basis:

1. Two of the four heat exchangers are required for the first 24-hours following an accident, and only one after this period.

2. Sufficient cooling water flow to all four heat exchangers can be obtained through either of two lines from the intake canal and through any one of the four MOV-SW-103 valves provided that normally open valves MOV-SW-106A and SW-106B are open.

4.0 COMPARISON OF OCONEE LPSWS AND SURRY CHRS

The CHRS system at Surry and the LPSWS at Oconee both rely on river water to cool the containment sump recirculating water and other portions of the operating plant. Major differences appear in the means by which this water is routed to the CHRS/LPSWS and the interface of the heat exchangers with the ESF systems. At

Surry, service water is pumped from the James River into the 25-million-gallon intake channel. This water gravity feeds the four heat exchangers in the CSRS then on to the discharge channel back into the river. At Oconee, water is obtained from the Little River arm of Lake Keowee and is delivered via a siphon effect created and maintained by vacuum pumps to the reactor building cooling system (RBCS) heat exchangers and the LPIS coolers. Other pumps are employed to overcome friction losses. Upon loss of offsite power the siphon effect is maintained by steam ejectors.

The RSS estimated a 8.5×10^{-5} unavailability for Surry's CHRS. Oconee's LPSWS unavailability was estimated in Section 5.2.2 to be 2.7×10^{-5}.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The LPSWS provides the containment overpressure protection function by extracting reactor decay heat from the containment via heat exchangers associated with the RBCS units and the LPRS coolers. The system also provides cooling of critical ESF components such as the high pressure injection and emergency feedwater pumps.

The LPSWS is required for successful RBCS operation and therefore contributes to events Y and Z on the LOCA event trees and event O on the transient trees. If containment overpressure protection is not established by the RBCS it can also be achieved by the operation of the CSRS, LPRS and cooling of the LPRS heat exchangers by the LPSWS. In this mode of operation, the containment atmosphere is cooled by mixing CSRS flow with the LPRS flow in the containment sump. This method of containment overpressure protection is modeled by event G on the LOCA event trees.

Since the LPSWS is required for high pressure injection pump cooling, it contributes to event D on the LOCA event tree and event U on the transient tree. Cooling by the system is also required by the emergency feedwater pumps. The LPSWS therefore contributes to event L on the transient trees.

In all situations successful operation of the LPSWS requires full flow from one of the two pumps.

5.2 LPSWS Model Description

5.2.1 LPSWS Boolean Equations

Two Boolean equations were developed to model LPSWS failure. The first equation models the failure of the normally operating train to remain functional and the inability to get the second LPSW train operational. The equation is:

$$LPSW = F1 \cdot (G1 + CH4 + RCSLOCM \cdot RBHICM + RCSRBCM).$$

This equation was input to the Boolean equations describing failure of the RBCS (Appendix B15), the HPIS (Appendix B8), the EFWS (Appendix B13), and the Boolean equation describing event G, failure of containment overpressure protection via the LPIS heat exchangers. The equation used to model event G is discussed below.

Table B14-1 lists descriptions of each term in the previous equation. Refer to Figure B14-1 for a simplified diagram of Oconee's LPSWS.

Table B14-2 lists component types in the LPSWS, fault identifiers that label specific components, and failures that contribute to the component unavailability. These unavailabilities are comprised of hardware, human, and test and maintenance faults. Testing of the LPSWS valves was found to add negligibly to the valve unavailability and was therefore not included.

Testing of the idle LPSWS pump is conducted monthly. The average outage time for pump test is taken from the RSS as 1.4 hours. The unavailability of the pump due to test is therefore:

$$\frac{1.4}{720} = 1.9 \times 10^{-3} \quad .$$

Technical specifications state that maintenance is allowed during power operation on any component which will not remove more than one train (flow path) of a system from service. Components shall not be removed from service so that the affected system is inoperable for more than 24 consecutive hours after which it will be shut down. The average maintenance interval used in the Reactor Safety Study is 4.5 months, which corresponds to a frequency of 0.22 per month. From the Reactor Safety Study (Table III 5-3), the lognormal maintenance act duration for components whose range is limited to 24 hours is a mean time of 7 hours. The unavailability of one component due to maintenance is estimated to be:

$$\frac{7(.22)}{720} = 2.1 \times 10^{-3} \quad .$$

The Boolean equation used to model event G is given below. The equation models failure of both LPRS trains or their associated

LPSWS trains to remove heat from the containment using the LPRS heat exchangers. One LPRS and LPSWS train must operate in conjunction with one CSRS train to provide successful containment overpressure protection during recirculation when the RBCS is unavailable. The equation is

$$\begin{aligned} LPCOOL = {} & (B + E + J + CH4 + E' + X + L1) \cdot \\ & (C + D + K + CH3 + D' + W + M1) + LPSW. \end{aligned}$$

Each term in the above equation except for L1, M1 and LPSW is described in Section 5.2 of the LPIS Appendix B6 or the LPRS Appendix B7. The term LPSW represents the first Boolean equation discussed in this section. The descriptions of the remaining terms and component unavailability estimates can be found in Tables B14-1 and B14-2.

5.2.2 LPSWS Unavailability

Using the first Boolean equation given in the last section and the term unavailabilities given in Table B14-1, an independent LPSWS point estimate unavailability can be calculated. This is found to be:

$$LPSW = 2.7 \times 10^{-5}/\text{reactor year.}$$

A quantitative ranking of the Boolean terms for the LPSWS is given in Table B6-3. As can be noted greater than 99 percent of the system unavailability is due to the first two terms F1 · G1 and F1 · CH4

Using the second Boolean equation given in the last section and the term unavailabilities given in Tables B14-1, B6-1 and

B7-1, an independent LPCOOL point estimate unavailability can be estimated. This is found to be:

$$\text{LPCOOL} = 1.4 \times 10^{-3}/\text{reactor year.}$$

Referring again to the Boolean equation, it can be noted that the terms in parenthesis would expand to 49 terms. However, 36 of the 49 terms represent combinations of double LPIS, double LPRS, or double LPIS train A-LPRS train B (or vice versa) failures. For example, one of these 36 would be D·F which is failure of both low pressure trains during the injection phase. In order for LPCOOL to be demanded, LPIS and LPRS must succeed (LPIS and CPRS success require at least one train operating). Double injection, double recirculation and double LPIS train A-LPRS train B (or vice versa) failure terms were therefore removed from the probability calculation. (During the accident sequence analysis these double terms in the LPCOOL Boolean equation were automatically removed by combining the complemented LPIS and LPRS Boolean equations with the LPCOOL equation. This is done by applying the Boolean identity $P \cdot \overline{P} = \emptyset$.)

A quantitative ranking of the Boolean terms is given in Table B14-4.

The reader should be cautioned that these are unavailabilities for Oconee's LPSWS and containment heat removal system via the LP coolers (LPCOOL) if the system is considered independent of all others. In general, these unavailabilities will depend on what other system successes or failures have occurred; i.e., the unavailability used for the LPSWS and LPCOOL in the sequence analysis calculation must be a conditional unavailabilty.

Table B14-1. Boolean Equation Term Descriptions

Boolean Term	Term Definition	Term Unavailability
F1	LPSW-P3B + VP1	1.4×10^{-3}
G1	LPSW-P3A + VP2	1.4×10^{-2}
CH4[1]	ESPS Actuation Train (Channel 4)	5×10^{-3}
RCSLOCM[1]	Sensor Group RCSLO Common Mode	1×10^{-3}
RBHICM[1]	Sensor Group RBHI Common Mode	1×10^{-3}
RCSRBCM[1]	Common Mode Failure Between RCSLO and RBHI	3.2×10^{-5}
L1	LPSW-72 + LPSW-78 + LPSW-5 + LPSW-76	1.3×10^{-2}
M1	LPSW-71 + LPSW-77 + LPSW-4 + LPSW-75	1.3×10^{-2}

1. Refer to Appendix B10.

Table B14-2. Component Unavailabilities

Component Description	Fault Identifiers	Fault Contributors	Q/Component
Check Valve	LPSW-75 LPSW-76	Hardware	1×10^{-4}
		Q Total	1×10^{-4}
Pump (Normally Operating)	LPSW-P3B (Centrifugal) VP1 (vacuum)	Fails to Run (3 x 10^{-5}/hr for 24 hrs	7.2×10^{-4}
		Q Total	7.2×10^{-4}
Pump (Normally Idle)	LPSW-P3A (Centrifugal) VP2 (vacuum)	Hardware	1×10^{-3}
		Control Circuitry	1.8×10^{-3}
		Test	1.9×10^{-3}
		Maintenance	2.1×10^{-3}
		Q Total	6.8×10^{-3}
Motor Operated Valve or Air Operated Valve (Normally Open)	LPSW-77 LPSW-78	Operator Error	1×10^{-3}
		Plugged	1×10^{-4}
		Maintenance	2.1×10^{-3}
		Q Total	3.2×10^{-3}
Motor Operated Valve (Normally Closed)	LPSW-5 LPSW-4	Hardware	1×10^{-3}
		Plugged	1×10^{-4}
		Control Circuitry	6.4×10^{-3}
		Maintenance	2.1×10^{-3}
		Q Total	9.6×10^{-3}
Manual Valve (Nornally Open)	LPSW-72 LPSW-71	Plugged	1×10^{-4}
		Operator Error	1×10^{-4}
		Q Total	2×10^{-4}

Table B14-3. Quantitative Ranking of Terms in LPSW Boolean Equation

F1·G1	2×10^{-5}
F1·CH4	7×10^{-6}
F1·RCSRBCM	4.5×10^{-8}
F1·RCSLOCM·RBHICM	1.4×10^{-9}
Point Unavailability	$= 2.7 \times 10^{-5}$

Table B14-4. Quantitative Ranking of Terms in LPCOOL Boolean Equations

L1·D	2.3×10^{-4}
M1·E	2.3×10^{-4}
L1·M1	1.7×10^{-4}
L1·W	1.2×10^{-4}
M1·X	1.2×10^{-4}
L1·CH3	6.5×10^{-5}
M1·CH4	6.5×10^{-5}
L1·D'	4.6×10^{-5}
M1·E'	4.6×10^{-5}
L1·C	4.3×10^{-5}
M1·B	4.3×10^{-5}
LPSW	2.7×10^{-5}
L1·K	1.3×10^{-6}
M1·J	1.3×10^{-6}
Point Unavailability	$= 1.4 \times 10^{-3}$

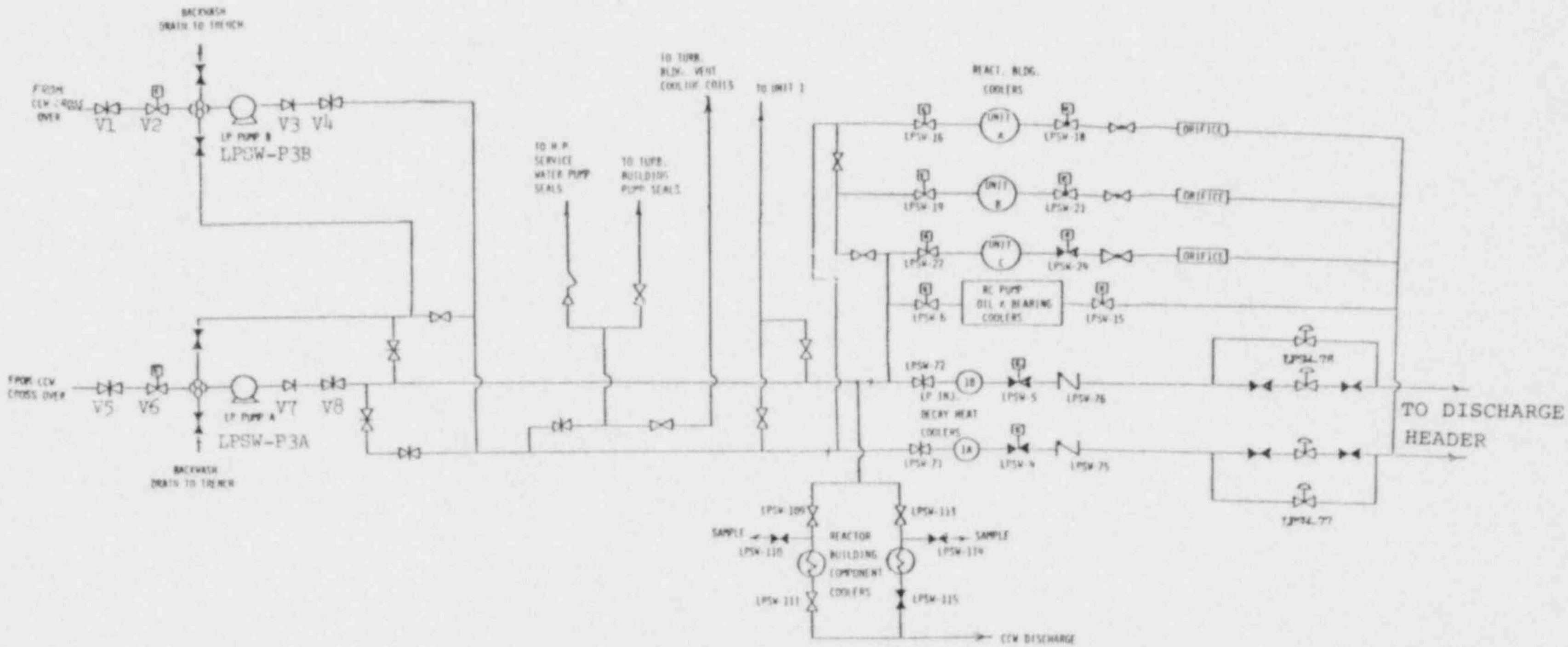


Figure B14-1. Oconee No. 3 LPSW System Schematic

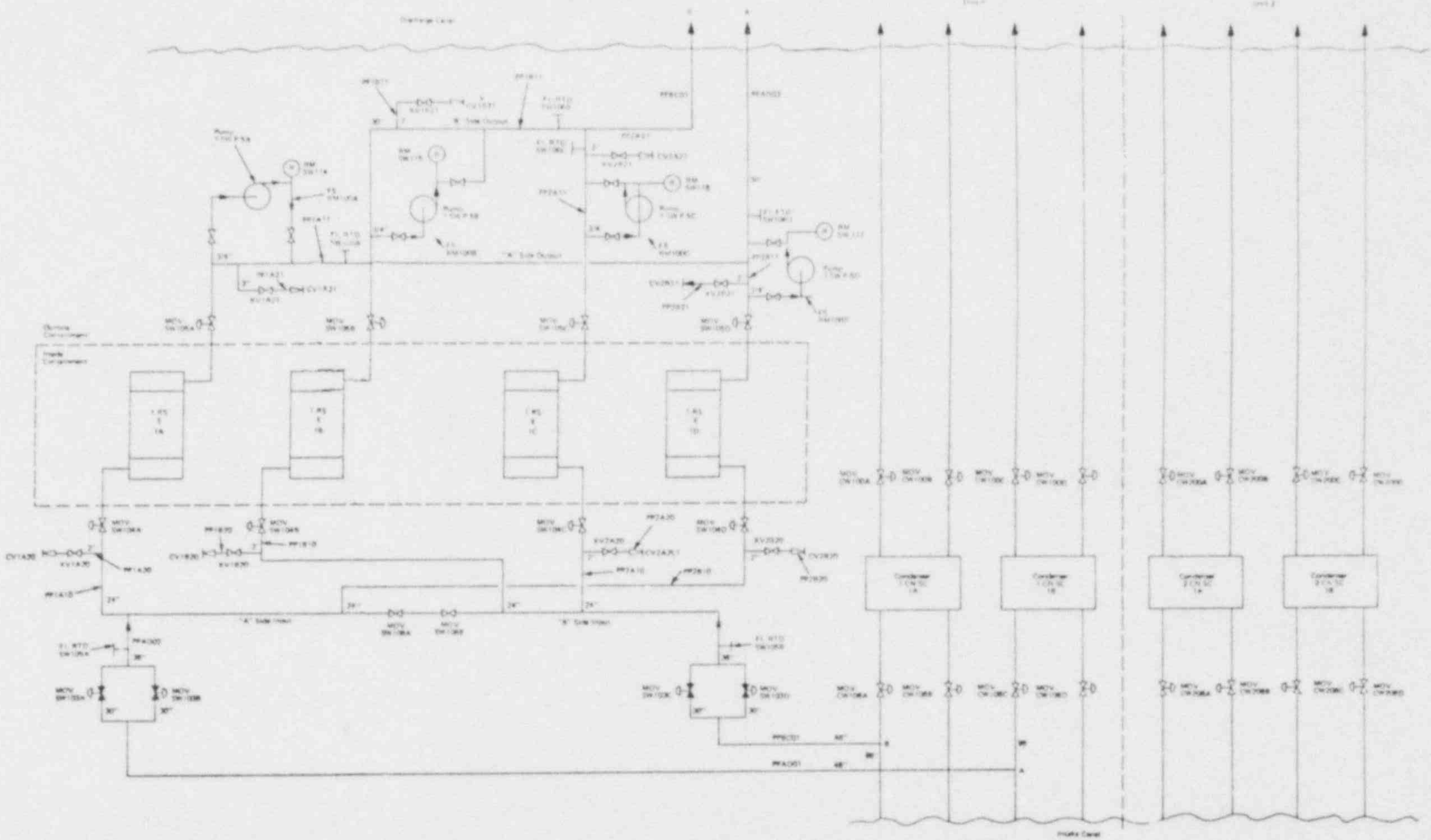


Figure B14-2. Surry CHRS System Flow Diagram

APPENDIX B15

SURVEY AND ANALYSIS

REACTOR BUILDING COOLING SYSTEM (RBCS) - OCONEE PLANT

TABLE OF CONTENTS

1.0 INTRODUCTION

The Oconee Unit 3 Reactor Building Cooling System (RBCS) was reviewed. Since the WASH-1400 Surry PWR does not have a similar system, a comparison could not be made. The RBCS design for Oconee is described in Section 2 of this report. RBCS event tree interrelationships are detailed in Section 5. Also included in Section 5 is a description of the model used to incorporate RBCS failures into the Oconee accident sequences and a point estimate of the RBCS unavailability assuming independence from all other Oconee systems.

2.0 OCONEE RBCS DESCRIPTION

2.1 System Description

The RBCS utilizes an independent portion of the normal reactor building ventilation system to remove heat from the containment atmosphere, after an accident, to prevent the building pressure from exceeding design limitations.

The reactor building ventilation system which is composed of three independent systems: the RBCS, the reactor building auxiliary fans, and the reactor building purge system. The portion of the ventilation system utilized for emergency building cooling is the RBCS which consists of three independent cooling units (Figure B15-1) located within the reactor building, but outside of the secondary shield for missile protection. Each unit consists of a fan, a tube cooler and associated common ducting to distribute the circulated building atmosphere to equipment and areas, including the reactor cavity, within the containment. The fan-cooling units are located at an elevation above the potential water level in the reactor building during post-accident conditions to protect them from flooding, and utilize lake supplied low pressure service water as the heat transfer medium. The service water is supplied to the coolers by two redundant and independent 15,000 gpm pumps through individual isolation protected supply and return lines (See Appendix B14).

Electric motor driven axial flow fans force the reactor building atmosphere through the coolers and ductwork for distribution within the containment. The ducting incorporates both blowout and fusible dropout plates to protect the fan and cooler at the onset of an accident and to provide unobstructed post-accident circulation.

2.2 System Operation

During normal reactor power operation, the RBCS provides for removal of normal heat losses from equipment and piping in the reactor building. This is accomplished by operation of two of the three fan-cooler units at full speed with their coolant flow throttled to 235 gpm/loop. The equipment, piping, valves and instrumentation, except for distribution ducting are located either outside the secondary shield within the reactor building or outside the reactor building itself. Thus the equipment can be regularly inspected, tested and maintained during reactor power operation. Cooler performance is individually monitored by inlet and outlet flow meters, thermocouples, and outlet radiation monitors; all of which are displayed in the main control room and annunciated in the case of flow leakage or high radioactivity. Operator control of inlet and outlet flow valves is provided for flow throttling and isolation.

Upon receipt of an engineered safeguards protective system signal the system is automatically reconfigured as follows:

- The low pressure service water valves in the cooler discharge, external to the reactor building, are fully opened to increase the coolant flow to 1400 gpm/loop (LPSW-18, LPSW-21, LPSW-24).
- The third fan-cooling unit is started and the speed of all three fans is set at half speed to reduce the power requirements generated by the denser building atmosphere.
- The fusible dropout plates in the cooler discharge duct melt and drop off, assuring an unobstructed discharge path.
- Depending on the accident severity, the downcomer blowout plates will be forced off, attenuating any possible shock waves before they damage the cooling coil and fan.
- Closure of the automatic isolation dampers provide shutdown of the reactor building purge system if it is in operation at the time of the accident.

The continuous circulation of the post-accident reactor building airstream mixture through the three coolers in this emergency mode is designed for removal of a minimum of 240×10^6 Btu/hr which is in excess of that required to depressurize the containment for Loss of Coolant Accidents (LOCA) with successful emergency core coolant injection. It is assumed that the cooler coils will not clog up during a LOCA.

3.0 SURRY RBCS DESCRIPTION

The Surry plant does not have the equivalent to a RBCS.

4.0 COMPARISON OF OCONEE AND SURRY RBCS

Since the Surry reactor does not have the equivalent of a RBCS, a description and comparison is not possible.

5.0 OCONEE SYSTEM EVALUATION

5.1 Event Tree Interrelationships

The RBCS operating in its emergency cooling mode, is one of two independent systems designed to provide immediate and long term cooling of the reactor building atmosphere to depressurize and maintain the containment below rupture pressure following the post-accident pressure excursion. The second system is the containment spray system which is automatically initiated at a reactor building pressure of 10 psig and is also designed to provide 100% of the design cooling capability. According to the definition of containment overpressure protection given in the FSAR, either of these two systems operating alone, at full capacity, or two of the three cooling units in conjunction with the spray system at one-half capacity will provide sufficient post-accident heat removal for successful reactor building pressure control. These criteria for success have been found in subsequent research conducted by Battelle Columbus Laboratories to be conservative. Their research has shown that one spray sub-system operating with a low pressure recirculation system heat exchanger or one fan cooling unit will provide adequate pressure control. These more realistic criteria have been used in this study.

Operation of the RBCS appears as event Y on the Oconee LOCA event trees. Continued operation of the RBCS during the time interval corresponding to the recirculation phase of the emergency coolant recirculation system (event H) and containment spray recirculation system (event F) is modeled by Event Z. The RBCS is also part of the containment pressure reduction event (event O) on the transient event tree. In all three events, Y, Z, and O, successful operation of the RBCS requires the operation or continued operation of 1 of 3 fan cooler units.

5.2 RBCS Model Description

5.2.1 RBCS Boolean Equations

The general form of the RBCS Boolean equation used in the accident sequence analysis is depicted below for one of three RBCS units required for success:

$$\begin{aligned} RBCS = {} & (H1 + CH5)\cdot(J1 + CH5\cdot CH6)\cdot \\ & (K1 + CH6) + LPSW + RBHICM \\ & + LOPNRE\cdot LOPNRL \end{aligned} \qquad \text{(Eq. B15-1)}$$

Table B15-1 relates each term in the ρ evious equation to the components shown in Figure B15-1. Table 15-2 lists component unavailabilities and each of the contributors to the component unavailability. The unavailabilities listed in Table B15-2 are comprised of hardware, human and maintenance faults.

The above equation, except for the last LOPNRE'LOPNRL term, was utilized in modeling the RBCS when AC power was available (all sequences except $T_1(B_3)$). Equation B15-1, without the last term, is referred to as Eq. B15-1(a) in Chapter 4 of the main report. The entire equation was used to model the system when no AC power is initially available (e.g., loss of offsite power followed by a failure of the emergency AC hydro system to start), $T_1(B_3)$.

Testing of the RBCS components was found to negligibly add to the component unavailability when compared to other contributions and was therefore not included.

The unavailability of one RBCS train due to maintenance is determined by considering the non-routine maintenance performed on the cooling units and the motor operated valves (MOVs). The maximum outage allowed for the MOVs is 24 hours. Maintenance time ranges from 30 minutes to 24 hours with a log normal mean time of 7 hours. Non-routine maintenance ranges from monthly to yearly with a mean maintenance interval of 4.5 months or a frequency of .22 per month. The unavailability due to maintenance of two valves is therefore:

$$2 \times \frac{7(.22)}{720} = 4.3 \times 10^{-3} .$$

One reactor building cooling fan and associated cooling unit can be out of service for 7 days provided both reactor building spray pumps and associated nozzles are in service at the same time. Maintenance time ranges from 30 minutes to 7 days with a log normal mean downtime of 55 hours and a maintenance frequency of .22 per month. The unavailability due to maintenance of one cooling unit is:

$$\frac{55(.22)}{720} = 1.7 \times 10^{-2} .$$

Therefore, the maintenance contribution per train is 2.1×10^{-3}.

A common mode failure was identified in the RBCS. The system is actuated by the reactor building high pressure sensor group RBHI employing 2 out of 3 logic. A 1×10^{-3} common mode unavailability was attributed to this sensor group due to a possible human error of miscalibrated two or more sensors in a group. This common mode is designated RBHICM in the Boolean equation. For more details concerning ESPS actuation faults and common mode failure, see Appendix B10.

5.2.2 RBCS Unavailability

Using the Boolean equations given in the last section and the term unavailabilities given in Table B15-1, independent RBCS point estimate unavailabilities can be calculated. These are found to be:

$Q(RBCS) = 1.6 \times 10^{-3}$ (Applies to cases with AC power available)

and

$Q(RBCS) = 4.6 \times 10^{-3}$ (Applies to cases with AC power not initially available)

It should be noted that the RBCS is unavailable if all AC is lost.

Double maintenance contributions, i.e. components of both train being in maintenance, were removed from these unavailabilities since this condition was not allowed by technical specifications.

A quantitative ranking of the Boolean terms for the 1 of 3 RBCS case for cases with AC power available is given in Table B15-3. As can be noted, 93% of the system unavailability is due to actuation faults with 63% due to the term RBHICM. For the case in which AC power is not initially available, the system unavailability is dominated by the failure to recover offsite power within approximately 40 minutes and failure of the operator to notify the Lee Steam Station AC power source. This failure is represented by the term LOPNRE·LOPNRL.

The reader should be cautioned that these are unavailabilities for Oconee's RBCS if the system is considered independent of all others. In general, the RBCS unavailability will depend on what other system successes or failures have occurred, i.e., the unavailability used in the sequence calculations must be a conditional unavailability.

Table B15-1. Boolean Equation Term Definitions[1]

Boolean Term	Term Definition	Term Unavailability
H1	LPSW-16 + LPSW-C1A + LPSW-18	2.6×10^{-2}
J1	LPSW-19 + LPSW-C1B + LPSW-21	2.6×10^{-2}
K1	LPSW-22 + LPSW-C1C + LPSW-24	2.6×10^{-2}
CH5[2]	ESPS Actuation Train A (Channel 5)	2.2×10^{-2}
CH6[2]	ESPS Actuation Train B (Channel 6)	2.2×10^{-2}
RBHICM[2]	Sensor Group RBHI Common Mode	1×10^{-3}
LPSW[3]	Low Pressure Service Water to RBCS Cooling Coils	2.7×10^{-5}
LOPNRE[1]	Offsite Power Not Restored within Approximately 40 minutes (Applies to Loss of All AC Only)	2×10^{-1}
LOPNRL[1]	Operator Fails to Notify Lee Steam Station AC Power Source (Applies to Loss of All AC Only)	1.5×10^{-2}

1. Refer to Appendix B1.
2. Refer to Appendix B10.
3. Refer to Appendix B14.

Table B15-2. Component Unavailabilities

Component Description	Fault Identifiers	Failure Contributors	Q/Component
Fan Cooler	LPSW-C1A	Fails to Run 24 Hrs.	
	LPSW-C1B	24 x $(1x10^{-5}$/hr.)	2.4×10^{-4}
	LPSW-C1C	Fails to Change	
		Speed (start)	3×10^{-4}
		Control Circuitry	1×10^{-3}
		Maintenance	1.7×10^{-2}
		Q Total	1.9×10^{-2}
Motor Operated	LPSW-16	Plugged	1×10^{-4}
Valve	LPSW-19	Operator Error	1×10^{-3}
(Normally Open)	LPSW-22	Maintenance	2.1×10^{-3}
		Q Total	3.2×10^{-3}
Motor Operated	LPSW-18	Hardware	1×10^{-3}
Valve	LPSW-21	Plugged	1×10^{-4}
(Normally	LPSW-24	Control Circuitry	1×10^{-3}
Throttled)		Maintenance	2.1×10^{-3}
		Q Total	4.2×10^{-3}

Table B15-3. Quantitative Ranking of Boolean Equation Terms

RBHICM	1×10^{-3}
CH5·CH6	4.8×10^{-4}
LPSW	2.7×10^{-5}
H1·J1·K1	1.8×10^{-5}
H1·J1·CH6	1.5×10^{-5}
CH5·J1·K1	1.5×10^{-5}
	1.6×10^{-3}

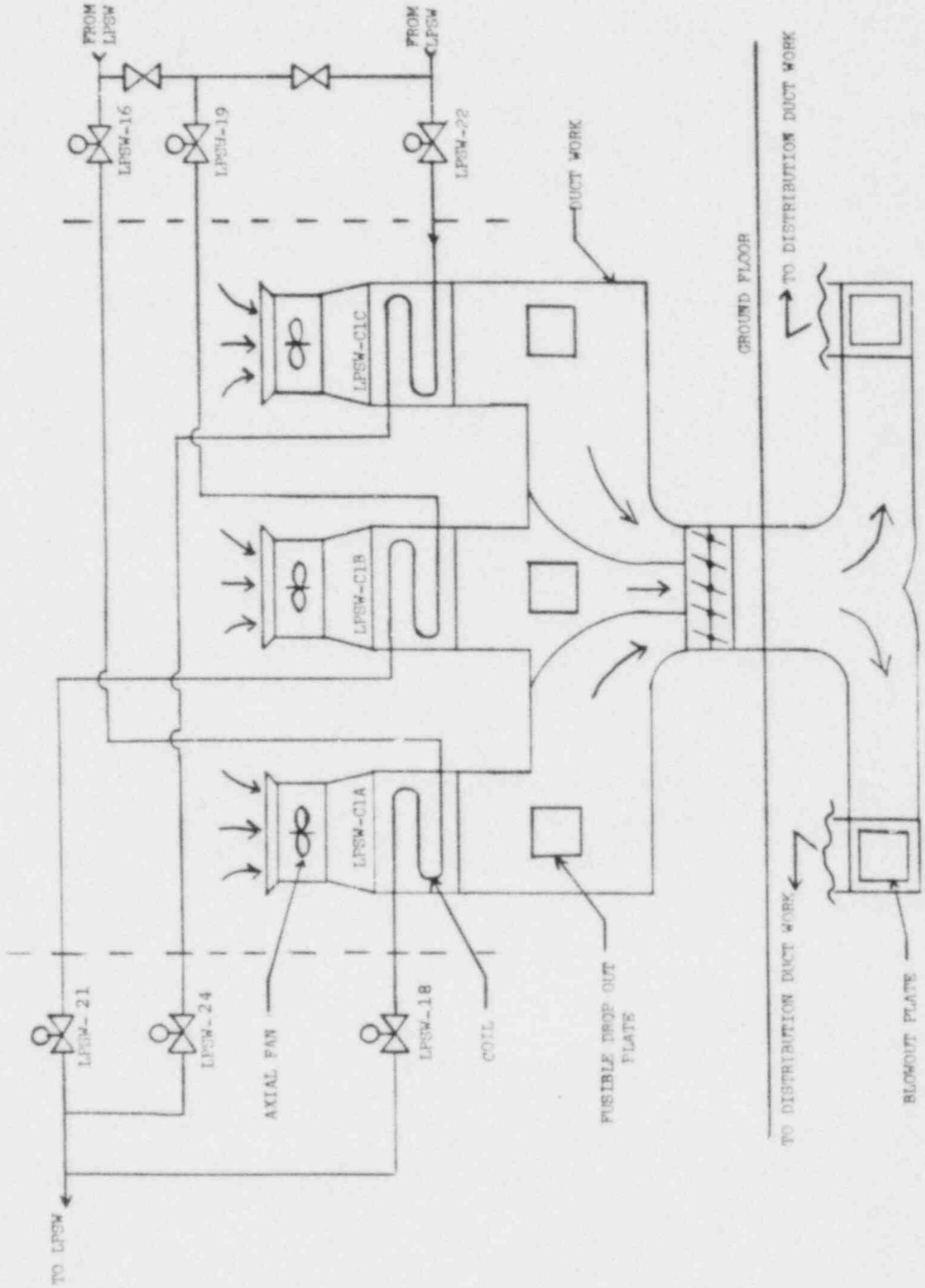


Figure B15-1. Reactor Building Cooling System

APPENDIX C

OCONEE CORE MELT SEQUENCES

TABLE OF CONTENTS

1.0 OCONEE LOCA SEQUENCES (A, S_1, S_2, S_3) D AND TMLQD

The Oconee LOCA cases are dominated by sequences in which the ECC fails either in the injection (D) or recirculation (H) modes. Generally, either the containment sprays or building coolers work in these sequences so that early containment failure due to excessive steam generation is not likely. However, the MARCH calculations indicate the containment will generally contain flammable hydrogen mixtures shortly after the end of the core meltdown period. If hydrogen burning is delayed until after head failure, when all the hydrogen produced (by reacting 100 percent of the cladding) is released to the containment, containment overpressurization is likely.

For some small break LOCAs in which neither ECC nor containment safeguards function, there is also a significant probability of containment overpressurization failure due to rapid boiloff of water from the reactor cavity following head failure. Since the major source of the water in the reactor cavity is the core flood tanks, the timing of core flood tank injection is important. The containment failure probability is significant only for those small LOCA break sizes for which the flood tanks do not inject until bottom head failure. MARCH calculations for a case in which the steam generator heat sink is lost indicate the cross-over point for core flood tank injection is a break size somewhat less than 2.3 inches. With successful ECC injection but failure in the recirculation mode, the cross-over break-size for core flood tank injection would be reduced. Availability of the steam generators would also affect these results. However, MARCH calculations were not performed to precisely define these cross-over values.

1.1 Sequence TMLQD

One of the dominant Oconee LOCAs is the transient-induced small LOCA sequence TMLQD. In this sequence there is no makeup to the steam generator secondary (ML) or to the primary system (D). One safety valve sticks open (Q) producing the equivalent of a 2.3 inch small LOCA. Containment safeguards function as designed. Figures C-1 through C-8 are plots of the MARCH calculations for this case.

The primary system pressure is plotted in Figure C-1. The pressure decreases below 1300 psia at 25 minutes and then increases to 1340 psia at 35 minutes due to the degraded steam generator heat sink. The core uncovers at 37 minutes (see Figure C-2). After 40 minutes, the primary system pressure decreases since the leakage out the open safety valve exceeds the decreasing boiloff rate. The pressure decreases to 600 psia at 76 minutes and reaches a minumum value of 512 psia just prior to core slumping at 78 minutes. After core slumping into the bottom head, the calculated pressure increases to about 3000 psia.

It was assumed in these calculations that core flood tank injection did not occur even though the calculated pressure fell below 600 psia. Figure C-3 shows the MARCH calculated blowdown rate. The MARCH modeling results in a liquid blowdown initially at a rate of about 17000 lb/min. At 17 minutes the surge line uncovers, and steam blowdown at about 3000 lb/min. follows. A MARCH calculation, in which core flood tank injection was assumed to occur at the 600 psia setpoint, indicated the core was about 70 percent melted at the time of injection (~75 minutes). Because the core flood tank injection pressure is just marginally achieved and because the BOIL core quenching models for such a large core melt fraction are of uncertain validity, the assumption of no core flood tank injection is judged to be reasonable. Assuming no core flood tank injection, complete core meltdown and head failure occur by 79 minutes.

Figure C-4 shows the core melt fraction and the fraction cladding reacted. Core melting starts at 59 minutes and is complete in about 20 minutes. About 35 percent of the cladding was reacted prior to core slumping into the bottom head.

The containment pressure is plotted in Figure C-5 and the temperature in Figure C-6. A peak containment pressure at 43 psia occurs at the time of bottom head failure (79 minutes) due to the rapid release of steam and hydrogen from the primary system. It was assumed in this MARCH calculation that the core debris did not fragment and rapidly boil the water out the reactor after head failure. Comparison with the similar TMLU case indicates the containment pressure would have peaked at 70-85 psia if fragmentation and rapid boiling had been assumed for this case. However, containment failure would not be likely at these pressures.

Flammable hydrogen mixtures first appear in the containment towards the end of core meltdown. The mixtures remain flammable for the remainder of the MARCH calculation. Figure C-7 indicates the containment pressures that would occur if all the hydrogen present in the containment rapidly burned. These calculated pressures assume no prior burn and complete, adiabatic combusion. Containment failure would be likely if burning were delayed until after head failure.

Figure C-8 shows plots of the concrete base pad penetration calculated by subroutine INTER. INTER predicts a vertical penetration rate of about 20 cm/hr for the first 10 hours. After 10 hours, the debris cools to and remains at about the liquid temperatures of the metal (~ 2450°F) and oxide (~ 2000°F) debris layers with the penetration rate being controlled by the decay heat. After 10 hours, INTER predicts the concrete decomposition continues, but the direction of the penetration becomes largely radial. The Oconee basepad is about 8.5 feet (259 cm) thick. The INTER calculations indicate the core debris will remain about 1.5 feet short of penetrating the basepad 2.5 days after meltdown. However, at the initial penetration rate, basepad meltthrough would have occurred at about 12 hours. Considering the uncertainties in the modeling of basepad meltthrough, basepad penetration about 1/2 day after core meltdown would appear to be credible in the Oconee plant.

1.2 Sequence S_3D (4.0 inch Break)

A second MARCH calculation was performed to examine the core flood tank behavior for a larger size break than that discussed above. MARCH results for a 4.0 inch LOCA with no HPI injection indicated core uncovery to about 4 ft. above the bottom of the core at 15 minutes. However, a few minutes later, the core flood tanks dumped and recovered the core. Peak core temperatures remained below 1200 F during this period. With no HPI makeup, the core flood tank water boiled off, and a second core uncovery period began at 40 minutes. The MARCH calculation was stopped at this point. However, based on the results of other MARCH calculations, core melting would have been expected to begin in an additional 20 to 30 minutes. For some large LOCA cases, core melting may begin as early as 15 minutes. After core melting starts, MARCH would predict similar results for these cases. Thus, the MARCH results for LOCAs larger than about 4.0 inches are similar, except for the timing of the start of core melting. Also, the core flood tanks will be empty prior to the start of core melting. Consequently, flood tank injection into the reactor cavity at head failure does not occur, and the containment pressure spike produced by rapid vaporization of the reactor cavity water will not be large enough to threaten the containment. If containment safeguards are available, hydrogen burning presents the major threat of early containment failure for LOCA pipe breaks greater than about 4.0 inches.

2.0 OCONEE V SEQUENCE

In the V sequence, the check valve separating the high pressure primary system from the low pressure ECC system fails. Failure of the check valve produces a failure of low pressure ECC piping in the penetration room. Failure of this piping is assumed to preclude pumped ECC injection, and a core meltdown results. The penetration room is of normal construction and is not designed to withstand blowdown pressures. Consequently, the penetration room nearly immediately after check valve failure. In this accident, the containment building is bypassed during blowdown, and there is a direct leakage path to the atmosphere for the meltdown fission product releases. After meltthrough of the bottom head of the reactor vessel, the core falls into the reactor cavity. Fission products released from the melt in the reactor cavity will be partially dispersed in the containment building prior to leaking to the atmosphere through the penetration room.

The check valve failure was assumed to produce a small LOCA (3.25 inch diameter) in the penetration room. The thermal-hydraulics of the blowdown is similar to that discussed in the section on Oconee LOCAs. The primary system pressure decreases to the core flood tank injection pressure (600 psia) at about 25 minutes. The core flood tank water is assumed to be injected to the vessel and keeps the core covered until about 62 minutes. Core melting starts at 84 minutes, and fission products begin to be released to the atmosphere through the failed Penetration Room. The core meltdown is complete by 117 minutes, and the bottom head fails at 132 minutes. The accident timing for this sequence would be sensitive to the assumed pipe break size. For a large LOCA, core melt can start as early as 15 minutes. The earlier start of core melt, however, would not have a significant effect on the fission product releases or consequences.

3.0 OCONEE SEQUENCE TMLU

Sequence TMLU is a transient in which the steam generator is lost as a heat sink due to failure to provide makeup to the steam generator secondary (ML). In addition, the primary makeup or ECC system fails (U). Containment safeguards are available. MARCH calculations for this sequence predict a core meltdown starting at about 2 hours. Complete core meltdown and failure of the bottom head are predicted to occur about one hour later. Because of the availability of containment safeguards, early containment over-pressurization failure due to excessive steam generation is unlikely. The most likely mechanism for early containment failure is over-pressurization resulting from rapid hydrogen burning occurring in coincidence with the large release of hydrogen from the primary system to the containment at the time of bottom head failure. MARCH calculations for the TMLU sequence are discussed below.

Two MARCH calculations were performed to examine the sensitivity of the timing of the initial core uncovery to the quality (water/steam content) of the leakage through the vent valves and to the shutdown power trace. In one leak scenario, the liquid leakage is mainly limited to that required to accommodate primary system liquid expansion from an initial temperature of 567^{o}F to a final temperature of 670^{o}F, corresponding to the saturation temperature at the safety valve setpoint of 2500 psia. A steam bubble is then assumed to form in the pressurizer. Steam leakage follows at a rate sufficient to accommodate decay heat boiloff. In the second scenario, the period of liquid coolant leakage is extended until the surge line connection (of the pressurizer) to the hotleg uncovers. The latter scenario is thought to be consistent with the thermal-hydraulic conditions observed in the initial stages of the Three Mile Island-2 accident where the pressurizer remained nearly water filled and most of the voiding occurred in the hotlegs and steam generators (Reference 9). MARCH does not contain models which can predict which of these leak scenarios is most likely. However, the effects on the accident timing can be examined. MARCH results are listed in Table C-1. The second leak scenario is also coupled with a higher shutdown power trace in which the drop to a decay heat power level is preceded by six full-power-seconds of operation. In the first scenario, an immediate drop to a decay heat power level is assumed.

For the higher power level, steam generator dryout is predicted to occur 5 minutes earlier. The combination of higher power level and the extension of the water leakage period until surge line uncovery results in the core uncovering 46 minutes earlier. Core meltdown and head failure are predicted to occur 55 minutes earlier. The more rapid core uncovery may have an effect on the likelihood of the reactor operators being able to respond and successfully recover from the accident. However, given that the meltdown occurs, the change in accident timing has little effect on the fission product releases or accident consequences. In the following discussion of the TMLU sequence, the accident timing is based on the slower meltdown corresponding to Case 1 in Table C-1.

Figure C-9 is a plot of the containment pressure. At the beginning of the accident, the containment pressure shows little increase until after the steam generators boil dry and the coolant boiloff rate increases at 40 minutes. Thus, the MARCH calculations indicate spray actuation is likely in the absence of operator intervention. Three building coolers were assumed to be started at 40 minutes at a containment pressure of 4 psig. Containment spray at a rate of 2000 gpm was started at a pressure of 10 psig. With the building coolers on, the spray is not initiated until 93 minutes or about 26 minutes before the start of core uncovery. With the coolers on but with no sprays the pressure would have peaked at about 15 psig at the time of core uncovery. The containment presure would then have decreased due to the reduced core boiloff rate.

At 193 minutes, the core slumps into the water in the bottom head of the reactor vessel, and at 202 minutes the bottom head fails. The containment pressure increases to 42 psia due to the large release of steam and hydrogen to the containment at this time. In the MARCH calculations, it was assumed the core slumped into the bottom head at a core melt fraction of 0.75. Thus, MARCH predicts for these assumptions, a time interval of only 9 minutes between a core melt fraction of 0.75 and head failure. The short time interval to head failure is due to the combined effects of head heating after bottom head dryout and the elevated primary system pressure. The calculated primary system pressure at the time of vessel failure was 2500 psia.

When the head fails, the molten core debris falls into the reactor cavity. The reactor cavity, in this problem, initially contained 185,400 lbs. of water at a temperature of 134°F. The source of this water was 124,800 lbs. from the accumulators, which were assumed to dump after head failure, and the remainder from overflow of water from the containment floor. The debris is assumed to fragment into 2.0 inch particles and boil the water out of the reactor cavity. It is assumed the cavity does not refill during the boiloff process due to overflow from the containment floor. The containment pressure peaks at 71 psia at 207 minutes when the 185,400 lbs. of water boils out of the reactor cavity. Another MARCH calculation indicates the pressure would have peaked at 85 psia if only the containment sprays were running. The containment pressure decreases to about 20 psia following reactor cavity dryout.

The core debris begins to attack the concrete base pad of the containment at 267 minutes. The containment pressure slowly builds up to about 31 psia after 10 hrs. of concrete attack due to the buildup of non-condensible gases. It is also assumed in this phase of the accident that water re-enters the reactor cavity and covers the top surface of the melt. Boiling of this water begins in about 2 hrs. The containment spray switches to the recirculation mode at 267 minutes. The containment sump temperature remains below 150°F due to recirculation of the water condensed by the building coolers. (The containment sump and reactor cavity are modeled as separate nodes in MARCH.)

During core meltdown, 1928 lbs. of hydrogen are produced corresponding to 100 percent reaction of the core zircaloy. MARCH predicts about half this hydrogen is released to the containment along with the steam vented from the primary when the molten core collapses into the bottom head. The remaining hydrogen is released at head failure. Additional hydrogen is produced during the concrete-attack portion of the accident. After 10 hrs. of concrete melt, the mass of hydrogen in the containment increases to 2891 lbs.

Flammable hydrogen mixtures first appear in the containment towards the end of core meltdown. For about 10 minutes during the boiloff of water from the reactor cavity, flammable mixtures do not occur because of the large concentration of steam in the containment atmosphere. After dryout of the reactor cavity at 207 min., the containment safeguards condense the steam out of the atmosphere and again bring the mixture into the flammable region. Figure C-9 shows the containment pressures which would occur from a complete, adiabatic burn of the hydrogen in the containment. Note that the hydrogen burn pressure shown in Figure C-9 for a given time assumes no prior burn. If a prior burn occurs, subsequent burns will be reduced or may not occur due to the decreased availability of hydrogen and oxygen. Other MARCH calculations indicate operation of containment safeguards would be expected to reduce the hydrogen burn pressures about 10 psi for a 3 sec. burn time. For the fission product release calculations, a MARCH calculation was performed in which containment failure was assumed at the hydrogen burn pressure peak following head failure. MARCH calculates hydrogen burn pressure in excess of 130 psia following head failure. Since the nominal containment failure pressure is taken to be about 133 psia, hydrogen burning of the type described has a significant probability of producing containment failure.

4.0 OCONEE SEQUENCE $T_1(B_3)$MLUOO'

Sequence $T_1(B_3)$MLUOO' is typified by a complete loss of electric power (equivalent to Surry TMLB'). Consequently, there is no makeup to the secondary of the steam generator. The HPI pumps are not available to provide primary makeup, and there are no containment safeguards. Since there is no secondary or primary makeup, the steam generators boil dry followed by boiloff of the primary water. Core heatup and meltdown follow. Since there are no containment safeguards, high steam pressure is produced in the containment by the primary system boiloff. A significant probability of containment overpressurization failure occurs shortly after bottom head failure due to rapid boiloff of water from the reactor cavity.

The timing of core heatup and meltdown for the $T_1(B_3)$MLUOO' sequence is similar to that for the TMLU sequence. As discussed for the TMLU sequence, the meltdown timing is sensitive to the thermal-hydraulics of the leakage out the safety relief valves. (See Table C1 for the TMLU results.) However, since the accident consequences are relatively insensitive to this timing, the $T_1(B_3)$MLUOO' calculations were performed only for the slower meltdown case. Table C-2 lists the MARCH results for the $T_1(B_3)$MLUOO' sequence. Figures C-10 and C-11 are plots of the containment pressures for the MARCH calculation. In the MARCH calculations for these plots, containment failure was assumed not to occur.

For the MARCH case illustrated in Figure C-10, the core debris was assumed to fragment and rapidly boil the water (185,200 lbs.) out of the reactor cavity following head failure. The major source of the water in the reactor cavity is the accumulators (124,800 lbs.), which are assumed to dump into the reactor cavity after head failure. The accumulators do not dump prior to head failure in the $T_1(B_3)$MLUOO' sequence because of the high primary system pressure. An additional 60,400 lbs. of water overflows into the reactor cavity from the containment floor. As seen in Table C-2 and Figure C-10, rapid vaporization of the reactor cavity water increases the containment pressure from 71 psia at the time of head failure to 113 psia. The containment pressure then slowly decreases to 74 psia at 360 minutes due to condensation of steam from the atmosphere on containment structures. The pressure begins another increase due to generation of non-condensable gases from concrete decomposition and steam from boiloff of water from the top surface of the debris in the reactor cavity. A pressure of 113 psia is again reached at 810 minutes. The nominal failure pressure of 133 psia is reached at 1730 minutes. If the core debris and water in the reactor cavity do not interact, the pressure spike of 113 psia does not occur. Containment pressures for this case are shown in Figure C-11. The nominal failure pressure is not reached until 1900 minutes.

The 113 psia containment pressure spike produced by the rapid vaporization of the water in the reactor cavity corresponds to a containment failure probability of 0.16.[1] The major portion of the consequences associated with the $T_1(B_3)$MLUOO' meltdown sequence results from this pressure spike. CORRAL calculations indicate that if containment overpressure failure can be delayed several hours after the end of core meltdown, many of the fission product particulates and halogens deposit on containment surfaces. Consequently, the atmospheric releases upon containment failure would be significantly reduced if failure is delayed until 1730 - 1900 minutes.

Except for one timestep just prior to head failure, MARCH predicts flammable hydrogen mixtures do not occur in the containment for the $T_1(B_3)$MLUOO' sequence. The predicted pressure assuming burning occurs is 99 psia, corresponding to a 0.045 probability of containment failure.[1] Generally, the mixtures are outside the flammable region due to the high steam concentrations in the atmosphere. Note that the restoration of containment safeguards would reduce the steam partial pressure and could bring with it the threat of containment failure due to hydrogen burning.

MARCH calculations performed for the TMLQD sequence were extended in time to 60 hrs. of base pad meltthrough time. Those calculations indicated that the core debris penetrated 90 percent of the base pad thickness in about one half day. Similar behavior would be expected for the $T_1(B_3)$MLUOO' sequence. After one half day, the containment pressure for the $T_1(B_3)$MLUOO' sequence would be in the 100 - 115 psia range, assuming failure did not occur during the earlier pressure spike to 113 psia due to rapid boiloff of the water in the reactor cavity. The MARCH calculations indicate there is a significant probability that base pad meltthrough will occur prior to overpressurization failure.

---

1. A normal probability distribution with σ = 20 psia assumed.

5.0 OCONFE SEQUENCE TMLOO'

The TMLOO' sequence is a transient in which both the main and auxiliary feedwater to the steam generator secondary fail. Consequently, the steam generator boils dry and is lost as a heat sink. In addition, the containment safeguards are inoperative in the TMLOO' sequence so there is not containment pressure reduction function. High pressure ECC injection is available. The Oconee HPI pumps have sufficient capacity to provide makeup when pumping against the safety valves. The operators are assumed to run the HPI pumps at full capacity (not throttled) in this sequence. For long term coolant makeup, the high pressure pumps must be aligned for recirculation from the sump through the low pressure ECC heat exchanger. The alignment to the recirculation mode must be made at about 30 hrs. with one HPI pump running.

MARCH calculations for the TMLOO' sequence indicate that because of the loss of containment safeguards, eventual over-pressurization failure of the containment occurs. At the time of containment failure, the ECC pumps are in the recirculation mode taking suction from the sump. Since the sump temperature is elevated (324°F), sump flashing, ECC pump cavitation, and pump failure are likely at the time of containment failure. With failure of the ECC, coolant boiloff and core meltdown follow.

Significant events in the TMLOO' sequence are discussed below. The transient begins with the plant at a normal operating power level of 2567 MW, a primary system pressure of 2250 psia, and an average primary system temperature of 567°F. Loss of the main and auxiliary feedwater to the steam generators results in an increase in primary system pressure. The MARCH calculations assume the system pressure increases to the 2500 psia setpoint of the safety relief valves. The pressure remains constant at 2500 psia for the duration of the transient as HPI water is fed into the primary, and the safety valves open and close venting excess primary inventory. In the calculations, the HPI pumps were assumed to have been started at 10 minutes. An alternative procedure to venting through the safety valves would be to vent through the pilot operated relief valve (PORV). The setpoint of the PORV has sufficient capacity to vent the excess primary inventory with full HPI injection. Thus, a somewhat lower system pressure could be maintained by venting through the PORV. However, the course of the accident would not be significantly different from that analyzed in the MARCH calculations. Prior to containment failure, heat removal from the primary system is accomplished by the flow of HPI water into the cold leg, down the annulus, up through the core, and out the relief valve. Except for the 3 - 9 hour period of the accident, the mixed-mean coolant exit temperature is subcooled, and boiling in the primary is suppressed. The temperature of the coolant venting out the safeties decreases from 670°F at 10 hours to 520° F at 70 hours. Part of the coolant flashes to steam in the containment and the remainder falls into the sump. Figure C-12 shows the containment pressure. Containment failure (at 133 psia) occurs at 70.4 hours. The containment sump remains about 20°F subcooled prior to containment failure due to the contribution of the air partial pressure to the total pressure. Thus, it is assumed the ECC pumps will not have cavitation problems in the recirculation mode even though the sump temperature increases to 325°F at 70 hours. ECC pump cavitation and failure are assumed when the containment fails at 70.4 hrs. Coolant boiloff follows, and the top of the core uncovers at 77.7 hours. Core melting begins at 78.8 hours, and meltdown is complete by 81.4 hours. The head fails at 81.5 hours. When the head fails, the accumulator dumps 125,000 lbs. of water into the reactor cavity. It is assumed in the MARCH calculations that the debris fragments in the reactor cavity and vaporizes all the water in the reactor cavity before starting melting of the concrete base pad.

As illustrated in Figure C-12, the containment pressurization is very slow, taking nearly three days to reach the assumed failure pressure of 133 psia. The results in Figure C-12 are for operation of one HPI pump (at an injection rate of about 1400 lb/min). Operation of two HPI pumps would further increase the time to containment failure. Because of the slow pressurization, there is a significant probability that the operators would attempt corrective action. Restoration of steam generator auxiliary feedwater or main feedwater prior to containment failure would lead to a successful recovery from the transient. Some operator actions could lead to earlier core meltdown. For example, containment venting would result in loss of the air partial pressure in the containment, initiate sump flashing, and cause ECC (recirculation mode) pump cavitation and failure. Thus, containment venting could lead to earlier meltdown.

6.0 MINIMUM CONTAINMENT SAFEGUARDS

A series of MARCH calculations were performed to determine the minimum containment safeguards required to prevent long term containment overpressurization. It was assumed in these calculations that the ECC works and keeps the core covered. In these cases, there is no question of core meltdown unless containment failure indirectly leads to failure of the ECC system.

Calculations were performed for an assumed large LOCA in which containment heat removal was provided by either (1) one building cooler or (2) the combination of one containment spray and one ECC heat exchanger. In these large LOCA calculations, the MARCH modeling assumes that the ECC provides only sufficient water to the reactor vessel to compensate for coolant boiloff. The boiloff rate is on the order of 1000 lb/min. The low head ECC pumps inject 24,000 lb/min. The excess of the pump capacity over the boiloff rate is assumed in the MARCH modeling to be dumped on the containment floor where it flows to the building sump.

The MARCH calculations for the two large LOCA cases above indicate sufficient long term containment cooling. For the first case, in which one building cooler and the ECC work but the containment spray and ECC heat exchanger do not work, MARCH predicts that containment pressures have decreased to about 24 psia at 1800 minutes. For the second case, in which the coolers do not work but one spray and the ECC heat exchanger work, containment pressure after blowdown peak at 48 psia at 300 minutes and decrease to 37 psia by 1800 minutes.

For a small LOCA, the situation is somewhat different for the case in which containment heat removal is provided by the ECC flowing through the ECC heat exchanger. The MARCH modeling for small LOCA ECC injection assumes perfect mixing (or thermodynamic equilibrium) with the water in the reactor vessel. MARCH predicts the ECC injection is sufficient to suppress boiling in the vessel at 325 psia after 300 minutes. However, because of the reduced flow rate of the HPI pumps in comparison with the low head pumps, the decay removal by ECC heat exchanger is reduced. Consequently, coolant temperatures remain high and the coolant leaking from the primary system flashes in the containment. The containment pressure slowly builds up to 42 psia between 20 and 26 hours before beginning a down trend. The MARCH calculations thus also indicate adequate long term cooling for the small LOCA cases.

7.0 FAILURE OF REACTOR PROTECTION SYSTEM

The Oconee event trees contain a number of sequences with high probabilities in which the reactor protection system fails. When the reactor protection system fails, the reactor power naturally decreases to a lower power level determined by core physics and heat transfer parameters. In many of these cases, the main feedwater to the steam generator is lost. Consequently, moderator water temperatures increase, and may be accompanied by boiloff of the coolant. The increase in water temperature and the boiling produce negative temperature coefficients which tend to decrease the core power level. The decrease in core power level from full power is accompanied by a decrease in fuel rod temperatures. The decrease in fuel temperatures contributes a positive Doppler component to the reactivity and balances the negative moderator components.

Calculations performed by Babcock and Wilcox[1] for Oconee-type plants indicate that generally the negative temperature coefficient is sufficient without coolant boiling to balance the positive Doppler effect. Thus, for these cases, no coolant boiloff or core uncovery occurs. Hand calculations performed by Battelle based on the B&W results indicate an additional negative component of reactivity may be required from coolant boiling for a small part of the initial fuel cycle. This occurs because the Doppler effect depends on the number of days at power and the fuel cycle. If coolant boiloff does occur, core uncovery and meltdown may follow. More definitive calculations are being performed by other groups.

Based on the present analyses, failure to scram sequences will not generally be core melt cases. However, more definitive calculations may alter this conclusion.

---

[1] "Analysis of B&W NSS Response to ATWS Events," BAW-1610, January, 1980.

Table C-1. MARCH Results for TMLU Sequence

	Time, min Case 1	Time, min Case 2
Steam Generator Dry	27	22
Core Uncovers	119	73
Start Melt	140	92
End of Meltdown	196	141
Head Failure	202	147

Table C-2. MARCH Results for Sequence $T_1(B_3)$MLUOO'

	Time, Min.	Containment Pressure, psia
Steam generator dry	27	15.9
Core uncovers	120	41.5
Start melt	142	42.4
End of meltdown	195	46.9
Head failure	201	71.5
End reactor cavity boiloff	205.6	112.9

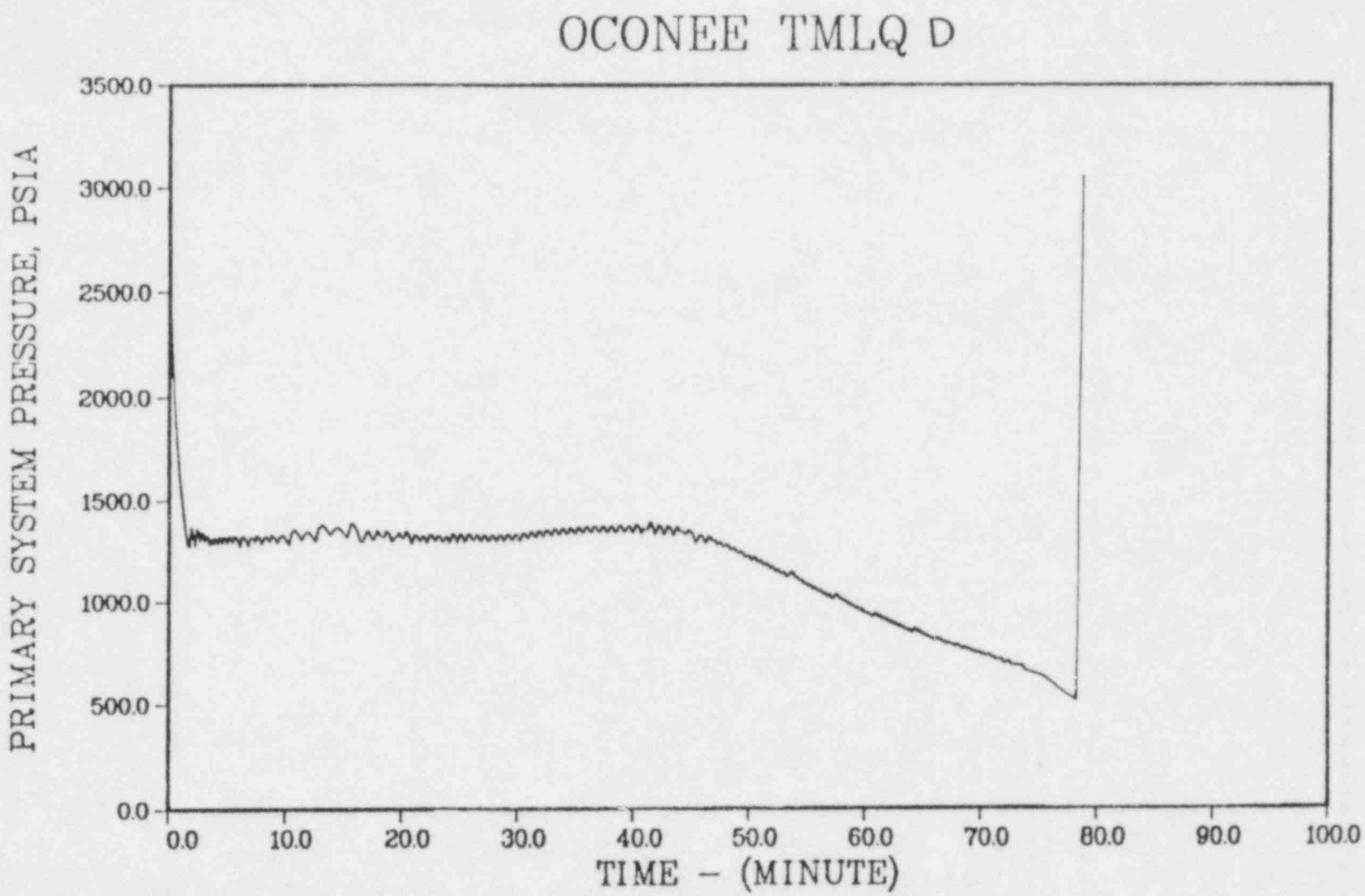


Figure C-1. Primary System Pressure Versus Time - TMLQD Sequence

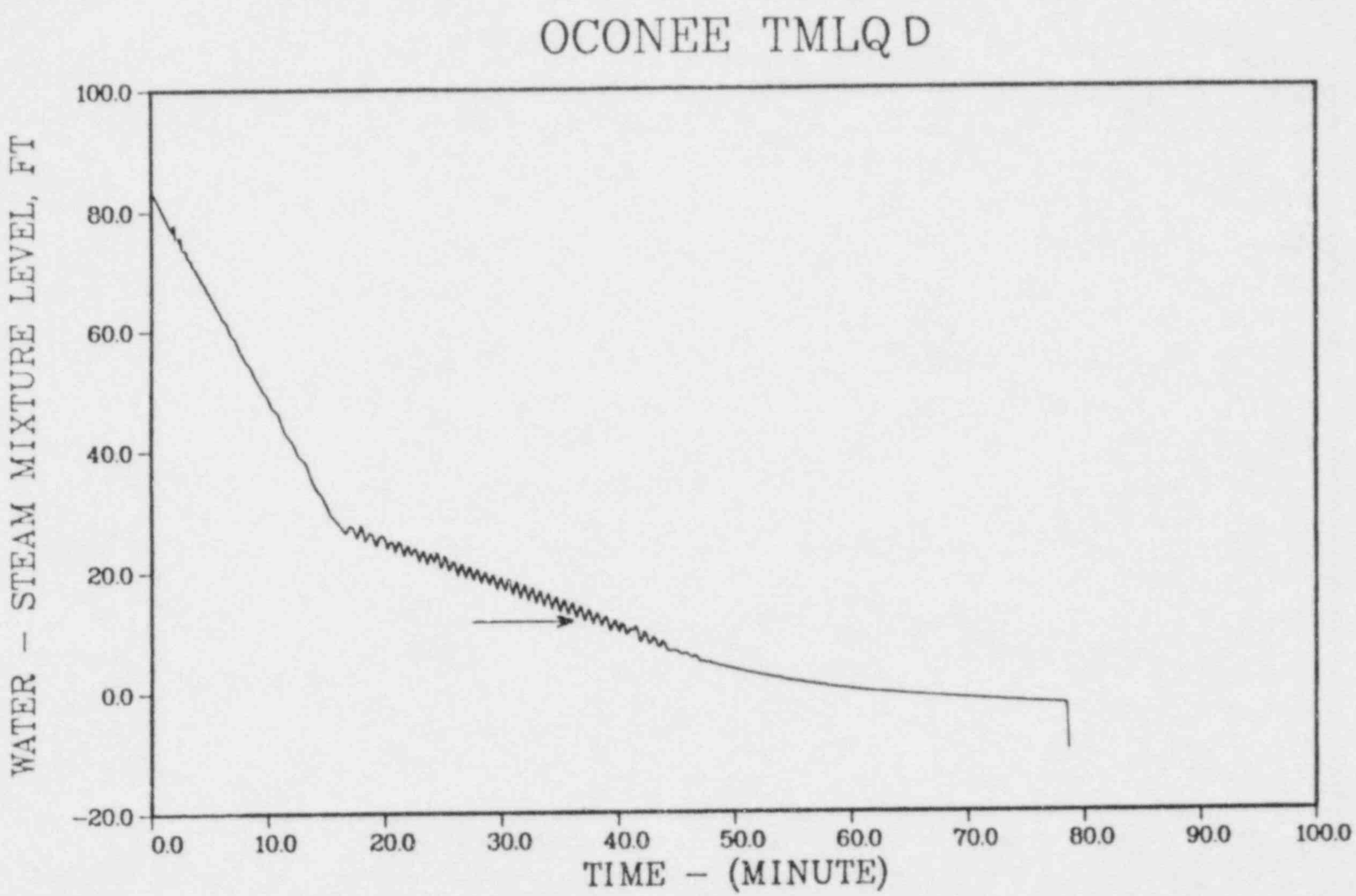


Figure C-2. Water-Steam Mixture Level Versus Time - TMLQD Sequence

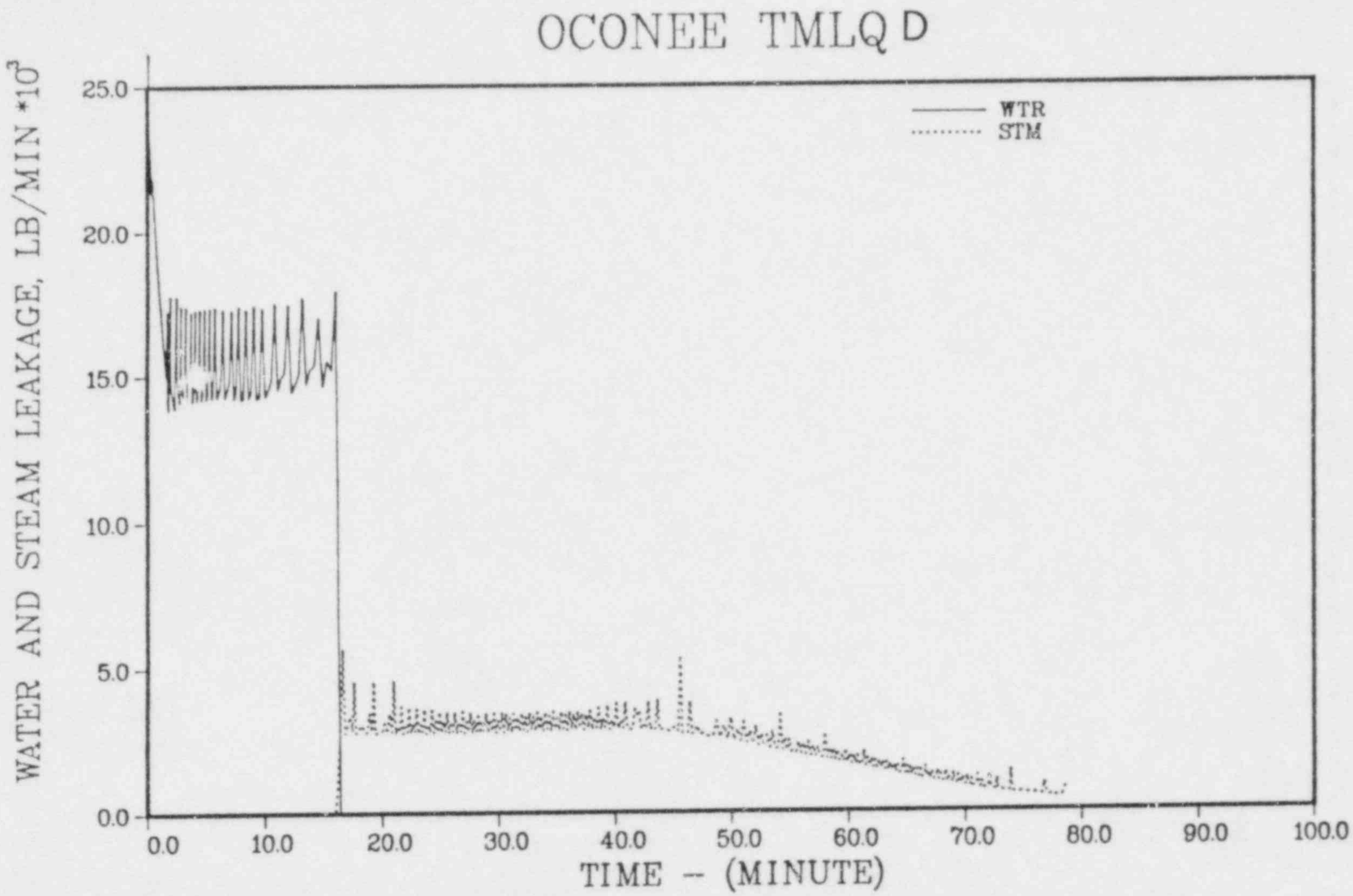


Figure C-3. Water and Steam Leakage Versus Time - TMLQD Sequence

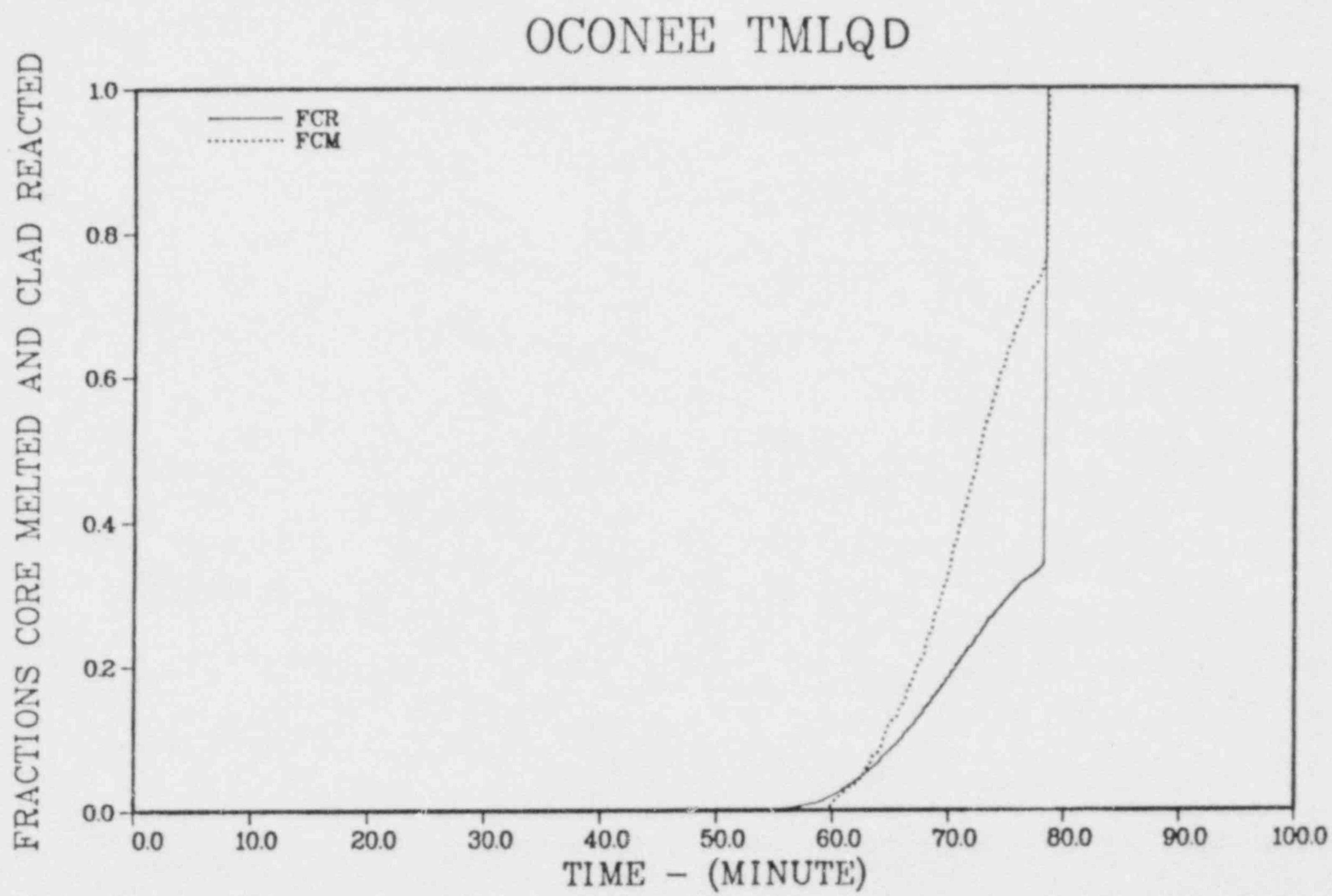


Figure C-4. Fractions Core Melted and Clad Reacted Versus Time - TMLQD Sequence

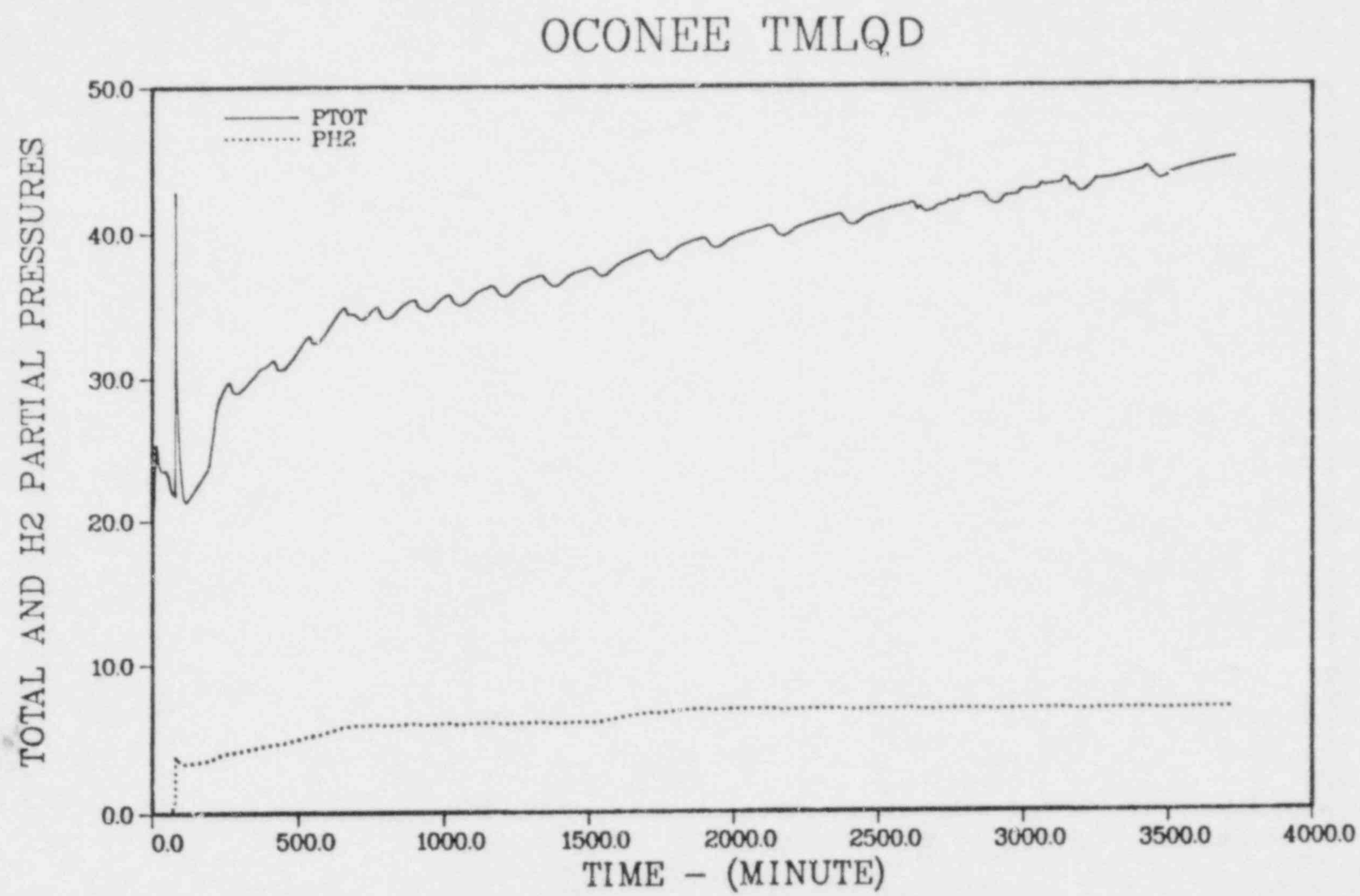


Figure C-5. Total and Partial H_2 Pressures Versus Time - TMLQD Sequence

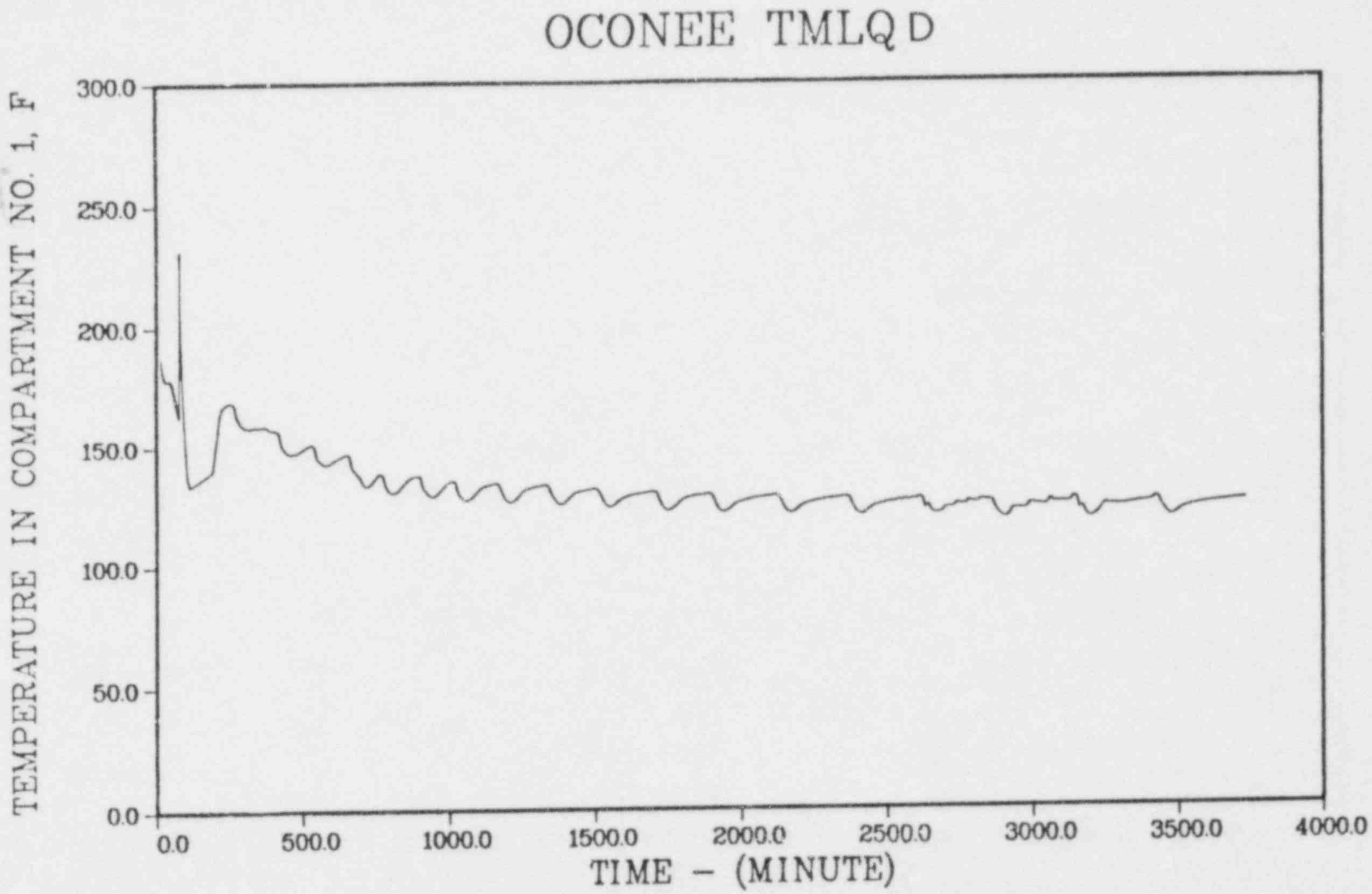


Figure C-6. Temperature in Compartment No. 1 Versus Time - TMLQD Sequence

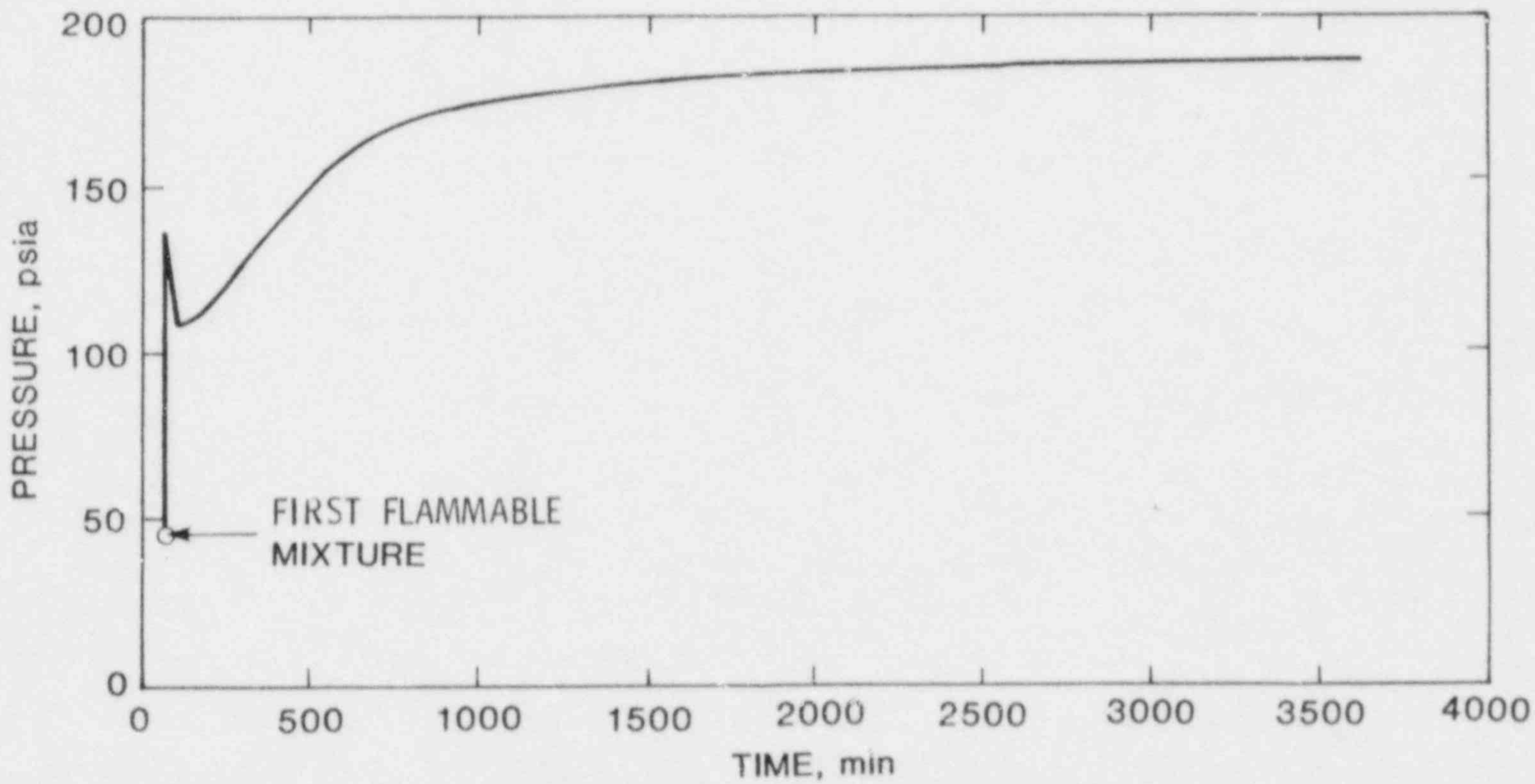


Figure C-7. Containment Pressure from Complete Adiabatic Burn of Hydrogen, Assuming no Prior Burn

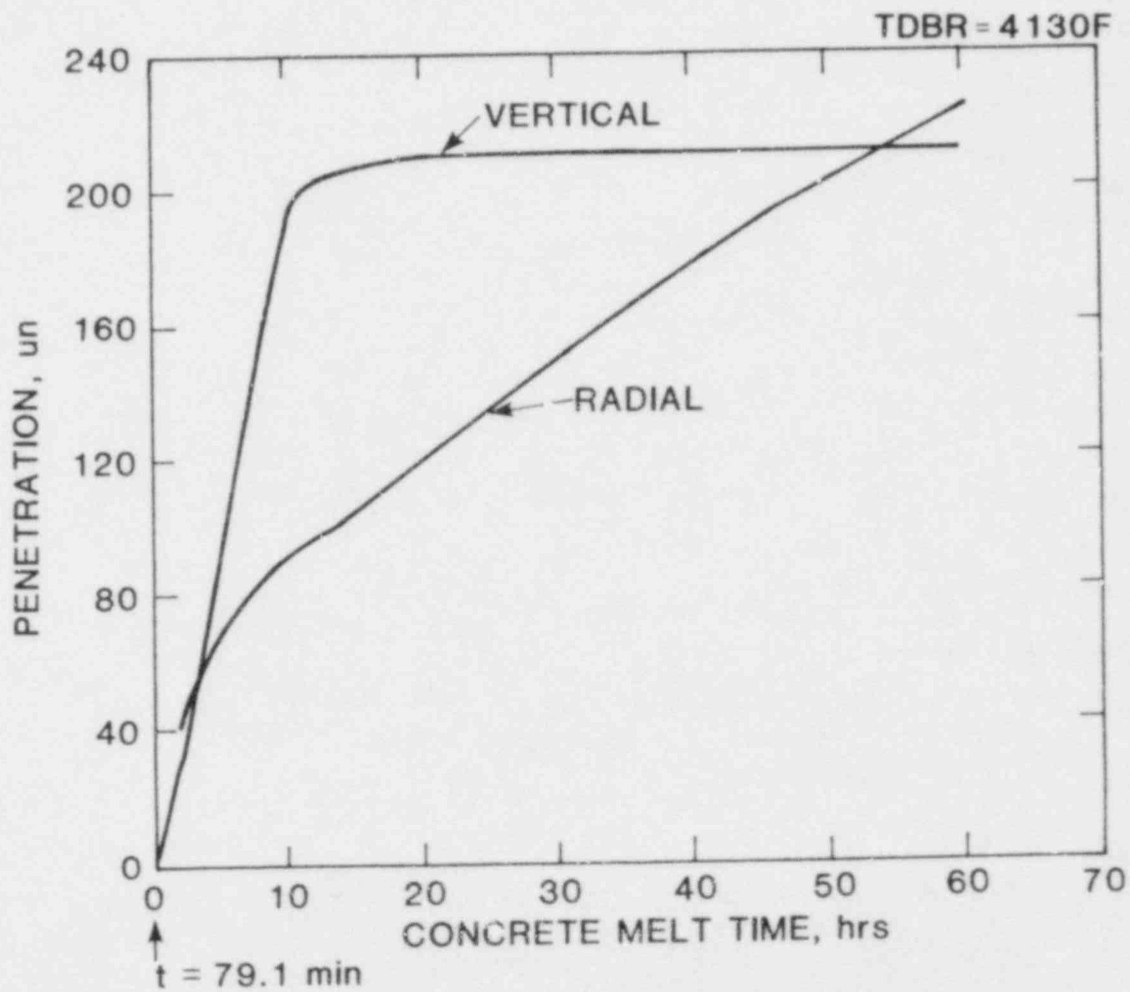


Figure C-8. Concrete Base Pad Penetration Versus Core Melt Time - TMLQD Sequence

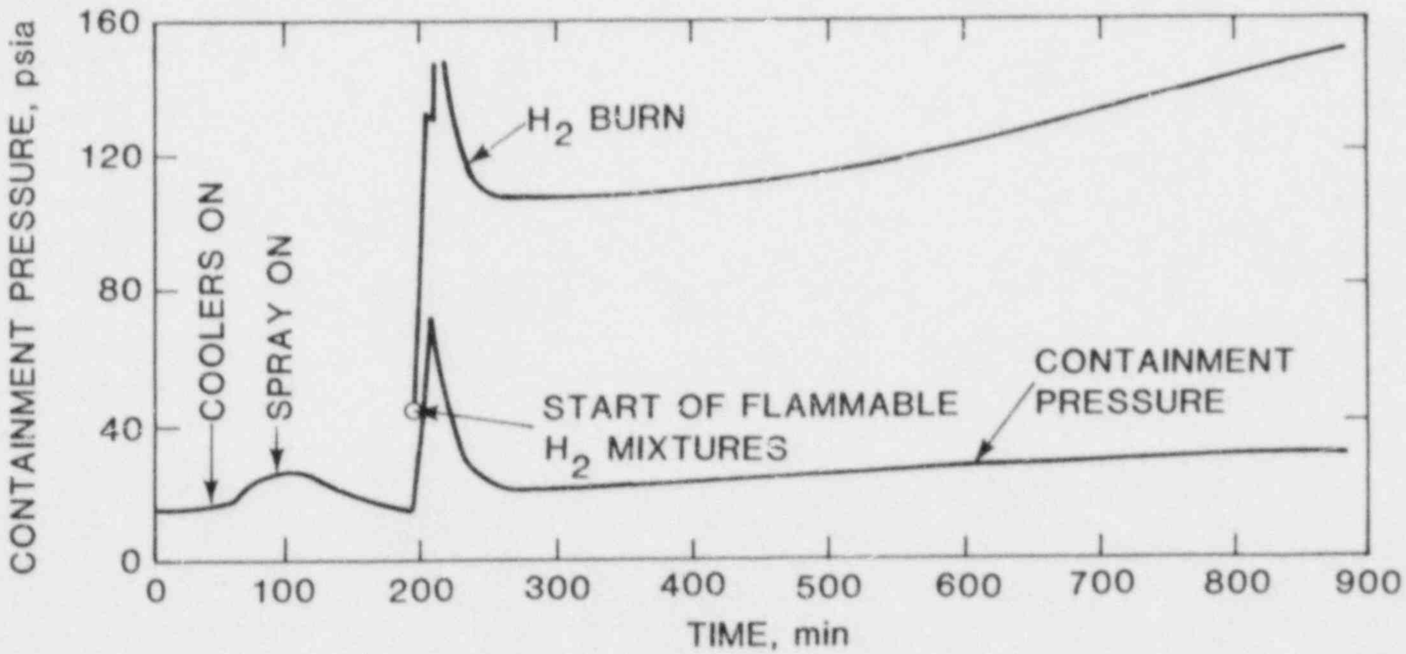


Figure C-9. Comparison of Containment Pressure with and without Complete, Adiabatic Hydrogen Burn. Case TMLU.

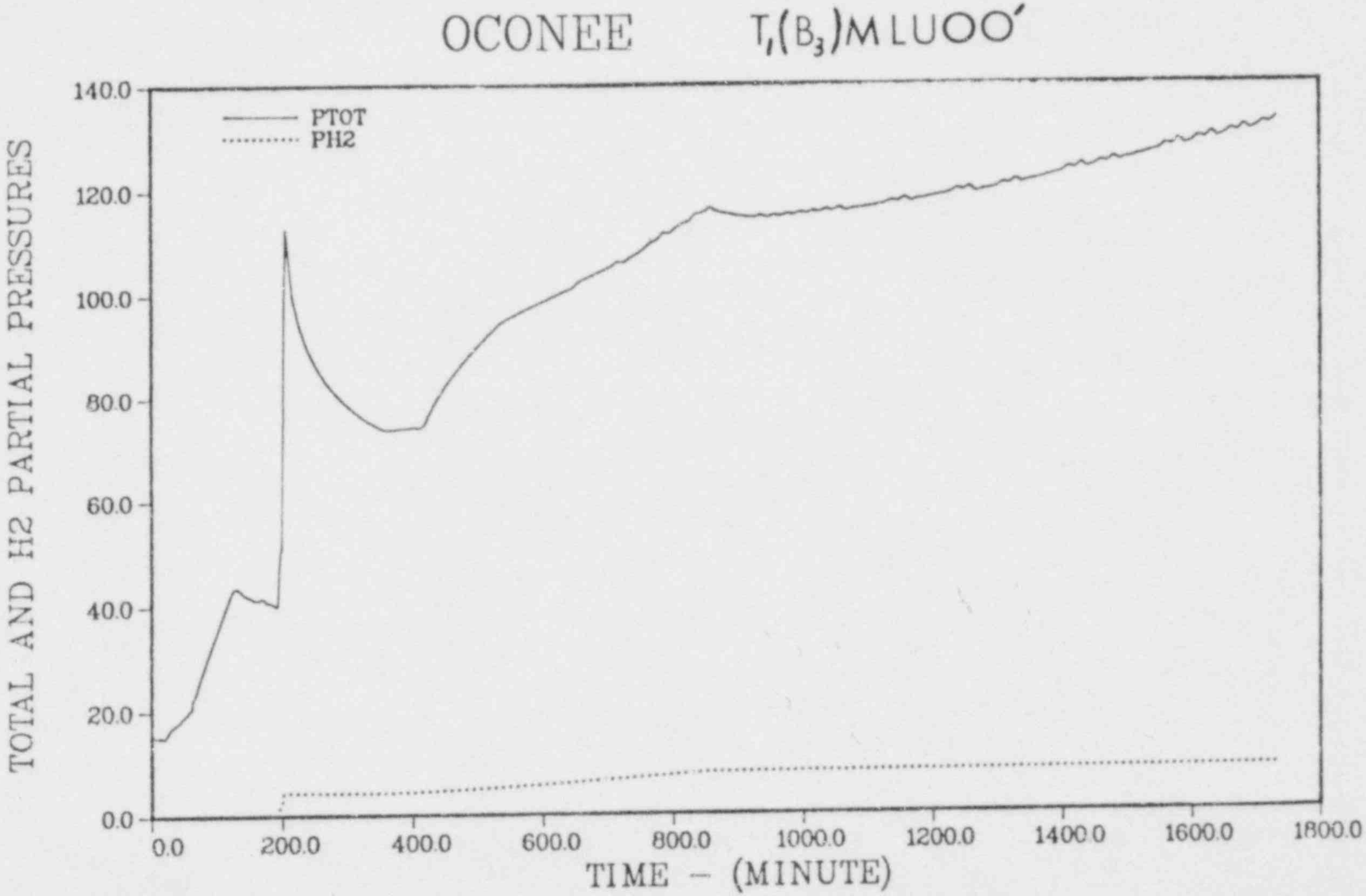


Figure [illegible]-10. Total and Partial H_2 Pressure Versus Time – $T_1(B_3)MLUOO'$ (Debris and Water React)

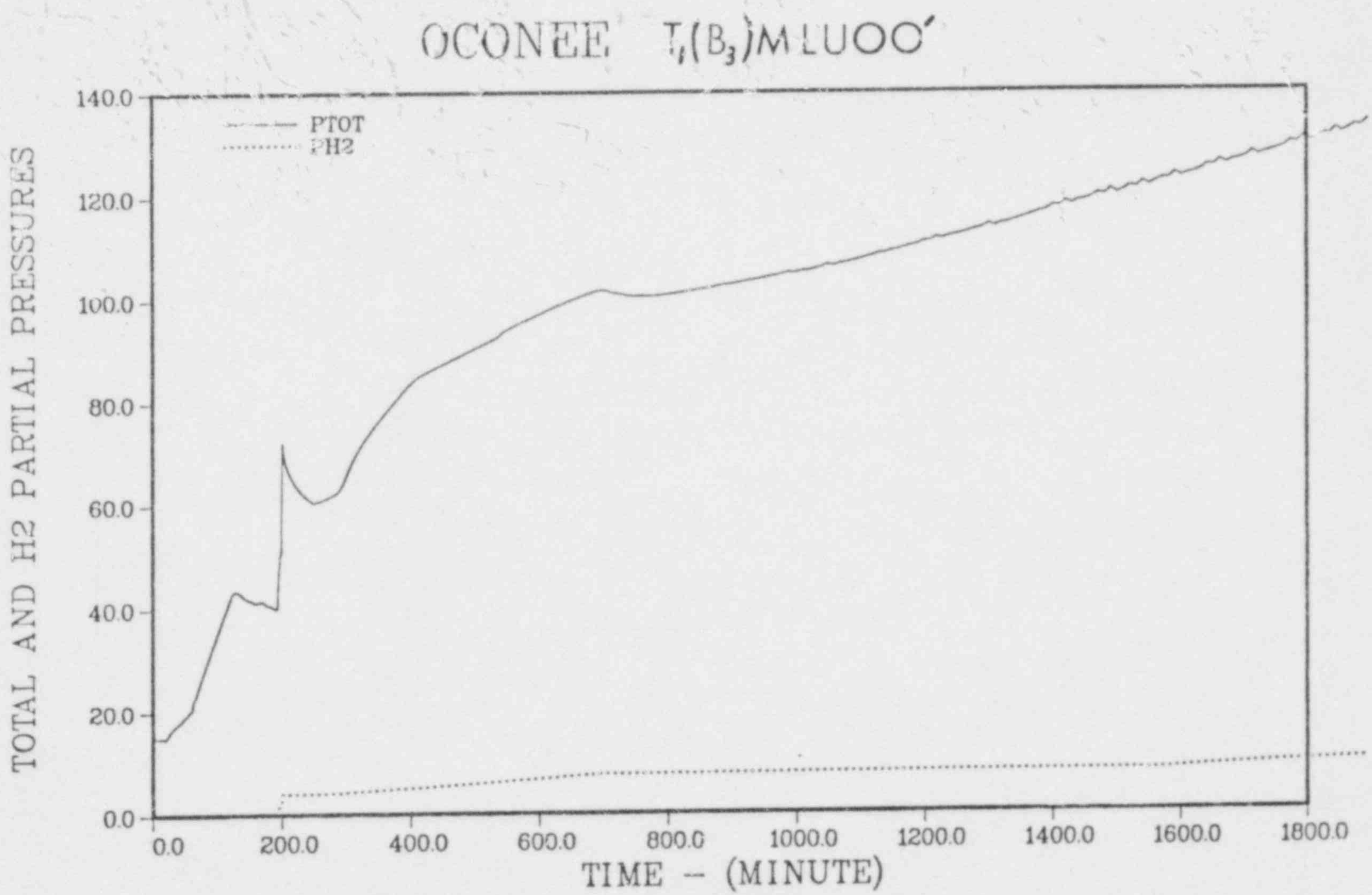


Figure C-11. Total and Partial H_2 Pressures Versus Time - $T_1(B_3)$MLUOO' (Debris and Water Do Not React)

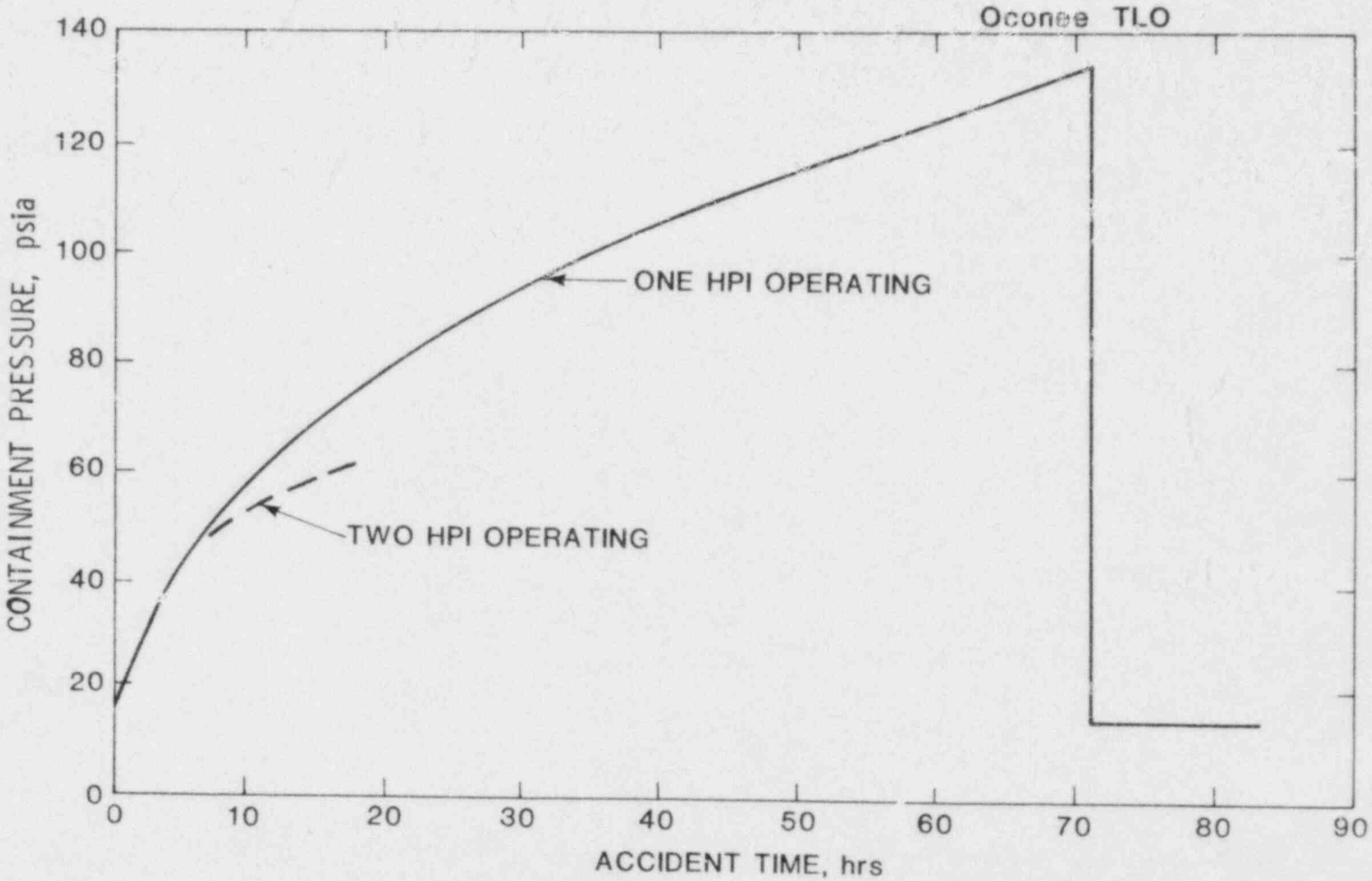


Figure C-12. Containment Pressure for Oconee TMLOO' Accident

APPENDIX D

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AFWS	Auxiliary Feedwater System
BWR	Boiling Water Reactor
BWST	Borated Water Storage Tank
CFS	Core Flooding System
CHRS	Containment Heat Removal System
CL	Containment Leakage
CLAS	Cold Leg Injection Accumulator System
CSIS	Containment Spray Injection System
CSRS	Containment Spray Recirculation System
CST	Condensate Storage Tank
DCPS	DC Power System
ECIS	Emergency Coolant Injection System
ECRS	Emergency Coolant Recirculation System
EFWS	Emergency Feedwater System
EPS	Emergency Power System
ESF	Engineered Safety Features
ESPS	Engineered Safeguards Protective System
FSAR	Final Safety Analysis Report
HHASWS	High Head Auxiliary Service Water System
HPIS	High Pressure Injection System
HPRS	High Pressure Recirculation System
LOCA	Loss of Coolant Accident
LOP	Loss of Offsite Power
LPIS	Low Pressure Injection System

LPRS	Low Pressure Recirculation System
LPSWS	Low Pressure Service Water System
LWR	Light Water Reactor
PAHR	Post Accident Heat Removal
PARR	Post Accident Radioactivity Removal
PCS	Power Conversion System
PWR	Pressurized Water Reactor
RBCS	Reactor Building Cooling System
RCS	Reactor Coolant System
RPS	Reactor Protection System
RSS	Reactor Safety Study
RSSMAP	Reactor Safety Study Methodology Applications Program
S/RV	Safety Relief Valves
T	Transient
VCT	Volume Control Tank

DISTRIBUTION:

U.S. NRC Distribution Contractor (CDSI) (130 copies for AN)
7300 Pearl Street
Bethesda, MD 20014

T. C. McCreless, Chief (2)
Project Review Branch #2
Advisory Committee on Reactor Safeguards
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Atomic Safety and Licensing Board Panel (2)
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Attn: J. R. Yore, Chairman
Technical Advisor

A. S. Rosenthal, Chairman
Atomic Safety and Licensing Appeal Panel
U. S. Nuclear Regulatory Commission
Washington, DC 20555

L. V. Gossick
Executive Director for Operations
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Office of Standards Development (3)
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Attn: R. B. Minogue, Director
G. A. Arlotto, Dir., Div. Engineering Standards
E. E. Held, Chief, Site Designation Standards Branch

Director
Office of the Analysis and
Evaluation of Operational Data
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Office of Nuclear Reactor Regulation (8)
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Attn: H. R. Denton, Director
R. H. Vollmer, Dir., Div. of Engineering
D. F. Ross, Dir., Div. Systems Integration
S. S. Hanauer, Dir., Div. Human Factors Safety
R. J. Mattson, Dir., Div. Safety Technology
R. P. Denise, Assist. Dir., Licensing Management
G. W. Knighton, Chief, Research & Standards Coord. Branch (2)

Distribution (cont'd):

W. J. Besaw, Director (10)
Division of Technical Information & Document Control
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Office of Nuclear Regulatory Research (30)
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Attn: R. J. Budnitz, Director
T. E. Murley, Dir., Div. Reactor Safety Research
C. Kelber, Assist. Dir., Advanced Reactor Safety Research
L. S. Tong, Assist. Dir., Water Reactor Safety Research
L. Shao, Assist. Dir., General Reactor Safety Research
F. Arsenault, Dir., Div. Safeguards, Fuel Cycle & Environmental Research
R. Bernero, Dir., Div. Systems & Reliability Research (25)

Office of Inspection & Enforcement (2)
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Attn: J. G. Davis, Director
N. C. Moseley, Dir., Div. Reactor Operations Inspection

B. H. Grier, Director
U. S. Nuclear Regulatory Commission, Region I
Office of Inspection & Enforcement
631 Park Avenue
King of Prussia, PA 19406

J. P. O'Reilly, Director
U. S. Nuclear Regulatory Commission, Region II
Office of Inspection & Enforcement
101 Marietta Street, Suite 3100
Atlanta, GA 30303

J. G. Keppler, Director
U. S. Nuclear Regulatory Commission, Region III
Office of Inspection & Enforcement
799 Roosevelt Road
Glan Ellyn, IL 60137

K. V. Seyfrit, Director
U. S. Nuclear Regulatory Commission, Region IV
Office of Inspection & Enforcement
611 Ryan Plaza Drive, Suite 1000
Arlington, TX 76012

R. H. Engelken, Director
U. S. Nuclear Regulatory Commission, Region V
Office of Inspection & Enforcement
1990 N. California Boulevard, Suite 202
Walnut Creek, CA 94596

Distribution (cont'd):

W. Wagner, Deputy Assistant Director
Naval Reactors Division
U. S. Department of Energy
Washington, DC 20545

R. Brodsky, Assistant Director (2)
Reactor Safety & Computation
Naval Reactors Division
U. S. Department of Energy
Washington, DC 20545

J. Crawford, Director
Reactor Research & Technology Division
U. S. Department of Energy
Washington, DC 20545

Chief
Safety Assessment Branch
Office of Reactor Research & Technology
U. S. Department of Energy
Washington, DC 20545

Deputy Assistant Administrator
for Radiation Programs (4)
U. S. Environmental Protection Agency
401 M Street, S.W.
Washington, DC 20460

U. S. Library of Congress
Federal Documents Section
10 First Street, S.E.
Washington, DC 20540

Library
National Bureau of Standards
Washington, DC 20234

Advanced Research & Applications Corporation
1223 E. Argues Avenue
Sunnyvale, CA 94086

Aerospace Corporation
P. O. Box 92957
Los Angeles, CA 90009

Assistant Vice President
American Electric Power Service Corporation
2 Broadway
New York, NY 10004

Distribution (cont'd):

Babcock & Wilcox Company
Product Development Division
P. O. Box 1260
Lynchburg, VA 24505

Battelle-Columbus Laboratories
505 King Avenue
Columbus, OH 42301

Library
Battelle Memorial Institute, Columbus Ohio
505 King Avenue
Columbus, OH 42301

Chief Librarian
Bechtel Power Corporation
P. O. Box 3965
San Francisco, CA 94119

Chief Nuclear Engineer
Bechtel Power Corporation
Shady Grove Road
Gaithersburg, MD 20760

Bell Laboratories
600 Mountain Avenue
Murry Hill, NJ 07974

Center for Environmental Studies
Princeton University
Princeton, NJ 08540

Henry Piper
CRBRP Project Office
P. O. Box U
Oak Ridge, Tennessee 37830

William Parker, Jr., Vice President (4)
Duke Power Company
Steam Production, Power Building
422 South Church Street
Charlotte, NC 28242

Engineering Technical Library
Duke Power Company
P. O. Box 2178
Charlotte, NC 28242

Director
E. I. DuPont de Nemours and Company
Savannah River Laboratory
Aiken, SC 29801

Distribution (cont'd):

Vice President Nuclear
Ebasco Services, Inc.
2 Reactor Street
New York, NY 10006

President
EG&G Idaho, Inc.
P. O. Box 1625
Idaho Falls, ID 83401

Nuclear Division Director
Nuclear Safety & Analysis
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94304

Larry Conradi
Energy, Inc., Suite 220
515 W. Harrison
Kent, WA 98301

General Electric Company
P. O. Box 81608
San Diego, CA 92102

Manager of Power Plant Reliability
Utilities Division
Gilbert Associates, Inc.
525 Lancaster Avenue
Reading, PA 19603

IBM
Thomas J. Watson Research Center
P. O. Box 218
Yorktown Heights, NY 10548

President
Intermountain Technologies
P. O. Box 1604
Idaho Falls, ID 83401

N. C. Rasmussen
Dept. of Nuclear Engineering
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

MPR Associates,
1140 Connecticut Avenue, N.W.
Washington, DC 20036

Distribution (cont'd):

Northeast Utilities
174 Brush Hill Avenue
W. Springfield, MA 01089

President, Nuclear & Systems Sciences
Holmes & Narver, Inc.
999 Town & Country Road
Orange, CA 92668

Director
Nuclear Safety Analysis Center
P. O. Box 10412
Palo Alto, CA 94303

Nuclear Services Corpcration
1700 Dell Avenue
Campbell, CA 95008

NUS Corporation
#4 Research Place
Rockville, MD 20850

Pacific Gas & Electric Company
Beale Street
San Francisco, CA 94105

Pickard, Lowe and Associates, Inc.
Suite 612
1200 18th Street, N.W.
Washington, DC 20036

Department of Mechanical Engineering
Rensselaer Polytechnic Institute
Troy, NY 12181

Science Applications
Suite 200
5 Palo Alto Square
Palo Alto, CA 94304

Vice President
Southern California Edison Company
P. O. Box 800
2244 Walnut Grove Avenue
Rosemead, CA 91770

Director
Southwest Research Institute
P. O. Drawer 28510
San Antonio, TX 78284

Distribution (cont'd):

Stanford Linear Accelerator Center
Stanford University
P. O. Box 4349
Stanford, CA 94305

Technology Energy Corporation
10770 Dutchtown Road
Knoxville, TN 37922

Westinghouse Electric Corporation (2)
P. O. Box 355
Pittsburg, PA 15230
Attn: Manager, Nuclear Safety
Library, Nuclear Energy Systems

Stone & Webster Engineering Corp.
P. O. Box 2325
Boston, MA 02107

Chief
Power Research & Development
Tennessee Valley Authority
Chattanooga, TN 37401

United Engineers & Constructors, Inc.
Advanced Power Engineering
1401 Arch Street
Philadelphia, PA 19102

Department of Statistics
University of Missouri
Columbia, MO 65211

Argonne National Laboratory (4)
9700 S. Cass Avenue
Argonne, IL 60439
Attn: Technical Library
Report Section 203-CR 125
Director, Engineering Research Division
Director, Reactor Analysis & Safety Division

Library
Battelle Pacific Northwest Laboratory
P. O. Box 999
Richland, WA 99352

Brookhaven National Laboratory (2)
Upton, NY 11973
Attn: Dept. Applied Science, Bldg. 197
Associated Chairman for Reactor Safety

Distribution (cont'd):

Technical Library
Idaho Nuclear Engineering Laboratory
550 Second Street
Idaho Falls, ID 83401

Lawrence Livermore Laboratory
P. O. Box 818
Livermore, CA 94550

Frank Gillman
Nuclear Safety, L-140
Lawrence Livermore Laboratory
P. O. Box 818
Livermore, CA 94550

Los Alamos Scientific Laboratory (2)
Los Alamos, NM 87544
Attn: Q-6 Division
A-Division

Oak Ridge National Laboratory (3)
Oak Ridge, TN 37830
Attn: Library
Director, Reactor Division
Library Records, Bldg. 4500 N., Rm. H205, P. O. Box X

Sandia National Laboratories (3)
Albuquerque, NM 87185
Attn: Technical Library
A. W. Snyder, Director, Nuclear Fuel Cycle Prog. (2)

Battelle Columbus Laboratories (2)
505 King Avenue
Columbus, OH 52301
Attn: Roger Wooten
Pete Cybuskis

Stuart V. Asselin
Technology for Energy Corporation
10770 Dutchtown Road
Knoxville, TN 37922

Evaluation Associates, Inc.
GSB Building
1 Belmont Avenue
Bala Cynwyd, PA 19004

U. S. Nuclear Regulatory Commission (200 copies for Licensee Dist.)
Division of Document Control
Distribution Services Branch
Washington, DC 20555
Attn: P. Larkins

Distribution (cont'd):

4400	A. W. Snyder
4410	D. J. McCloskey
4412	J. W. Hickman (25)
4412	D. D. Carlson
4412	W. R. Cramond
4412	F. Harper
4412	S. W. Hatch (4)
4412	A. Kolaczkowski
4412	G. J. Kolb (4)
4412	B. J. Roscoe
4412	R. G. Spulak
4413	N. R. Ortiz
4414	G. B. Varnado
4416	L. D. Chapman
4420	J. V. Walker
4440	G. R. Otey
4450	J. A. Reuscher
8214	M. A. Pound
3141	L. J. Erickson (5)
3151	W. L. Garner (3)
3154-3	C. H. Dalin (25)
	For: NRC Distribution to NTIS