NUREG/CR-2787
SAND82-0978
AN, RG, XA, 1S
Printed June 1982

Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant
Vol 1 of 2

Gregory J. Kolb, Principal Investigator

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

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-2787
SAND82-0978
AN, RG, XA, 1S
Vol. 1 of 2

INTERIM RELIABILITY EVALUATION PROGRAM:

ANALYSIS OF THE ARKANSAS NUCLEAR ONE - UNIT 1 NUCLEAR POWER PLANT

Gregory J. Kolb
Sandia National Laboratories

David M. Kunsman
Science Applications, Inc.

Barbara J. Bell
Norman L. Brisbin
David D. Carlson
Steven W. Hatch
Dwight P. Miller
Benjamin J. Roscoe
Desmond W. Stack
Richard B. Worrell
Sandia National Laboratories

Jack Robertson
Arkansas Power and Light Company

Roger O. Wooton
Battelle Columbus Laboratories

Sidney H. McAhren
Remote Sensing, Inc.

Walter L. Ferrell
William J. Galyean
Science Applications, Inc.

Joseph A. Murphy
US Nuclear Regulatory Commission

June 1982

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

Prepared for
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
Washington, DC 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1241

ACKNOWLEDGMENT

The efforts of the quality assurance review team which periodically reviewed the conduct of the work and provided technical guidance are acknowledged. This team consisted of:

David D. Carlson, Sandia National Laboratories
Jack W. Hickman, Sandia National Laboratories
Joseph A. Murphy, U.S. Nuclear Regulatory Commission
Jonathan Young, Energy, Inc.

The authors also would like to thank Emily Preston, June Cristy, Ruby Cochrell, and Capri Corlis for their assistance in typing and assembling this report.

CONTENTS

CONTENTS (Cont'd)

EXECUTIVE SUMMARY

This report represents the results of the analysis of Arkansas Nuclear One (ANO) Unit 1 nuclear power plant which was performed as part of the Interim Reliability Evaluation Program (IREP). The IREP has several objectives, two of which are achieved by the analysis presented in this report. These objectives are (1) the identification, in a preliminary way, of those accident sequences which are expected to dominate the public health and safety risks, and (2) the development of state-of-the-art plant system models which can be used as a foundation for subsequent, more intensive applications of probabilistic risk assessment.

The primary methodological tools used in the analysis were event trees and fault trees. These tools were used to study core melt accidents initiated by loss of coolant accidents (LOCAs) of six different break size ranges and eight different types of transients. The emphasis of the study was on the estimation of core melt accident sequence frequencies. Core melt accidents with the highest frequency were analyzed in terms of containment phenomenology, and associated radioactive material release categories were estimated.

The most significant sequences contributing to both the core melt frequency and the risk were of four types: (1) small loss of coolant accidents (LOCAs) initiated by reactor coolant pump seal ruptures or reactor coolant system pipe breaks with failure of emergency core cooling during the injection or recirculation phase;

(2) transients caused by AC and DC power failures which involve loss of all feedwater, high pressure injection and, in some cases, loss of containment systems; (3) transient induced LOCAs (i.e., LOCAs involving stuck-open pressurizer safety valves) with failure of emergency core cooling; and (4) anticipated transients without scram sequences.

Insights were developed concerning the importance of plant design features. For instance, several single failure mechanisms were identified in systems called upon to mitigate accidents. Some of these, however, were found to be recoverable by judicious operator action. Support systems, e.g., AC/DC power and service water, were modeled in detail and were found to be important to risk. Recent improvements in the emergency feedwater system and upgrades of other plant equipment were evaluated. The analysis led to identification of key components/events which contribute most to the core melt frequency.

Similar insights were developed into plant operations. Operator errors during the course of the accident were a small contribution to core melt frequency. However, operator recovery actions were important in reducing the core melt frequency. Test and maintenance contributions to safety system unavailabilities were small. Several changes were made to the ANO-1 procedures as a result of this study.

The estimated core melt frequency for ANO-1 is similar to values predicted by probabilistic risk assessments of other light water reactor plants.

SUMMARY

This section summarizes the ANO-1 dominant accident sequences, engineering insights gained via the analysis, and changes to the design and operation of the plant as the result of this study. These topics are briefly discussed below. A more detailed discussion can be found in Chapter 8.

ANO-1 Dominant Accident Sequences

Accident sequences are combinations of system failures following an initiating event such as LOCA, succeeded by some mode of containment failure. ANO-1 accident sequences which were determined to lead to core melt were examined and quantified. Those core melt sequences with the highest frequency were reexamined to consider operator recovery actions. The frequency of these sequences was then recalculated considering recovery and a new sequence frequency was derived. Those sequences which still remained dominant are presented in Figure 1. The solid lines on the histogram represent the release category frequencies. (Release categories define the severity of the post core melt radioactive material release from containment. Category 1 releases are the most severe and category 7 are the least.) The sequences shown represent 90 percent of the total release category frequency for categories 2, 4, and 6, and 85 percent of categories 3, 5, and 7. They represent 75 percent of category 1.

Sequence $B(1.2)D_1$ α, γ, β, ϵ:

This sequence is initiated by a reactor coolant pump seal rupture or a rupture in the reactor coolant system in the range .38"<D≤1.2" (B(1.2)), followed by failure

Dominant Accident Sequences	Release Category						
	1	2	3	4	5	6	7
$B(1.2)D_1$	α 3×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ε 1×10^{-6}
$B(1.2)D_1C$	α 4×10^{-10}	γ 2×10^{-6}		β 3×10^{-8}		ε 2×10^{-6}	
$T(LOP)LD_1YC$	α 1×10^{-9}	δ 2×10^{-6}		β 7×10^{-8}		ε 8×10^{-6}	
$B(4)H_1$	α 1×10^{-8}	γ 7×10^{-7}			β 1×10^{-8}		ε 7×10^{-7}
$T(D01)LD_1YC$	α 3×10^{-10}	δ 6×10^{-7}		β 2×10^{-8}		ε 2×10^{-6}	
$T(D02)LD_1YC$	α 2×10^{-10}	δ 5×10^{-7}		β 2×10^{-8}		ε 2×10^{-6}	
$B(1.66)H_1$	α 1×10^{-10}	γ 6×10^{-7}			β 8×10^{-9}		ε 6×10^{-7}
$T(D01)LQ\text{-}D_3$	α 4×10^{-10}	γ 2×10^{-6}			β 3×10^{-8}		ε 2×10^{-6}
$T(A3)LQ\text{-}D_3$	α 3×10^{-10}	γ 2×10^{-6}			β 2×10^{-8}		ε 2×10^{-6}
$T(FIA)XD_1$	α 3×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ε 1×10^{-6}
$T(D01)LD_1$	α 2×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ε 1×10^{-6}
$T(A3)LD_1$	α 1×10^{-10}	γ 5×10^{-7}			β 7×10^{-9}		ε 5×10^{-7}
$T(D01)LD_1C$	α 2×10^{-10}	γ 9×10^{-7}		β 1×10^{-8}		ε 9×10^{-7}	
$T(A3)LD_1C$	α 1×10^{-10}	γ 7×10^{-7}		β 1×10^{-8}		ε 7×10^{-7}	
Category Total	2×10^{-8}	2×10^{-5}	$<10^{-7}$	2×10^{-7}	2×10^{-7}	2×10^{-5}	1×10^{-5}

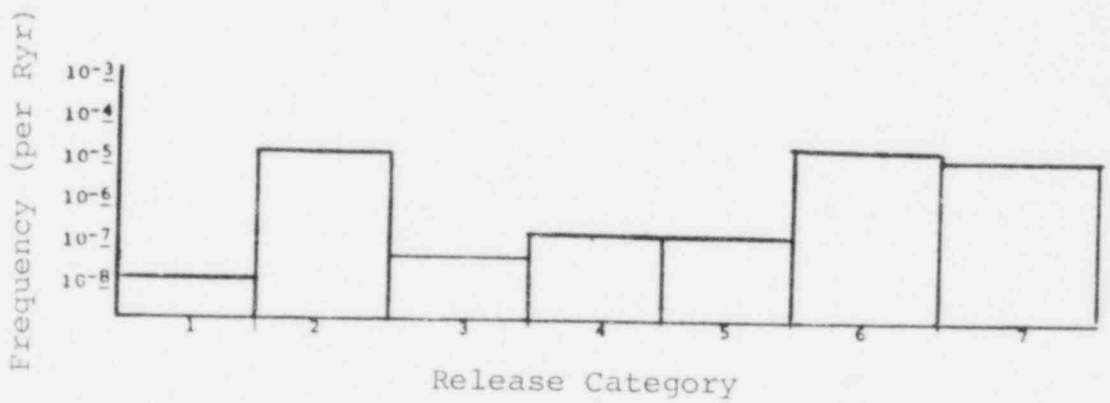


Figure 1. ANO-1 Dominant Accident Sequences

Table 1

Symbols Used in Figure 1

Initiating Events

B(1.2) - Reactor Coolant Pump Seal Rupture or Small-Small LOCA (.38"<D≤1.2")

B(1.66) - Small LOCA (1.2"<D≤1.66")

B(4) - Small LOCA (1.66"<D≤4")

T(LOP) - Loss of Offsite Power Transient

T(PCS) - Loss of Power Conversion System Transient Caused by Other Than a Loss of Offsite Power

T(FIA) - Transients With All Front Line Systems Initially Available

T(A3) - Transient Initiated by Failure of the ES Bus A3 (4160VAC)

T(DO1) - Transient Initiated by Failure of the ES Bus DO1 (125VDC)

T(DO2) - Transient Initiated by Failure of the ES Bus DO2 (125VDC)

System Failure

C - Reactor Building Spray Injection System

D_1 - High Pressure Injection System (1 of 3 pumps)

D_3 - High Pressure Injection System (2 of 3 pumps)

H_1 - High Pressure Recirculation System

K - Reactor Protection System

L - Emergency Feedwater System

Q - Reclosure of Pressurizer Safety/Relief Valves

Y - Reactor Building Cooling System

Containment Failure Modes

α - Vessel Steam Explosion

β - Penetration Leakage

γ - Overpressure Due to Hydrogen Burning

ϵ - Base Mat Melt-Through

δ - Overpressure Due to Gas Generation

failure of the high pressure injection system (D_1). 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 a small LOCA occurs followed by failure of the high pressure injection system (HPIS). 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 dominant failure mode (though small probabilistically) of the HPIS is predicted to be failure of the operator to initiate the system. Information received from Babcock and Wilcox[3] indicates an engineered safeguards (ES) HPIS actuation signal due to low RCS pressure may not be generated following some LOCAs < 1.2" D. This sequence assumes an ES signal will not be generated prior to core uncovery and that the operator must initiate the system.

An important insight realized from the analysis of this sequence is that a possibility exists for failing one of the three HPIS pumps, given a LOCA 1.2" diameter, prior to generation of an ES signal. During normal operation, one of the pumps is operating and takes suction from the makeup (MU) tank to perform the function of makeup and purification of the RCS. (This same pump is realigned to take suction from the borated water storage tank (BWST) upon an ES signal to perform the function of emergency core cooling.) Upon a small LOCA the pressurizer level and pressure would begin to decrease and automatic

control actions will cause the makeup flow control valve to go full open and the pressurizer heaters to turn on, respectively. Calculations indicate that the pressurizer heaters will remain covered for an extended period and thus maintain RCS pressure well above the ES actuation set point. The calculation also indicates that the MU tank would empty prior to uncovering the pressurizer heaters. The MU tank is estimated to empty within approximately 14 minutes after LOCA initiation or about 10 minutes after the low MU tank level alarm. Upon dry-out of the MU tank, it is assessed that the operating HPI pump will fail in a short time.

Sequence B(1.2) D_1C α, β, γ, ϵ:

This sequence is initiated by a reactor coolant pump seal rupture or a rupture in the RCS piping in the range .38"<D≤1.2" (B(1.2)), followed by failure of the high pressure injection system (D_1) and reactor building spray injection system (C). 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 B(1.2) D_1 sequence described previously except that the reactor building spray injection system is also unavailable. Failure of the spray system results in a more severe release of radioactive material from the containment because the sprays are not available to scrub the containment atmosphere. The primary contributors to the frequency of this sequence are due to failures which are common to the suction paths of all three HPI pumps and both spray pumps. All five pumps take suction from the BWST via a single

manual valve in series with two motor operated valves (MOVs) in parallel. If the single manual valve or both MOVs are failed closed, the HPI pumps would fail within a few minutes, followed by failure of the spray pumps within approximately 15 minutes. Very little time is available to recover these faults before HPI pump failure and thus no recovery credit is given.

The remaining contributors are combinations of suction MOV faults in one train and failure of pump support systems in the other train.

Sequence T(LOP)LD$_1$YC α, β, δ, ϵ:

This sequence is initiated by a loss of offsite power with concomitant failure of the power conversion system (T(LOP)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D_1), the reactor building cooling system (Y), and the reactor building spray injection system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure (δ), penetration leakage (β) or base mat melt-through (ϵ).

This sequence is equivalent to the well-known TMLB' sequence which was one of the dominant risk contributors for the Surry PWR reported in WASH-1400.

This sequence is initiated by a loss of offsite power transient followed by failure of all core cooling and containment systems capable of mitigating the accident. It is estimated that core melting will begin in approximately one hour.

Approximately 80 percent of the sequence frequency is due to common mode failure of both station batteries on demand following the loss of offsite power. Common

mode failure of both batteries was calculated based on the methodology presented in NUREG-0666 "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants."(5) Since all mitigating systems require DC power for successful operation, all mitigating systems will fail following failure of both batteries. The remaining 20 percent of the sequence frequency is due to double and triple faults in the AC, DC and emergency feedwater systems. It is estimated that approximately 75 percent of the system faults causing this sequence can be recovered prior to the onset of core melt. Most recovery actions involve recovery of offsite power.

Sequence B(4) H_1 α, γ, β, ϵ:

This sequence is initiated by a rupture in the RCS piping in the range 1.66"<D≤4" (B(4)) followed by failure of the high pressure recirculation system (H_1). 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 that the LOCA systems perform successfully during the injection phase but the high pressure recirculation system (HPRS) fails during the recirculation phase. Failure of the HPRS would lead to boil off of the water covering the core resulting in core melt.

The prime contributor to HPRS failure (though small probabilistically) is failure of the operators to initiate or correctly follow emergency procedures while initiating the HPRS. The HPRS is initiated when the BWST is 84 percent empty and requires several operator actions,

some of which are conducted away from the control room: manual valves connecting the suction of the high pressure pumps to the discharge of the low pressure pumps are opened in the auxiliary building and motor operated valves connecting the suction of the low pressure pumps to the containment sump are opened from the control room.

Another potentially important contributor to HPRS failure is failure of the pump room cooling system. All three pumps are kept below their design operating temperature by a single operating cooler which consists of a fan/service water heat exchanger. (Two other nonoperating coolers could potentially be used, but they must be started by the operator.)

Many single failures of the operating room cooler were identified. These include failure of the room cooler itself, failures in the fan electric power subsystem and failures in the heat exchanger service water subsystem. The number of single failures was large partly due to the fact that the service water pump supplying the heat exchanger is powered by the "odd" electrical load division and the fan is powered by the "even" load division. (ANO-1 has two load divisions, commonly referred to as "even" and "odd".) Because of this the room cooler is dependent on both load divisions. This arrangement roughly doubles the number of single failures.

Most of the single HPRS room cooler failures were assessed to have a 99 percent recovery probability. The recovery actions involve manual initiation of one of the two nonoperating room coolers. Initiation of these coolers is performed outside the control room and would most likely be done following a high pump stator winding

temperature alarm. Initiation of the alternate room coolers is not described in the LOCA procedures, but we feel that recovery following failure of HPRS room cooling is likely because the room heat up would be slow since the water pumped by the HPRS is cooled by the low pressure heat exchangers. It should be noted that failure of the HPRS via room cooling failure should be considered to be "potentially" important since no plant tests have been performed which absolutely establish the need for HPRS room cooling.

Sequence T(DO1)LD$_1$YC $\alpha, \beta, \delta, \epsilon$:

This sequence is initiated by a failure of the engineered safeguards power bus DO1 (125DVC) with concomitant failure of the power conversion system (T(DO1)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D$_1$), the reactor building cooling system (Y), and the reactor building spray injection system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure (δ), penetration leakage (β), or base mat melt-through (ϵ).

This sequence assumes a transient induced by the failure of the "odd" DC bus followed by failure of all core cooling and containment systems capable of mitigating the accident.

Roughly 60 percent of the sequence frequency is due to subsequent failure of the "even" DC bus. Failure of this bus would render the plant totally without DC power. DC control power is required by all transient front line systems and thus no mitigating systems would be available.

Recovery from this event would depend upon the severity of the DC bus failure. We have assumed that the fault is non-recoverable since insufficient data was available to estimate recovery action, and recovery actions must be performed within approximately one hour to prevent the onset of core melt.

The remaining 40 percent of the sequence frequency is comprised of several combinations of failures due to the initiating event, faults in the emergency feedwater system and support system (i.e., AC power, actuation system faults, service water system) faults.

Sequence T(D02)LD$_1$YC α, β, δ, ϵ:

This sequence is initiated by a failure of engineered safeguards bus D02 (125VDC) with concomitant failure of the power conversion system (T(D02)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D$_1$), the reactor building cooling system (Y), and the reactor building spray system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure (δ), penetration leakage (β), or base mat melt-through (ϵ).

This sequence is similar to the T(D01) LD$_1$YC sequence just described, except that in this case, failure of the "even" DC bus is the initiating event.

Roughly, 70 percent of the sequence frequency is due to subsequent failure of the "odd" DC bus. Failure of this bus would render the plant totally without DC power. DC control power is required by all transient front line systems, and thus, no mitigating systems would be available. As was the case for the previous

sequence, no recovery credit for this fault was given because of the relatively short time to the onset of core melt (~1 hour) and since insufficient data was available to estimate recovery.

Sequence $B(1.66)H_1, \alpha, \gamma, \beta, \epsilon$:

This sequence is initiated by a rupture in the RCS piping in the range $1.2" < D \leq 1.66"$ (B(1.66)) followed by failure of the high pressure recirculation system (H_1). 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 $B(4)H_1$ sequence discussed previously. The prime contributor to the sequence failure is the same; namely, failure of the operators to initiate the HPRS.

Sequence $T(DO1)LQ - D_3 \alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of the engineered safeguards power bus DO1 (125 VDC) with concomitant failure of the power conversion system T(DO1), followed by failure of the emergency feedwater system (L), failure of one pressurizer safety/relief valve to reclose (Q), and failure to inject flow from two of three high pressure injection pumps (D_3). 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 a transient induced LOCA (TQ) in which core cooling fails during the injection phase (LD_3). TQ sequences require the same core cooling

requirements during the injection phase (ECI) as B(1.66) LOCAs since a stuck open pressurizer safety valve falls in $1.2<D\leq1.66$ break size range. ECI success requires either two of three high pressure pumps OR one of three high pressure pumps and the emergency feedwater system (EFS). Failure of events L and D_3 precludes either ECI success mode.

Loss of DC power bus D01, the initiating event, precludes the success of two high pressure pumps and fails approximately one-half of the EFS. The dominant contributors therefore all involve single failures of the remaining half of the EFS.

Sequence T(A3)LQ - D_3 α, β, γ, ϵ:

This sequence is initiated by a failure of the engineered safeguards power bus A3 (4160VAC) with concomitant failure of the power conversion system (T(A3)), followed by failure of the emergency feedwater system (L), failure of one pressurizer safety/relief valve to reclose (Q), and failure to inject flow from two of the three high pressure injection pumps (D_3). 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 one just discussed except it is initiated by an AC rather than a DC bus failure. It is a transient induced LOCA (TQ) in which core cooling fails during the injection phase (LD_3). TQ sequences require the same core cooling requirements during the injection phase (ECI) as B(1.66) LOCAs since a stuck open pressurizer safety valve falls in $1.2<D\leq1.66$ break size range. ECI success requires either two of

of three high pressure pumps OR one of three high pressure pumps and the emergency feedwater system (EFS). Failure of events L and D_3 precludes either ECI success mode.

Loss of AC power bus A3, the initiating event, precludes the success of two high pressure pumps and fails approximately one half of the EFS. The dominant contributors therefore involve single failures of the remaining half of the EFS.

Sequence T(FIA)KD_1, α, γ, β, ε:

This sequence is initiated by a requirement for a reactor trip with all front line systems initially available (T(FIA)), followed by failure of the reactor protection system (K), and failure of the high pressure injection system (D_1). Containment failure is predicted by one of the following: vessel steam exposion (α), 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.(1) This report states that if the reactor protection system fails to scram the reactor following a transient, an RCS peak pressures of 4900 psi range may result.[1] (The 4900 psi value is quoted for cases in which the pressurizer electromatic relief valve (ERV) fails to open. This case applies to ANO-1, since the ERV has been effectively disabled due to closure of its block valve.) Analysis conducted by B&W indicates that RCS components should

[1]It should be noted that in order to attain a peak pressure of 4900 psi, Reference 1 assumed pessimistic values for certain parameters, e.g., moderator temperature coefficient.

remain functional after this peak pressure.[12] The analysis of this sequence assumes that the RCS components would survive the peak pressure. (It should be noted that ATWS for B&W plants is currently an unresolved safety issue which, for PWRs, rests primarily upon the peak pressure question.)

The 4900 psi pressure quoted in Reference 1 assumed an ATWS following a loss of main feedwater (LOMF). The LOMF ATWS is the worst case in terms of peak pressure because the only available RCS heat removal system capable of reducing the peak pressure is the emergency feedwater system (EFS). Since the EFS has a heat removal capacity much smaller than the main feedwater system, it is relatively ineffective (in comparison with main feedwater) in reducing the peak pressure. It should be noted, however, that in the sequence analyzed here, main feedwater is initially available. Whether or not main feedwater is initially available at ANO-1 is not expected to significantly affect the peak pressure. The reason for this is that many requirements for a reactor trip also automatically cause the main feedwater system to trip off one main feed pump and runback the remaining feed pump to a level approximately that of the EFS (e.g., these actions would be taken following a turbine trip).

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 these situations the high pressure injection system must be actuated by the operator to inject borated (i.e., negative reactivity) water to successfully shut down the reactor and to replace RCS inventory lost via the pressurizer safety valves during the pressure transient. This sequence assumes that the high pressure injection fails followed by an eventual core melt.

The dominant contributors to RPS failure are due to double circuit breaker failures. (These circuit breaker failures cannot be recovered by pushing the trip buttons within the control room and were, therefore, assessed to be non-recoverable.) HPIS failure is dominated by failure of the operator to actuate the system.

Sequence $T(D01)LD_1\alpha,\beta,\gamma,\epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus D01 (125VDC) with concomitant failure of the power conversion system T(D01), followed by failure of the emergency feedwater system (L), and the high pressure injection system (D_1). 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 depicts a loss of the systems which provide the normal and emergency 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 actuate the high pressure injection system (HPIS) and establish a "feed and bleed" core cooling operation.

If the operator fails to actuate the HPIS or the HPIS subsequently fails, the RCS inventory would boil off through the pressurizer safety relief valves leading to uncovering the core and eventual core melt. It is estimated that core melting will begin at approximately one hour.

This sequence is initiated by failure of the "odd" DC bus. Failure of this bus causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the HPIS and emergency feedwater system. Hardware and human failures in the remaining one-half of these two systems comprise the dominant contributors to the sequence frequency. It is estimated that roughly 85 percent of these failures can be recovered before the onset of core melt. Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

Sequence $T(A3)LD_1\ \alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus A3(4160VAC) with comcomitant failure of the power conversion system (TA3), followed by failure of the emergency feedwater system (L), and the high pressure injection system (D_1). 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 $T(D01)LD_1$ sequence just described, except that in this case the initiating event is caused by failure of an "odd" AC bus. Like in

the previous sequence, failure of this bus causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the high pressure injection system and emergency feedwater system. Hardware and human failures in the remaining one-half of these two systems comprise the dominant contributors to the sequence frequency. It is estimated that roughly 85 percent of these failures can be recovered before the onset of core melt (~1 hour). Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

Sequence $T(D01)LD_1C\,\alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus D01 (125VDC) with concomitant failure of the power conversion system T(D01), followed by failure of the emergency feedwater system (L), the high pressure system (D_1), and the reactor building spray system (C). 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 $T(D01)LD_1$ discussed earlier except that for this sequence the reactor building spray system (RBSS) also fails. Failure of DC bus D01 causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the emergency feedwater system, high pressure injection system (HPIS), and RBSS. Hardware failures in the remaining half of the latter three systems comprise the dominant contributors to the sequence frequency. Failure of the

HPIS and RBSS is dominated by a MOV which is common to the suction of the pumps in the remaining half of these systems. It is estimated that roughly 85 percent of the hardware failures can be recovered before the onset of core melt (~1 hour). Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

Sequence T(A3)LD$_1$C α, β, γ, ϵ:

This sequence is initiated by a failure of engineered safeguards power bus A3 (4160VAC) with concomitant failure of the power conversion system T(A3), followed by failure of the emergency feedwater system (L), the high pressure injection system (D$_1$), and the reactor building spray system (C). 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 very similar to T(D01)LD$_1$ C just discussed except that this sequence is initiated by an AC rather than a DC bus failure. Failure of AC bus A3 causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the emergency feedwater system, high pressure injection system (HPIS), and RBSS. Hardware failures in the remaining half of the latter three systems comprise the dominant contributors to the sequence frequency. Failure of the HPIS and RBSS is dominated as in the previous sequence, by a MOV which is common to the suction of the pumps in the remaining half of these systems. It is estimated that roughly 60 percent of the hardware failures can be recovered before the onset of core melt (~1 hour). Most

recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

The frequency of the sequence is dominated, however, by two cut sets which are estimated to have little or no recovery potential. If the HPIS/RBSS common suction valve fails closed, the HPI pumps would fail within a few minutes followed by failure of the spray pumps within approximately 15 minutes. The emergency feedwater system non-recoverable faults are due to failure of the turbine pump or one of its condensate storage tank (CST) suction valves. No plant data was available to estimate recovery of the turbine pump given a start failure and thus no recovery credit was given. Also, if one of the turbine pump CST suction valves fails closed, the pump is predicted to fail before the operator can realign the pump to the alternate service water system water source.

Engineering Insights

During the course of this analysis, several engineering insights were realized concerning the operational safety of ANO-1. These insights can be categorized as being related to either plant design and hardware or plant operations.

Plant Design Insights

- The list of the dominant sequences (Figure 1) and those identified to be near dominant in Appendix C indicates that the following general types of accident sequences contribute most to the ANO-1 core melt frequency

- LOCAs initiated by reactor coolant pump seal ruptures contribute ~20 percent.
- Station blackout sequences contribute ~20 percent.
- Sequences initiated by ANO AC and DC power bus failures contribute ~35 percent.
- Other transients and small LOCAs contribute ~20 percent.
- Large LOCA sequences contribute <5 percent.

- The total frequency of core melt for ANO-1 is estimated at 5×10^{-5}/yr. This estimate is similar to estimates made for several other light water reactors in other probabilistic risk assessments, e.g., Surry, Peach Bottom[18], Oconee[2] and Grand Gulf[26].

- Several single failures were identified in front line/support systems. Operator recovery of some of these single failures is possible, however. The singles identified were:
  - The high pressure recirculation system pump room cooling is susceptible to several single failures in its electric power and service water support systems. The operator may recover from this event by starting an alternate room cooler.
  - A single valve failure can obstruct the common service water discharge line. This would cause a reactor trip and several transient mitigating systems to be unavailable. The operator may recover from this event by performing actions away from the control room and utilizing an alternate discharge line.

- Both emergency feedwater pumps take suction from the condensate storage tank through a common header containing three valves. Both pumps could fail before the operator recognizes the problem and valves in an alternate water supply.

- All pumps located within the high pressure, low pressure, and spray system take suction from the borated water storage tank via a common header containing a manual valve. Failure of this valve would cause failure of all three systems. No recovery action was identified since the dominant valve failure mode would require disassembly of the valve to correct.

- The list of dominant accident sequences indicates that support system faults are important to the risk of the plant. The most important support systems were AC/DC power and service water. Of lesser importance were room cooling systems and automatic actuation systems. The former were most important because faults within these systems can cause a reactor trip initiating event with concomitant failure of several safety system components. AC/DC and service water faults also had lower recovery potential than other support systems. Room cooling and auto actuation system faults were of less importance because significant initiating events were not identified and recovery potential was generally high.

- Review of ANO-1 logs revealed the following safety-related data trends as compared with generic nuclear industry data. (The generic data was provided by NRC and was very similar to the WASH-1400 data base.)

- Motor operated valve failure on demand probabilities are higher than industry data (~ factor of 4).
- Air operated valve failure on demand probabilities are higher than industry data (~ factor of 10).
- Diesel generator failure on demand probabilities are about the same as industry data.
- Pump and valve control circuit failure on demand probabilities are lower than what can be derived from industry data (~ factor of 4).
- Reactor building fan coolers have a higher failure on demand probability than industry fan data because of the policy at ANO-1 not to repair a reactor building fan until the next reactor shutdown.
- The probability of main feedwater system failure following reactor trips not initiated by loss of main feedwater (e.g., turbine trip, loss of load, etc.) is higher than that reported in WASH-1400 (~ factor of 6).
- Review of ANO-1 trip logs and comparison with reactor trip data presented in EPRI-NP801 indicated that ANO-1 transient frequencies and type are typical of the nuclear industry.

- An upgrade of the emergency feedwater system and installation of a new emergency feedwater control system/steam generator isolation control system is scheduled to be completed by 1982. The new control systems were designed such that single integrated

control system (ICS) faults or non-nuclear instrumentation (NNI) faults will not fail or significantly degrade the emergency feedwater system. (These types of failures have plagued B&W reactors in the past.) Review of preliminary design information verified this to be the case.

- An upgrade of NNI power supplies has been implemented at ANO-1. This upgrade has enhanced the reliability of NNI power supplies and has eliminated NNI single failures which can cause an inadvertant LOCA due to opening of the PORV. (This type of failure was possible in the previous NNI/PORV design.)
- The switchover from the borated water storage tank to the containment sump, in response to small LOCA, requires some operator actions outside the control room in radiation areas. Switchover and all other required actions at other plants we have studied can be performed within the control room.
- Via use of probabilistic importance measures, the ANO-1 components/events which contribute most to the core melt frequency, assuming the operator does not attempt to recover failed system components, are all related to the plant design. The top ten consist of six initiating events, failure of the pressurizer safety valves to reclose after being demanded open, common mode battery failure, failure of the turbine driven emergency feedwater pump, and failure of the thermostat which actuates an AC/DC room cooler.
- The core meltdown analysis presented in Section 8.1.2 suggests that there is a strong correlation

between the ANO core melt frequency and expected ANO risk. Table 8-2 indicates that every core melt sequence has a .2 to .5 probability of being placed in a high risk release category (Category 2).

Plant Operations Insights

- A review of the dominant and near dominant accident sequence cut sets reveals that only ~10 percent of the total core melt frequency is attributed to operator errors committed during the course of an accident. One of the main reasons for this low contribution is due to the post Three Mile Island directive by the NRC requiring an increased number of licensed operators to be present in the control room. The added human redundancy afforded by this directive significantly increases the probability of recovering from operator errors. Another reason for the low contribution is due to the recent installation of the Safety Parameter Display System (SPDS) at ANO-1. The SPDS continuously plots the reactor coolant system pressure and temperature and compares them to operating envelopes and saturation curves. We feel the SPDS is an excellent diagnostic tool and thus affords recovery potential from operator errors. The SPDS also provides the type of information necessary to determine that a core damage accident is likely.

- A review of the dominant and near dominant sequences reveals that operator recovery actions play an important role in reducing the frequency of various accidents. Overall, operator recovery reduced the ANO-1 core melt frequency by approximately a factor of five.

- The unavailability of ANO-1 systems due to outages resulting from test and maintenance is generally small compared with other faults. Test unavailabilities are small because most systems are not taken out of service during the test and are thus able to perform their safety function. For those systems that are taken from service, test personnel are, in general, kept in contact with control room operators so that the system could be quickly restored to service upon request by the operator. Review of plant maintenance logs revealed that the frequency at which a given active component is taken out for maintenance while the plant is at power is small. A comparison of the ANO maintenance frequency with the plants studied in the RSS, for example, indicates that components are taken out for maintenance about an order of magnitude less frequently at ANO. The primary reason for the small maintenance frequency is due to the policy at ANO-1 not to do periodic preventative maintenance on safety systems when the plant is at power. Preventive maintenance on these systems is conducted during reactor shutdowns.

- Safety system/component unavailabilities caused by the failure of personnel to realign valves and circuit breakers to their safeguards positions after test and maintenance activities are generally small compared with other faults. There are several reasons for this including: (1) the component tagging procedure requires the operators to perform redundant checks of valve and circuit breakers alignment following test and maintenance, (2) most safety system valves and circuit breakers have alignment indication in

the control room and are verified via a check list to be in the correct position every 8-hour shift, (3) required post maintenance tests of components would, in general, inform the operator that valves and circuit breakers have not been aligned properly.

Design and Procedural Changes Made at ANO-1

There were three changes made to ANO-1 procedures as a result of this study. The systems analysis presented in this study is based on the implementation of these changes. The changes are listed and discussed below.

1. Quarterly tests of the two station batteries are now required to be performed on a staggered basis, i.e., one battery every six weeks. The previous procedure allowed both batteries to be tested on the same day by the same personnel.

2. AC and DC switchgear room cooler actuation circuitry are now required to undergo a complete test. The previous test procedure omitted a portion of the circuitry.

3. A nomenclature error identified in the low pressure pump test procedure was corrected.

Results presented in NUREG-0666 "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants" indicates that failure of multiple station batteries at nuclear power plants have occurred in the past. One of the potential causes for such failures identified in that report was a common mode test and maintenance error. The changes introduced to the battery test procedure, requiring staggered battery tests, reduced the probability of such common mode failures.

Cooling of the AC and DC switchgear rooms is required for successful long term operation of LOCA and transient safety systems. The fault tree analysis of the room chillers revealed that the thermostat circuitry which actuates the room chillers was not required to be tested. The change introduced to the room chiller test procedure now requires the chillers to be actuated by applying a heat source to the thermostats.

A potentially significant error was identified in the low pressure injection system pump test procedure. Upon completion of a pump test, certain valves must be realigned to return the pump train to service. The procedure requested the wrong valves to be realigned. Discussions with plant personnel revealed that this error had been identified and corrected a few years previous. However, they could not account for the reintroduction of the error. Upon closer examination, it became evident the error was reintroduced because the names of the valves to be realigned violated the standard component naming scheme implemented at the plant. In most systems at the plant, components in train A have an "A" in the component identifier and components in train B have a "B" in the component identifier. However, an exception to this rule exists in the low pressure injection system. Some valves with a "B" identifier must be realigned to return an "A" pump to service and vice versa. An unknowing reviewer of the test procedure must have seen an "A" and "B" together and thought it was a typographical error. It has been suggested to the plant that for all procedures involving a violation of the component naming scheme that a special note be attached warning reviewers and test personnel that the procedure is correct.

CHAPTER 1

INTRODUCTION

Probabilistic safety analysis and risk assessment techniques are widely believed to offer powerful tools for the safety design and safety evaluation of nuclear power plants. Past attempts to apply such techniques to commercial nuclear plants have provided useful catalogues of accident sequences, identified many strengths and weaknesses in the design and operation of the plants, provided insights into the importance of accident contributors, and provided rough estimates of the likelihood of serious accidents. Recent evidence tends to suggest that plant-to-plant differences in design and operation may give rise to significant differences in the likelihood or course of accidents. Therefore, the extensive application of these safety analysis techniques to many reactor plants appears to be desirable. This need is reflected in the Nuclear Regulatory Commission's Three Mile Island Action Plan (NUREG-0660) in which the Interim Reliability Evaluation Program (IREP) is identified as a high priority effort leading to the systematic risk assessment of all reactors (Section II.C).

The Interim Reliability Evaluation Program is intended to apply probabilistic risk analysis techniques to several nuclear power plants and to develop procedures adequate for the consistent analysis of all plants with the following specific objectives: (1) Identify--in a preliminary way--those accident sequences that dominate the contribution to the public health and safety risks originating in nuclear power plant accidents; (2) develop a foundation for subsequent, more intensive, applications of probabilistic safety analysis or risk assessment on the

subject plants; (3) expand the cadre of experience practitioners of risk assessment methods within NRC and the nuclear power industry; and (4) evolve procedures codifying the competent use of these techniques for use in the extension of IREP to all domestic light water reactor plants.

Phase I of the IREP study consisted of a reliability analysis of the Crystal River Unit 3 facility. A report on that effort has been published (NUREG/CR-2515). Using methodological insights gained from the Crystal River Study, the Phase II IREP studies were initiated in September 1980. The Phase II studies consist of analyses of four plants:

1. Browns Ferry Unit 1, by a team composed of personnel from EG&G, Idaho, and Energy, Inc.
2. Arkansas Nuclear One Unit 1, by a team composed of personnel from Sandia National Laboratories, Science Applications, Inc., (SAI) and Arkansas Power and Light Company.
3. Calvert Cliffs Unit 1, by a team composed of personnel from Science Applications, Inc., Evaluation Associates, and NRC.
4. Millstone Unit 1, by a team composed of personnel from Science Applications, Inc., Northeast Utilities, and NRC.

Responsibility for overall technical management of the study rested with Sandia National Laboratories. Periodic reviews to assure the quality of the product were conducted by Sandia National Laboratories and NRC personnel not involved directly with the work of any one team, with the assistance of Energy, Inc.

This report is one of a series of four reporting the results of these Phase II studies. Separate reports will be issued regarding procedures for conducting future analyses of the same scope and breadth as these four studies and detailing the technical and methodological insights and nuclear safety perspectives gained from this activity.

The reader is cautioned that while it is our opinion that these studies represent the state-of-the-art given their scope, there are associated limitations. External events (earthquakes, fires, etc.) are not included and the assignment of accident sequences to release categories was performed in a subjective manner with limited plant-specific calculations. Thus, this portion of the study relied heavily on analyses performed previously on similar facilities. Other limitations are discussed in detail in Chapter 8. While accident sequence and release category frequencies were quantified, they are of value primarily in comparative analyses and the absolute values determined should not be used without a clear appreciation of their inherent uncertainties. The principal product obtained is the integrated engineering logic presented in the plant and system models and insights into plant features contributing significantly to risk, not the specific values computed for accident frequencies.

1.1 Makeup of the ANO-1 Analysis Team

The team was comprised of 13 individuals from Sandia National Laboratories, Science Applications, Inc., and Arkansas Power and Light. Four members worked full time, while the other nine contributed on a part-time basis. Sandia National Laboratories was responsible for team leadership. The team members had varying degrees of risk analysis experience. Some had little or no experience

while others had participated in risk studies such as the Reactor Safety Study Methodology Applications Program, the Limerick study, and the Crystal River study.

Seven of the 13 members were systems analysts. They were responsible for construction of the event tree and fault tree models which were utilized in determining the most probable core meltdown accident sequences.

Two of the members were human factors specialists. It was their duty to review, with the aid of the systems analysts, the procedures followed by ANO personnel during test and maintenance activities and in response to accidents initiated by a variety of LOCAs and transients. The purpose of the review was to identify the most probable human errors associated with performing these procedures. These faults were then incorporated into the fault tree models.

Three of the members were computer specialists. One of these was responsible for manipulation and debugging of the computerized fault tree models. The remaining two were responsible for running the SETS code.(16) SETS operates on the system fault tree models and performs the Boolean algebra necessary to determine the most frequent core meltdown accident sequences.

The last, and one of the more valuable team members, was the individual provided by Arkansas Power and Light. His job was to gather necessary plant information and to review all work for technical accuracy. His past experience as a shift supervisor at ANO and his knowledge of the plant design and operations facilitated correct modeling of plant and operator response.

CHAPTER 2

IREP METHODOLOGY

To provide guidance for the IREP analyses and to assist in consistency among the four IREP teams, procedures for the analysis were developed. Since these procedures had never been used in their entirety, it was recognized that some flexibility in approach would be necessary. Nevertheless, the four teams generally followed the same approach. This is described below.

2.1 Information Base

The IREP analyses represent an integrated plant systems analyses. Detailed analyses were performed of those systems required to respond to a variety of initiating events and of those systems supporting the responding systems. The analysis included unavailabilities during test and maintenance activities, human errors which could arise in restoring the systems to operability following test and maintenance and in response to accident situations, and a thorough investigation of support system faults which could affect operation of more than one system.

To perform the analysis, considerable information and, in some instances, very detailed information was obtained from the plant. The sources of information used in the ANO-1 analysis are listed in Table 2-1.

The final safety analysis report (FSAR) and plant system descriptions and drawings provided the basic information base for the analysis. This was supplemented by information contained in other studies of the plants (where available) and by more detailed information in support of particular aspects of the analysis.

Table 2-1

Information Sources for ANO-1 IREP

- Final Safety Analysis Report
- System description and plant drawings
- EPRI NP-801, "ATWS: A Reappraisal - Part III, Frequency of Anticipated Transients"
- Licensee Event Reports for the plant and similar plants
- System performance documentation
- Electrical one-line drawings
- Control and actuation circuitry drawings
- Test and maintenance procedures
- Emergency procedures
- Modified WASH-1400 data base
- Plant logs
- "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications" (NUREG/CR-1278)
- Plant visits
- Discussions with and review by plant personnel
- Technical specifications
- ANO Abnormal Transient Operating Procedures (ATOG)
- Analyses of similar plants - Oconee RSSMAP (NUREG/CR-1659), Crystal River IREP (NUREG/CR-2515), Babcock and Wilcox Generic Studies (NUREG-0560, -0565, etc.), TMI Studies (NSAC-1)
- ANO-1 MARCH Code Deck

To identify initiating events and initiating event frequencies, EPRI NP-801, "ATWS: A Reappraisal - Part III, Frequency of Anticipated Transients," was used as the basic source. Additional insight was obtained through reviewing licensee event reports for the plant and for plants of similar design. To identify the systems needed to respond to an accident and their success criteria, the FSAR was used. In some instances, documentation from the plant or vendor was obtained suggesting and supporting the use of less stringent success criteria.

To construct the fault tree models, more detailed drawings were obtained, particularly for electrical systems and control and actuation circuitry. Test, maintenance, and emergency procedures were reviewed to identify potential human errors to be included in the plant models.

Data for quantifying the fault trees was a mixture of generic and plant specific data. Basic hardware failure rate data was obtained from a modified WASH-1400 data base assembled by NRC personnel participating in the study. For particular components, plant specific data obtained from plant logs was used. Plant specific test and maintenance frequencies obtained from plant logs were used in the analysis. Data for human error rates were obtained from the "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278.

In addition to the above documentation, the utility personnel participating in the study served as contacts with the plant to obtain more information when needed. Each team visited their plant to view particular equipment

and to discuss questions with plant personnel. The utilities also reviewed periodic reports to ensure accuracy of information.

2.2 Methodology

The IREP analyses consisted of eight tasks:

1. Plant familiarization
2. Event tree construction
3. Systems analysis
4. Human reliability and procedural analysis
5. Data Base development
6. Accident sequence evaluation
7. Containment analysis
8. Interpretation and analysis of results.

The relationships between these tasks are illustrated in Figure 2-1. Each is discussed briefly below.

2.2.1 Plant Familiarization

The initial task of the analysis involved the analysts' becoming familiar with the plant. This began by identifying those functions which must be performed to prevent core melt or to mitigate its consequences. By reviewing the FSAR and other documentation, the systems which perform these functions, termed "front line systems," were identified.

Initiating events for consideration in the analysis were determined from EPRI-NP801 and a review of licensee event reports. These were grouped such that all initiating events requiring the same systems to respond were placed in the same group. ANO-1 loss of coolant accidents (LOCA) were split into six groups. This grouping was by size of LOCA since mitigating requirements generally depend on the size of the break. ANO-1 transients

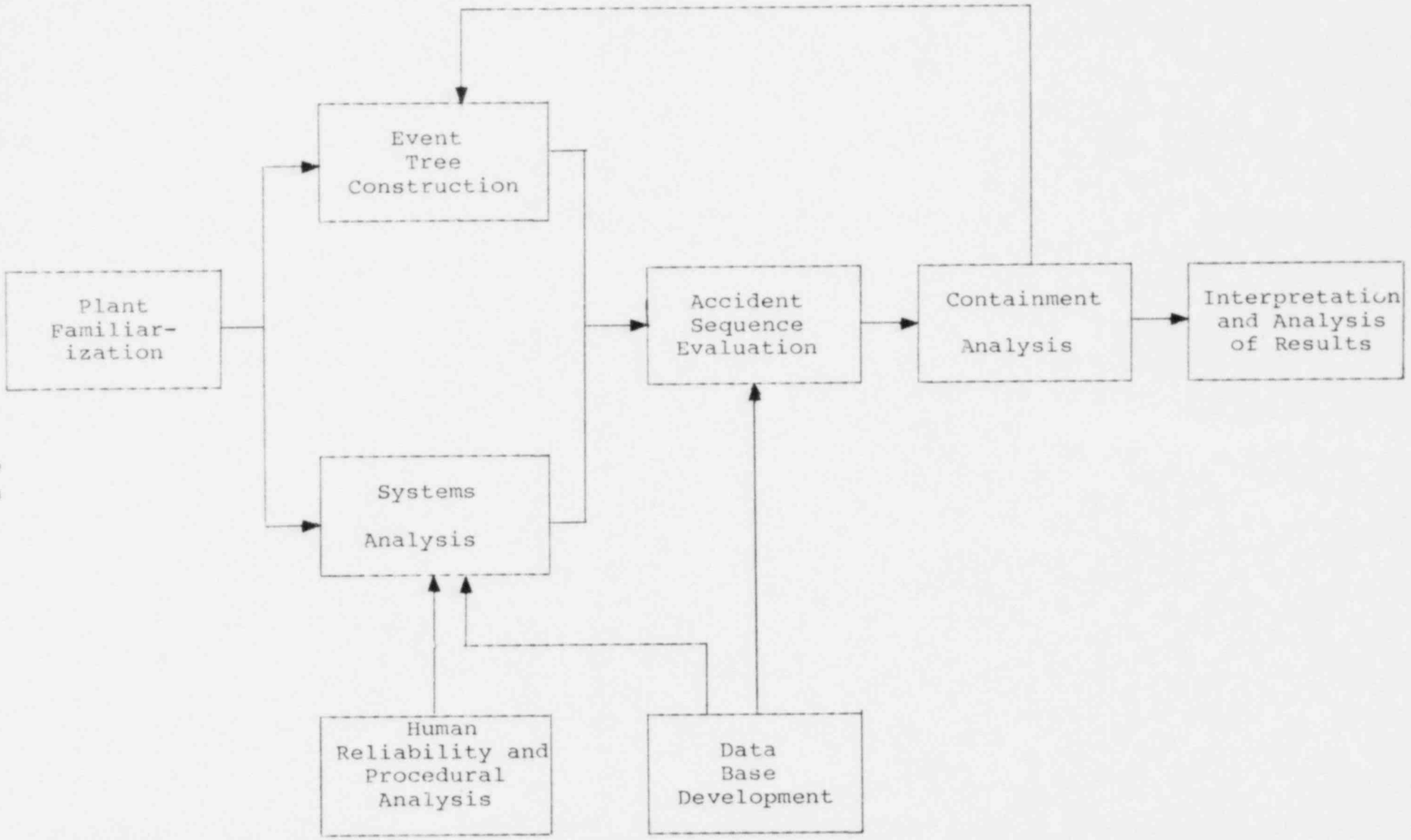


Figure 2-1. IREP Methodology

fell into eight groups. The grouping often reflected equipment lost as a result of the initiating event.

For each initiating event grouping, the criteria for successful system operation to mitigate the accident were determined. This information was usually found in the FSAR. Utility and vendor calculations sometimes indicated that the FSAR criteria were too conservative. Where appropriate documentation existed, the IREP teams used the more realistic criterion.

A final activity during the plant familiarization task was the identification of system dependencies. Systems which support the front line systems were identified; dependencies among various support systems were also noted.

Upon completion of the plant familiarization task, the following information had been developed:

1. The necessary functions to prevent core melt or to mitigate its consequence;
2. The systems which perform these functions (front line systems);
3. The initiating events included in the analysis and grouped according to mitigating requirements;
4. The systems required to respond to each initiating event group and the criteria for system success; and
5. Dependencies between front line and support systems and among support systems.

This task set the groundwork for construction of the models used in the study. The systems to be analyzed were identified, and the number of and headings for event trees were defined.

2.2.2 Event Tree Construction

The accident sequences to be analyzed in IREP were delineated by event trees. Functional event trees were constructed to clarify functional dependencies. From these and information developed in the plant familiarization activity, systemic event trees were constructed. Sequences delineated on the systemic trees were analyzed in the study.

In general, separate systemic event trees were constructed for each initiating event group. Each event tree had a different structure since the initiating events were grouped according to mitigating requirements. Different mitigating requirements result in different tree structure. Headings for the event trees correspond to the systems responding to the initiating event. Only front line systems appear on the trees. System dependencies and dependencies arising from phenomenological aspects of the accident are reflected in the tree structure.

2.2.3 Systems Analysis

Fault tree models were constructed for each front line system. Support system fault trees were constructed to model the particular interfaces with the front line systems. The fault tree modelling approach used in the ANO-1 analysis is discussed in Chapter 6. Top events for the front line system fault trees correspond to the success criteria defined in the plant familiarization task. The fault trees were developed to the component level. Component faults which affected only the particular component were grouped as "local faults." Faults which could affect multiple components, generally those

faults associated with support systems, were further developed. The level of detail in the fault trees generally corresponded to the detail of available data.

In addition to hardware faults, the fault trees included unavailability due to test and maintenance, human errors associated with failing to restore components to their operable state following test and maintenance, and human errors associated with accident responses. Human reliability analysis is discussed in the next section.

The detailed development contained in the system fault trees facilitated identification of hardware, test and maintenance, and human error faults which could cause multiple component failures. These classes of common mode failures were explicitly modeled in the fault trees. Other potential common mode failures such as environmental conditions or manufacturing defects were not considered in the study.

2.2.4 Human Reliability and Procedural Analysis

Test, maintenance, and emergency procedures were reviewed to determine potential human errors. Human errors associated with failing to restore the system to its operable state following test and maintenance were included explicitly in the fault trees. Potential operator errors in response to an accident were included in a limited way. The emergency procedures expected to be used in response to each accident sequence were reviewed to identify actions expected to be performed. Incorrect performance or omission of the actions were postulated and included in the model. The investigation, however, was limited to those actions expected to be performed,

rather than postulating all actions an operator might take.

2.2.5 Data Base Development

A modified WASH-1400 data base was used for quantification of hardware faults. In some instances, plant specific data was used instead. Test and maintenance intervals and durations were obtained, where possible, from discussions with plant personnel and from reviewing plant logs. Estimated upper values were chosen for human error rates for initial calculations. For those human errors which appeared in potentially dominant accident sequences, detailed analyses were performed with the assistance of human factors specialists. This approach to human error quantification permitted more efficient utilization of limited human factors expertise.

2.2.6 Accident Sequence Evaluation

For each accident sequence, a frequency was calculated. This was performed by logically combining the initiating event and the system successes and failures to develop combinations of failures (cut sets) which could result in the accident sequence. Frequencies assigned to the initiating events and probabilities assigned to each failure were combined to produce a frequency for each sequence.

The evaluation process was an iterative one. Initial calculations used generic data and upper bound human error rates. From these initial calculations, a collection of potentially dominant accident sequences was chosen. These were chosen based on a certain frequency below which none of the sequences were expected to contribute significantly.

The potentially dominant sequences were examined more closely to ensure that the probabilities chosen were as accurate as they could be and to develop better human error rate estimates. The potential for recovery actions which could terminate the sequence was evaluated in a rough manner. These more refined calculations resulted in a list of dominant accident sequences.

2.2.7 Containment Analysis

Each potential dominant accident sequence was evaluated by Battelle Columbus Laboratories to determine the expected mechanism of containment failure, the associated probability of failure, and to characterize the potential radioactive release. This analysis was quite limited in nature, relying primarily on insights developed from similar analyses in the past, but supplemented by further calculations where necessary.

2.2.8 Interpretation and Analysis of Results

The dominant accident sequences in terms of risk (the highest frequency sequences in the most severe release categories) were examined to draw engineering insights of interest from the analysis. Those plant features contributing most significantly to risk were identified. These constitute the principal results of the study. Limited uncertainty and sensitivity analyses were performed to ascertain a rough estimate of uncertainty in results and to identify assumptions which, if changed, could significantly alter the results.

CHAPTER 3

PLANT DESIGN

3.1 General

The Arkansas Nuclear One Unit-1 (ANO-1) nuclear power plant is an 886 MWe pressurized water reactor (PWR) located on Lake Dardanelle near Russelville, Arkansas. Arkansas Power and Light Company owns and operates the facility. ANO-1 entered commercial operation on December 19, 1974.

The reactor vendor for ANO-1 is Babcock and Wilcox (B&W). The architectural engineer is Bechtel Power Corporation. The design of the reactor coolant system is typical of other B&W plants currently in commercial operation; there are two once-through steam generators and four reactor coolant pump loops. Most of the major safety systems designs are also fairly typical. The ANO systems studied in the IREP along with some major design highlights are given in Table 3-1. More detailed discussions of these systems are presented in Chapter 6 and Appendix B.

3.2 ANO-1 Plant Functions/Systems

The systems presented in Table 3-1 perform one or more plant safety functions. The safety functions of concern in the IREP are those that are required to either successfully mitigate a LOCA or transient (i.e., requirement for reactor shutdown not caused by a LOCA), or lessen the consequences of a core melt if mitigation of the LOCA or transient is unsuccessful. These safety functions and the systems which perform them will now be discussed.

Table 3-1

Systems Studied in the ANO-1 IREP Analysis

ANO System	Design Highlights
° High Pressure System	° 3 pumps (2900 psi shutoff head) ° Injects into 4 RCS cold legs ° Actuates upon RCS pressure of 1500 psi or containment pressure of 4 psig
° Low Pressure System	° 2 pump trains (190 psi shutoff head) ° Injects into reactor vessel via 2 low pressure injection lines ° Actuates upon RCS pressure of 1500 psi or containment pressure of 4 psig
° Core Flood System	° 2 tank trains ° Injects into reactor vessel via 2 low pressure injection lines ° Actuates upon RCS pressure of 600 psi
° Reactor Building Cooling System	° 4 containment fan coolers ° Actuates upon containment pressure of 4 psig
° Reactor Building Spray System	° 2 pump trains ° Sprays containment atmosphere via 2 spray headers ° Actuates upon containment pressure of 30 psig
° Emergency Feedwater System/Emergency Feedwater Initiation and Control System	° 2 pumps (1 electric, 1 turbine ° Injects into both, once through steam generators ° Actuates on reactor coolant pump trip, main feed pump trip, low steam generator level, low steam generator pressure ° Design upgrade complete in 1982
° Power Conversion System	° 6 pumps (3 electric condensate, 2 steam main feed, 1 auxiliary feed) ° Normal post-trip steam generator cooling system

Table 3-1 (Cont.)

ANO System	Design Highlights
° Reactor Protection System	° 7 shutdown rod groups ° 10 automatic scrams initiated upon a variety of high and low RCS pressure and/or temperature signals, overpower, reactor coolant pump status, power/flow imbalance, high containment pressure, loss of main feedwater turbine trip
° AC Power System	° 2 load divisions ° 2 4160 V emergency diesel generators ° Several bus interties
° DC Power System	° 2 load divisions ° 2 125V batteries ° Limited bus interties
° Engineered Safeguards Actuation System	° Actuates high pressure system, low pressure system, reactor building cooling system, and several support system components. ° 10 actuation channels ° 2 out of 3 logic actuates upon 4 psig/30 psig containment pressure or 1500 psig RCS pressure
° Service Water System	° 3 pumps/2 pump trains ° Provides required support system cooling for high pressure system, low pressure system, spray system, reactor building cooling system, HVAC room cooling, diesel generator cooling
° Heating, Ventilation, Air Conditioning Systems (HVAC)	° Required for high pressure, low pressure, spray pump rooms ° Required for AC and DC switchgear rooms
° Pressurizer Relief Valves	° 2 code safety relief valves (both open at 2500 psig) ° 1 electromatic relief valve (opens at 2450 psig)

Table 3-1 (Cont.)

ANO System	Design Highlights
°Integrated Control System	° Controls proper coordination between reactor, steam generators, main feedwater, and turbine during normal operation ° Recent design upgrade has essentially eliminated ICS caused failures of safety systems
° Instrument Air	° Several non-safety systems require instrument air for proper operation ° Safety related components fail safe upon loss of instrument air
° Non-Nuclear Instrumentation Power	° 2 load divisions; NNI-X NNI-Y ° Provides power to much safety related instrumentation in control room ° Recent design upgrade has essentially eliminated single NNI caused failures of safety systems ° NNI-X or NNI-Y can be lost with sufficient instrumentation available to shut down the plant.

3.2.1 ANO LOCA Functions/Front Line Systems

Upon review of the ANO-1 FSAR,[7] it was noted that in response to a LOCA, the safety systems perform the following functions:

A) reactor subcriticality

B1) emergency core cooling during the injection phase

B2) emergency core cooling during the recirculation phase

C1) containment overpressure protection during the injection phase

C2) containment overpressure protection during the recirculation phase

D1) radioactivity removal during the injection phase

D2) radioactivity removal during the recirculation phase.

The ANO-1 safety systems which directly perform these LOCA functions are presented in Table 3-2. These systems are defined as "LOCA front line systems." This table will now be discussed.

The reactor protection system (RPS) performs the function of reactor subcriticality by inserting shutdown rods into the core immediately following a LOCA signal. Reactor subcriticality must be performed to lower the core power output to the decay heat level. At this level emergency core cooling systems have an adequate capacity to prevent core melting.

The core flooding system (CFS), high pressure injection system (HPIS), low pressure injection system (LPIS), emergency feedwater system (EFS) and the pressurizer

Table 3-2

ANO-1 LOCA Function/System Index

LOCA Function	System(s)
Reactor Subcriticality	Reactor Protection System (RPS)
Emergency Core Cooling During Injection Phase	a) Core Flooding System (CFS)
	b) HPIS
	c) Low Pressure Injection System (LPIS)
	d) Emergency Feedwater System (EFS)
	e) Pressurizer Code Safety Relief Valves (SRVs)
Emergency Core Cooling During Recirculation Phase	a) High Pressure Recirculation System (HPRS)
	b) Low Pressure Recirculation System (LPRS)
	c) Decay Heat Removal System (DHRS)
Containment Over-pressure Protection During Injection Phase	a) Reactor Building Cooling System (RBCS)
	b) Reactor Building Spray Injection System (RBSI)
Containment Over-pressure Protection During Recirculation Phase	a) RBCS
	b) Reactor Building Spray Recirculaton System/Low Pressure Recirculation System (RBSR/LPRS)
Radioactivity Removal During Injection Phase	RBSI
Radioactivity Removal During Recirculation Phase	RBSR

code safety relief valves (SRVs) comprise the systems which perform the function of emergency core cooling during the injection phase. (Referring to Table 3-1, it can be noted that the pressurizer contains two SRVs and one electromatic relief valve (ERV). Due to leakage, the plant has effectively disabled the ERV by closing its block valve. Operation of the ERV was therefore not analyzed in this study.) Emergency core cooling must be performed to prevent core melt. During the injection phase, water is pumped from the borated water storage tank (BWST) by the HPIS and LPIS into the reactor vessel. For intermediate to large LOCAs, the HPIS, LPIS and CFS operate together to keep the core cool. As the reactor coolant system (RCS) depressurizes, the HPIS automatically actuates at 1500 psi, the LPIS at 1500 psi (the pumps are started at 1500 psi, but injection does not occur until 190 psi), and the CFS at 600 psi. For small LOCAs, the HPIS, EFS and pressurizer SRVs operate together to keep the core cool. (The RCS pressure is too high to allow use of the CFS and LPIS for small LOCAs.) The HPIS automatically actuates at 1500 psi. The EFS and pressurizer SRVs operate to reduce RCS pressure so that the HPIS may inject more cooling water into the core. The EFS reduces RCS pressure by removing decay heat through the steam generators. RCS pressure is also reduced by relieving decay heat through the pressurizer SRVs.

The decay heat removal system (DHRS), low pressure recirculation system (LPRS) and high pressure recirculation system (HPRS) comprise the systems which perform the function of emergency core cooling during the recirculation phase. The recirculation phase begins when the suction of the high pressure and low pressure pumps are

realigned to draw from either the containment sump or the RCS. This phase begins prior to emptying the BWST. For very small LOCAs, the RCS can be depressurized and the break effectively isolated before emptying the BWST. This allows the DHRS to be implemented (the DHRS is the low pressure pumps taking suction from the RCS). For somewhat larger breaks, the RCS cannot be depressurized before emptying the BWST. Because of this, the HPRS must be implemented to take suction from the containment sump. For intermediate to large breaks the RCS depressurizes, the BWST empties and the LPRS is utilized (the LPRS is the low pressure pumps taking suction from the containment sump). The DHRS cannot be implemented for these latter breaks because the BWST empties fairly quickly and time is not available to perform the DHRS lineup.

During the emergency core cooling injection and sump recirculation phases, steam emitted through the break will cause the containment pressure to increase. If the steam is not condensed, the containment would eventually fail due to overpressure within several hours. To prevent containment failure, ANO-1 employs fan cooler (RBCS) and containment spray systems (RBSI and RBSR) to condense the steam and perform the function of containment overpressure protection from steam evolution. The RBCS actuates at 4 psig and condenses steam by rejecting heat contained within the containment atmosphere to the environment via heat exchangers. During the injection phase, the RBSI actuates at 30 psig and condenses steam by spraying the containment atmosphere with cool water from the BWST. During the sump recirculation phase, steam is condensed via the RBSR by spraying the containment atmosphere with sump water which is cooled by mixing with the LPRS flow. The LPRS

flow is cooled by service water heat exchangers located within its pump trains.

If successful mitigation of the LOCA cannot be achieved and a core melt ensues, the consequences of the accident can be reduced if the functions of containment overpressure protection and radioactivity removal are performed.

The ANO systems described above (i.e., RBIS, RBCS, and RBSR/LPRS) which prevent a containment overpressure failure following a LOCA can also prevent or delay a post-core-melt overpressure failure during both the injection and sump recirculation phases. Success of this function would depressurize the portion of the containment pressure due to steam by condensing it. The ANO systems which perform this function, however, do not significantly reduce the portion of the containment pressure due to the non-condensable gases released during the meltdown. This function will therefore prevent a post-core meltdown overpressure only if a containment basemat meltthrough occurs (i.e., relieves pressure through the ground) prior to an overpressure due to non-condensables.

A post-core melt radioactive material release to the environment can be substantially reduced if the function of radioactivity removal is successful. At ANO-1 the RBSI and RBSR performs this function by scrubbing the containment atmosphere of radioactive materials during both the injection and sump recirculation phases.

3.2.2 ANO Transient Functions/Front Line Systems

Upon review of the ANO-1 FSAR (Reference 7), it was noted that in response to a transient, the safety systems perform the following functions:

A) reactor subcriticality

B) core cooling

C) RCS overpressure protection/RCS integrity

D) RCS inventory makeup

E) containment overpressure protection

F) radioactivity removal

The ANO-1 safety systems which directly perform these transient functions are presented in Table 3-3. These systems are defined as "transient front line systems." This table will now be discussed.

The RPS performs the function of reactor subcriticality by inserting shutdown rods into the core immediately following a SCRAM signal. Reactor subcriticality must be performed to lower the core power to the decay heat level. At this level core cooling systems have an adequate capacity to prevent core melting. The RPS must also operate to prevent a potentially severe RCS overpressure transient. (Reference 1 states that peak RCS pressures in the neighborhood of 4,000 psi may occur given certain transients in which the RPS fails.) If the RPS fails and the RCS components survive the overpressure transient, reactor subcriticality can also be achieved by injecting borated water from the BWST into the RCS via the HPIS.

After achieving reactor subcriticality the core must be kept cool by removing decay heat from the RCS. This is normally accomplished at ANO by delivering feedwater to the steam generators from the power conversion system (PCS) at a rate commensurate with decay heat and boiling off of this water to the condenser or to the atmosphere via the secondary safety/relief valves. If, however, the

Table 3-3

ANO-1 Transient Function/System Index

Transient Function	System(s)
Reactor Subcriticality	a) Reactor Protection System (RPS) b) High Pressure Injection System (HPIS)[1]
Core Cooling	a) Power Conversion System (PCS) b) Emergency Feedwater System (EFS) c) High Pressure Injection System (HPIS) & Pressurizer Code Safety Relief Valves (SRVs)
Reactor Coolant System (RCS) Overpressure Protection/RCS Integrity	SRVs
RCS Inventory Makeup	HPIS
Radioactivity Removal	Reactor Building Spray System (RBSI)
Containment Overpressure Protection	a) RBSI b) Reactor Building Cooling System (RBCS)

1. HPIS may only perform reactor subcriticality if the RCS components survive the overpressure transient following RPS failure.

shutdown involves a loss of the PCS, backup decay heat removal systems may be utilized. The first backup system is the EFS, which automatically actuates given loss of the PCS. This system also removes decay heat by delivering feedwater to the steam generators. If the EFS is unavailable, decay heat may also be removed directly from the RCS. This may be accomplished via a "feed and bleed" operation. Success of this method requires the operator to establish flow from the HPIS. The core is cooled by boiloff of the RCS water into the containment via the SRVs.

For those reactor shutdowns in which the RPS immediately scrams the reactor, and core cooling via the steam generators is achieved within a few 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 a delay in steam generator cooling or a failure of the RPS, the operability of one or both of the pressurizer SRVs would be required to prevent a potential rupture of the RCS. The SRVs that open as a result of the transient must all reclose to insure the integrity of the RCS. Otherwise, a valve sticking open following the transient would result in a small LOCA.

Success of the RCS integrity function mentioned above will prevent a small LOCA. Even though a small LOCA has been prevented, however, a potential still exists for slowly losing RCS inventory via various smaller leaks. In order to prevent an eventual core uncovery within several hours, the function of RCS inventory makeup (RCSIM) is provided by adding makeup from the BWST via the HPIS.

(Reactor coolant pump seal leaks due to loss of seal cooling and technical specification allowed leakage are the most likely sources. Reference 17 indicates that core uncovery due to technical specification leaks takes greater than 60 hours. This should be more than ample time to restore the HPIS if it is initially unavailable. RCSIM is therefore assumed to be required following reactor coolant pump seal leaks only.)

The functions discussed thus far are those required to bring the plant to a safe shutdown condition if the systems providing core cooling are the PCS and EFS. If, however, "feed and bleed" core cooling via the HPIS is utilized, decay heat is dumped to the containment and additional systems are required to provide the function of containment overpressure protection. The ANO-1 systems which provide this function are the RBCS and RBSI. Operation of these systems was described previously for LOCAs.

If successful mitigation of the transient cannot be achieved and a core melt ensues, the functions of containment overpressure protection and radioactivity removal can aid in lessening the consequences of the accident. Containment overpressure protection is provided by the RBCS and RBSI as mentioned above. Radioactivity removal is provided by the RBSI. Operation of these systems was described previously for LOCAs.

3.3 ANO-1 Support Systems

It should be noted that successful operation of the LOCA and transient front line systems may require the operability of one or more support systems. Table 3-4 depicts the front line systems and the support systems upon which they depend. In many instances successful

Table 3-4

ANO-1 Front Line vs. Support Systems Dependencies (Read Across)

Front Line Systems / Support Systems	Offsite AC Power	Diesel AC Generators	125V DC Power	Engineered Safeguards Actuation System	Emergency Feedwater Initiation and Control System	Service Water System	Instrument Air System	Integrated Control System	Intermediate Cooling System	AC Switchgear Room Cooling	DC Switchgear Room Cooling	High Pressure Pump Room Cooling	Low Pressure/Spray Pump Room Cooling	Non-Nuclear Instrumentation Power
Reactor Protection System														
Core Flood System														
High Pressure Injection/ Recirculation	✓	✓	✓	✓		✓				✓	✓	✓		
Low Pressure Injection/ Recirculation Decay Heat Removal	✓	✓	✓	✓		✓				✓	✓		✓	
Reactor Building Spray Injection/Recirculation	✓	✓	✓	✓		✓				✓	✓		✓	
Reactor Building Cooling System	✓	✓	✓	✓		✓				✓	✓			
Power Conversion System	✓		✓		✓	✓	✓	✓	✓	✓	✓			✓
Emergency Feedwater System	✓	✓	✓		✓	✓				✓	✓			
Pressurizer Safety Relief Valves														

Note: All requirements for diesel generators assume loss of station power.

operation of ANO-1 support systems requires the operability of other support systems. Table 3-5 depicts support system interdependencies. Chapter 6 and Appendix B discuss the role of these support systems in detail.

A thorough understanding of front line system/support system and support system/support system interdependencies is fundamental to the study of reactor accidents. Nuclear industry operating experience has indicated that some of the more severe accidents have originated from failures originating in support systems. The reason for this is twofold. Firstly, since support systems are common to several front line systems, the reliability of several front line systems can be degraded due to single support system failures. Secondly, certain support system failures not only degrade several front line systems but can simultaneously cause a reactor trip which requires these front line systems to operate. Identification of these second type of support system failures, which are also transient initiating events, is described in Chapter 4.

Table 3-5

ANO-1 Support vs. Support Systems Dependencies (Read Across)

Support Systems	Offsite AC Power	Diesel AC Generators	125V DC Power	Engineered Safeguards Actuation System	Emergency Feedwater Initiation and Control System	Service Water System	Instrument Air System	Integrated Control System	Intermediate Cooling System	AC Switchgear Room Cooling	DC Switchgear Room Cooling	High Pressure Pump Room Cooling	Low Pressure/Spray Pump Room Cooling	Non-Nuclear Instrumentation Power
Offsite AC Power	X													
Diesel AC Generators		X	✓	✓		✓				✓	✓			
125V DC Power	✓	✓	X					✓			✓			
Engineered Safeguards Actuation System	✓	✓	✓	X						✓				
Emergency Feedwater Initiation and Control System	✓	✓	✓		X					✓	✓			
Service Water System	✓	✓	✓	✓		X				✓	✓			
Instrument Air System	✓		✓			✓	X		✓	✓				
Integrated Control System	✓	✓	✓					X		✓	✓			
Intermediate Cooling System	✓		✓	✓		✓			X	✓	✓			
AC Switchgear Room Cooling	✓	✓				✓				X				
DC Switchgear Room Cooling	✓	✓				✓				✓	X			
High Pressure Pump Room Cooling	✓	✓		✓		✓				✓		X		
Low Pressure/Spray Pump Room Cooling	✓	✓		✓		✓				✓			X	
Non-Nuclear Instrumentation Power	✓	✓	✓								✓			X

CHAPTER 4

INITIATING EVENTS

4.1 Introduction

The use of event tree methodology in the probabilistic risk assessment of ANO-1 requires that accident initiating events be defined. These initiating events represent the starting points of many different accident sequences and delineate the initial conditions for these sequences.

This chapter describes which initiating events were chosen for the ANO-1 analysis, how they were grouped, and how they were quantified. The end product of the chapter is a list of the ANO-1 initiating events and is described in Section 4.3.

4.2 Initiating Events Chosen for ANO-1

Two general types of initiating events have been considered for the ANO-1 analysis: loss of coolant accidents (LOCAs) and transients.

In order to determine the specific types of LOCA and transient initiating events to be studied, a failure mode and effects analysis (FMEA) was performed on the RCS piping and front line systems and their support subsystems which are operating when the reactor is at power.

The RCS FMEA consisted of postulating different size RCS breaks and break locations to determine if different combinations of plant systems were required to mitigate the LOCA. Those breaks with similar front line system mitigating requirements were placed in the same group. As a result, LOCAs at ANO-1 were divided into six categories ranging from small pump seal ruptures to large

RCS pipe breaks. The LOCA initiating events for ANO-1 are described in Section 4.2.1.

The FMEA performed to identify transients consisted of postulating a single fault in a normally operating system or subsystem and studying the plant response to that fault. For each postulated fault, the following questions were asked:

1. Does the fault lead to a reactor trip?
2. If the reactor trips, is the reliability of the front line systems and their support systems which must respond to the trip affected? If so, how?

Throughout the FMEA, generic transient information presented in EPRI-NP801, "Frequency of Anticipated Transients,"[4] and plant specific information presented in licensee event reports and trip logs provided guidance in choosing the general types of system faults to be considered.

A fault was only considered to be important if the answer to the first question was yes. If the reactor did not trip, it was assumed that the fault would be detected and corrected before a reactor trip from some other cause occurred. The faults that did cause a reactor trip were then grouped. Those which affected the reliability of the systems in a similar manner were placed in the same group. As a result, ANO-1 transients were split into eight groups. Some of these groups were loss of offsite power, loss of the power conversion system, loss of AC or DC power to a particular bus, loss of service water, etc. The ANO-1 transient initiating events are described in Section 4.2.2.

4.2.1 LOCA Initiating Events

A number of LOCA break size ranges were determined for ANO-1. Each LOCA break size range defines a unique set of emergency core cooling requirements for the injection or recirculation phase of a loss of coolant accident. Table 4-1 presents the different LOCA sizes and the appropriate success criteria for various plant functions. The emergency core cooling success criteria were determined by Babcock and Wilcox.[6] The criteria used for the other functions were obtained from previous calculations made by Battelle Columbus Laboratories, the Final Safety Analysis Report for ANO-1, or other B&W studies.[2,6,7,8]

The initiating event frequencies for each LOCA break size range were calculated using Reactor Safety Study data. Two basic assumptions were made in the calculation of the ANO-1 LOCA frequencies. The first assumption was that the total frequency of random LOCAs at ANO-1 was the same as that identified for the RSS plants. It was also assumed that the probability distribution over each RSS break range was constant. This assumption allowed constant probability functions to be generated for each RSS LOCA break size range. These probability functions were then integrated over the ANO-1 break ranges to produce ANO-1 specific LOCA initiating event frequencies. The RSS and ANO-1 LOCA break size ranges, frequencies and an example calculation, are given in Table 4-2.

One ANO-1 LOCA break size range has an additional initiating event frequency contribution that is not included in the RSS data. For the smallest ANO-1 LOCA break range (.38 to 1.2 inches equivalent diameter), a .02 frequency was assessed for certain types of reactor

Table 4-1

LOCA Success Criteria

LOCA Size	Reactor Subcriticality	INJECTION PHASE			RECIRCULATION PHASE		
		Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Emergency Core Cooling	Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Emergency Core Cooling
7.9E-4 - .008 ft^2 .38" - 1.2"D Stuck Open ERV = .0056 ft^2 Max. Recorded RCP Seal Failure .0035 ft^2	> 6 Control Rod Groups Inserted Into the Core by the Reactor Protection System (RPS)*	1/2 Reactor Bldg. Spray Injection (RBSI) OR 1/4 Reactor Bldg. Fan Coolers (RBCS)	1/2 RBSI	1/3 High Pressure Injection (HPIS) and 1/2 Safety/Relief Valves (SRV) OR 1/3 HPIS and 1/2 Emergency Feedwater (EFS)	1/2 Reactor Bldg. Spray Recirc. (RBSR) and Sump Mixing With 1/3 HPRS and 1/2 LPRS Heat Exchanger OR 1/4 RBCS	1/2 RBSR	1/3 High Pressure Recirc. (HPRS) and 1/2 LPRS Heat Exchanger OR 1/2 EFS (During Injection Phase) & 1/2 Decay Heat Removal System
.008 - .015 ft^2 1.2 - 1.66"D Stuck Open P_z Safety .0145 ft^2				2/3 HPIS and 1/2 SRV OR 1/3 HPIS and 1/2 EFS			1/3 HRPS and 1/2 LPRS Heat Exchanger
.015 - .087 ft^2 1.66 - 4"D				1/3 HPIS			
.087 - .55 ft^2 4 - 10"D				1/3 HPIS and 1/2 Low Pressure Injection (LPIS)	1/2 RBSR and Sump Mixing With 1/2 LPRS Heat Exchanger OR 1/4 RBCS		1/2 Low Pressure Recirc. (LPRS)
.55 - 1.0 ft^2 10 - 13.5"D	No System Needed			1/2 LPIS and 1/2 Core Flood Tanks (CFT)			
>1 ft^2 >13.5"D				1/2 LPIS and 2/2 CFT			

*The HPIS can perform reactor subcriticality by injecting borated water in the event of RPS failure. However, since operation of the HPIS cannot prevent the pressure transient associated with RPS failure, the HPIS should not be considered a reactor subcriticality fron line system.

**The ECC success criteria shown assumes either the operator trips the RCPs shortly after an ES signal or the operator never trips the RCPs. If the pumps are tripped at some intermediate point, Babcock and Wilcox could not provide an ECC success criteria.

Table 4-2

Comparison of RSS and ANO-1
LOCA Frequencies

Reactor Safety Study		Arkansas Nuclear One Unit 1	
LOCA Break[1] Size Range	Frequency	LOCA break[1] Size Range	Frequency
		B(1.2) = .38 to 1.2 inches	2.0×10^{-2}
S_2 = .5 to 2 inches	1.0×10^{-3}	B(1.66) = 1.2 to 1.66 inches	3.1×10^{-4}
		B(4) = 1.66 to 4 inches	3.8×10^{-4}
S_1 = 2 to 6 inches	3.0×10^{-4}	B(10) = 4 to 10 inches	1.6×10^{-4}
A = 6 inches and larger	1.0×10^{-4}	B(13.5) = 10 to 13.5 inches	1.2×10^{-5}
		B(>13.5) = greater than 13.5 inches	7.5×10^{-5}

[1]Equivalent diameter in inches.

Sample Calculation

$$\text{For RSS } S_2\text{LOCA, } \int_{.5}^{2} P_{S2}\,dx = 1.0 \times 10^{-3}$$

Assume P_{S2} is a constant probability distribution. Therefore, $P_{S2} = 6.67 \times 10^{-4}$. Now, integrate this distribution over ANO-1's B(1.66) LOCA break size range to obtain B(1.66) frequency.

$$\int_{1.2}^{1.66} P_{S2}\,dx = 3.1 \times 10^{-4}.$$

coolant pump seal ruptures. The RSS data only includes data on random pipe failures and therefore does not cover this type of LOCA. The .02 number overshadows the random failure contribution for this break size range. The pump seal information was obtained from an NRC memo on the subject.[9] Note that no LOCAs smaller than .38 inch equivalent diameter were analyzed. It was ascertained that breaks of this magnitude could be mitigated by normally operating makeup systems.

A final comment should be made concerning the LOCA initiating events analyzed for ANO-1. The interfacing systems LOCA, which was found to be important to risk in other PRAs (e.g., Surry in the RSS and Oconee in the RSSMAP,[2]) was not found to be significant at ANO-1.

One type of interfacing systems LOCA at ANO would require failure of two series check valves in one of the low pressure injection lines and 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 RCS water to enter the low pressure piping outside containment and pipe rupture to occur. A core melt would ensue because the core cooling system is not designed to mitigate a LOCA outside containment. Since all low pressure injection series check valves are required to be leak tested on a regular basis (e.g., following cold shutdown operations, etc.) via procedure 1102.01, the frequency of this event is dominated by undetected rupture of the series check valves. Reference 2 indicates that this frequency is small (less than 10^{-6}/Ryr). This type of interfacing system LOCA was therefore not considered as a separate initiating event.

Another type of interfacing systems LOCA could be postulated at the low pressure pump suction line from the RCS. An extra containment LOCA at this locality would require the simultaneous opening or rupture of two series MOVs. Failure of these valves is predicted to be probabilistically insignificant for the following reasons:

1. Each valve contains an independent interlock which prohibits the operator from opening them when the reactor is at high pressure.

2. If a valve spuriously opened, it would be detected within 8 hours since the position of these valves are verified closed via checklist every shift.

3. We could not find adequate data applicable to massive ruptures of MOVs and thus assume such failures are extremely rare.

For these reasons, this type of interfacing system LOCA was not considered as a separate initiating event.

4.2.2 Transient Initiating Events

A number of transient initiating events were identified for ANO-1. The success criteria for front line systems which function to mitigate transient initiated accidents are given in Table 4-3.

Three types of transient initiating events which do not involve specific component failures and which were quantified using industry data were analyzed for ANO-1. These are:

1. Loss of station power (designated T(LOP)).

2. Events which totally interrupt the power conversion system (T(PCS)).

Table 4-3

Transient Success Criteria

Subcriticality	Core Cooling	Reactor Coolant System (RCS) Overpressure Protection	RCS Integrity	RCS Inventory Makeup	Containment Overpressure Protection Due to Steam Evolution	Post-Accident Radioactivity Removal
> 6 Control Rod Groups Inserted Into Core by the Reactor Protection System (RPS)	Given RPS Success Power Conversion System (PCS) OR 1/2 Emergency Feedwater System (EFS) OR 1/3 High Pressure Injection System (HPIS) and 1/3 Safety/PORV Valves Open Given RPS Failure PCS and HPIS and 2/2 Safety Relief Valves Open OR EFS and HPIS and 2/2 Safety Relief Valves Open	Given RPS Success 1/2 Safety Relief Valves Open When Demanded Given RPS Failure 2/2 Safety Relief Valves Open	All Safety/PORV Relief Valves Reseat After Opening	1/3 HPIS	1/4 Reactor Building Cooling System Fan Coolers OR 1/2 Reactor Building Spray Injection System	1/2 Reactor Building Spray Injection System

3. All other transient initiating events which do not affect the front line systems significantly (T(FIA)).

The sources used to define and quantify these transient initiators were plant specific information from the utility and EPRI NP-801.[4] A list of the transient categories defined in the EPRI document is given in Table 4-4. Also shown are the calculated transient event frequencies using updated EPRI data and certain ANO-1 information on the plant response to different transients. Table 4-5 shows which EPRI transient categories were grouped together to produce the three transient types listed above.

A number of normally operating support systems components were found at ANO-1 whose failure would cause a reactor shutdown and somehow degrade safety systems required post trip or affect recovery actions. These component failures were identified via performance of the FMEA (described in Section 4.2) on all normally operating support systems. The normally operating support systems are a subset of the support systems presented in Tables 3-4 and 3-5 and are listed inTable 4-6.

In the following sections, the normally operating support systems which were reviewed in-depth are discussed. The components identified as possible initiating events are included in the list of initiating events described in Section 4.3

4.2.2.1 Service Water System Analysis

The Service Water System (SWS) at ANO-1 is a two train, three pump system which supplies cooling water to

Table 4-5

Grouped EPRI NP-801 Transient Initiating Events
Requiring an Immediate Rapid Reactor Shutdown
at ANO-1

Transient Designator	Description	EPRI NP-801 Transients	Total Frequency (Per Ryr)
T(LOP)	Loss of offsite power	35	.32
T(PCS)	Total interruption of the Power Conversion System (main feedwater)	16, 17[1], 18, 20, 21, 22, 24, 25, 29, 30	1.0
T(FIA)	All other transients which do not affect front line systems significantly	1, 2, 3, 6, 10, 14, 15, 17[1], 33, 34, 37, 38, 39, 23	7.1

[1]One feedwater pump will be lost on a MSIV closure of one steam generator loop. Both feedwater pumps could be lost depending on the position of a trip selector switch in the control room. Therefore, since it is a 50-50 chance of losing both pumps, half of #17's frequency falls in T(PCS) and half in T(FIA).

Table 4-6

Support Systems Reviewed in the ANO-1
Initiating Event Analysis

The following systems were reviewed to identify possible failures which could act as an accident initiator:

Service Water System

AC Power System

DC Power System

Instrument Air System

Integrated Control System

Non-Nuclear Instrumentation

Heating, Venting, and Air Conditioning System

Emergency Feedwater Instrumentation and Control System

Engineered Safeguards Activation System

many safety and nonsafety systems. (Refer to SWS discussion in Section 6.3.2 and Appendix B10.)

One failure in this system was identified as a possible initiating event. There is a normally open, motor-operated valve (CV-3824) in the single discharge line which is common to both service water trains. If this valve should fail and obstruct the discharge line during normal operation, SWS flow to most safety system components would be severely degraded or interrupted. Discussions with utility personnel and a review of plant procedures indicate that given failure of CV-3824, a plant trip could be expected due to a trip of the reactor

coolant pumps following loss of pump cooling. Given a loss of all service water, many safe shutdown systems would be unavailable.

The initiating event frequency for this service water failure was taken from the IREP quantification guide. A frequency of 2.6×10^{-3} per reactor year was assessed for this fault based on the plug standby failure rate for motor-operated valves over a year period (i.e., 3×10^{-7} x 8760 hours). It is acknowledged that an operating failure rate rather than a standby failure rate should be used and may be different than the assigned value. No operating failure rate was available; however, it was felt that value used represents an upper bound to the real value. The initiating event representation used in the analysis for this SWS fault is T(LOSW).

4.2.2.2 Vital AC Power Bus Analysis

The Vital AC Power System provides AC power to several front line/support systems which may be required to operate after an initiating event. (Refer to AC power discussion in Section 6.3.3 and Appendix B11.)

A FMEA was performed on each vital AC bus to determine the effects of the bus shorting to ground. Only two AC buses were identified which would cause a reactor trip and degrade front line systems if lost. These are AC buses, A3 (4160 VAC) and B5 (480 VAC).

In terms of the initial severity of the bus failure, failure of bus A3 is worse than B5 since bus A3 feeds bus B5. However, in terms of recovery potential, failure of the 4160 volt A3 bus is much different than the failure of the 480 volt B5 bus. This is due to a cross-tie between buses B5 and B6. This cross-tie provides good recovery

potential if bus A3 shorts to ground. This recovery potential is lost, however, if bus B5 fails.

The initiating event frequencies for these initiating events were obtained from a data base developed for the Oconee PRA.[1] The initiating event representations used in the analysis for these AC bus faults are T(A3), and T(B5).

4.2.2.3 Vital DC Power Bus Analysis

The analysis of the two main DC power buses (D01 and D02) was very similar to that done for the AC buses. Given a loss of one DC bus, it is expected that the following events will occur:

1. One steam generator will isolate.
2. The reactor will trip, mostly likely due to overpower.
3. The turbine and one feedwater pump will trip with a 50 percent chance that both feedwater pumps will trip.

Both of the DC power buses are included in the analysis as initiating events as these buses supply power to various safety related components. The initiating event frequencies for DC bus failure were also obtained from NSAC data generated for the Oconee PRA. The initiating event representations used in the analysis for these DC bus faults are T(D01) and T(D02). Refer to Section 6.3.4 and Appendix B12.

---

[1]Telephone conversation with G. J. Boyd, Technology for Energy Corporation.

4.2.2.4 Instrument Air System Analysis

The instrument air system (IAS) provides process air to many plant components, mainly air-operated control valves. The analysis uncovered that the only front line or support system which would degrade or fail on loss of the IAS is the power conversion system. The reason for this is that most safety system components which interface with the IAS fail safe on loss of instrument air. Loss of the IAS would probably not cause an immediate reactor trip; the operator would lose control of main feedwater and eventually be forced to trip the system. Since instrument air only affects main feedwater, its failure was considered as part of the T(PCS) initiating event. For this reason, no instrument air faults were analyzed as specific initiating events.

4.2.2.5 Integrated Control System and Non-Nuclear Instrumentation Analysis

The integrated control system (ICS) at ANO-1 provides the proper coordination of the reactor, steam generators, main feedwater control, and turbine under all operating conditions. Two non-nuclear instrumentation buses (NNI-X and NNI-Y) are utilized at the plant to supply power to various valve control circuits and instrumentation channels. Many instrumentation signals generated by NNI are used by the ICS.

In order to determine the effect of ICS and NNI failures on other ANO-1 systems, a review of past incidents was undertaken to identify general types of failures and interactions that have occurred. Also, the results of a B&W analysis of the ICS were studied.(11) The knowledge and insights gained from these sources were used to determine potential ICS/NNI initiating events at ANO-1.

The B&W analysis consisted of a failure modes and effects analysis (FMEA) of an ICS and a review of operating experiences. Appropriate conclusions for each part are given below.

Conclusions drawn from the FMEA are as follows:

1. ICS failures could cause an inadvertantly opened or stuck open turbine bypass valve or feedwater startup valve which could result in overcooling.

2. ICS failures do exist that would result in a reactor trip main feedwater trip, and require additional safety systems to mitigate the failure.

Conclusions drawn from analyses of past transients are as follows:

1. ICS/NNI power supplies are vulnerable to single failures with significant consequences. Power supply failure or malfunction to or from the ICS/NNI was the only event found which could have caused loss of both main and emergency feedwater flow.

2. The ICS has shown a tendency to cause or to participate in feedwater oscillations, which have led to high reactor coolant trips, low reactor coolant trips, actuation of engineered safety systems, loss of main feedwater, and loss of emergency feedwater.

A more detailed review of specific incidents occurring at Rancho Seco, Oconee, Crystal River, and other plants revealed the following additional insights:

1. Each NNI bus supplies ± 24 V DC power to various components such as the PORV. Loss of one half of the ± 24 volt source has caused a PORV to open and remain open in one incident. A complete loss of the ± 24 volt source would not have caused the PORV to open at all.

2. Interactions were found between ICS failures and several emergency feedwater system valves. In at least one incident, emergency feedwater was lost completely for a time due to ICS/NNI problems.

3. Critical control room indication may be lost or undependable after ICS or NNI faults, particularly feedwater flow and steam generator level indication. The loss of control room indication has resulted in dryout of both steam generators and overfill conditions.

4. Loss of NNI or ICS power has caused depressurization of both steam generators. This led to isolation of main and emergency feedwater flow to both steam generators due to the design of the steam generator isolation logic.

The ANO-1 ICS and NNI have been reviewed for the possible interactions described above. In general, post-Crystal River design changes to the ICS, NNI, emergency feedwater system (EFS), and steam generator isolation logic have significantly reduced the probability and effect of such interactions. These design changes will now be discussed.

An EFS upgrade is being implemented at ANO-1 (Refer to Section 6.2.5). The new EFS will include safety grade control valve positioners, sensors, and control

and actuation circuits which are independent of the ICS and NNI. The EFS upgrade, due to be finished in 1982, is expected to eliminate the EFS/ICS interactions previously described.

Part of the EFS upgrade includes installation of a new control system known as the emergency feedwater initiation and control system (EFIC). The EFIC system performs multiple functions including EFS initiation, EFS control, and steam generator isolation upon low pressure or on approach to overfill conditions (Refer to EFIC disscussion in Section 6.3.6 and Appendix B14.) The EFIC system performs some control actions which were in the past performed by elements of the ICS, NNI and steam line break isolation and control system. (The latter system was the old steam generator isolation system.) A review of the preliminary EFIC design indicated that total isolation of emergency feedwater flow to the steam generators caused by single NNI, ICS, or EFIC power failures was not possible.

The ANO-1 NNI and ICS power supplies have also been upgraded in recent years. Each NNI and ICS bus has two separate power supplies each coming from a different bus. Failures of nonredundant power supplies have been identified as the cause of at least one past ICS/NNI incident.

Each ICS/NNI bus outputs through an auctioneered $\pm$ 24 volt DC supply. A power supply monitor is attached to each bus which monitors the two voltages. A loss of either voltage for .5 seconds will cause the monitor to trip breakers which will cut off both voltage supplies. This monitoring of the $\pm$ 24 V DC output sources of the ICS and NNI buses is expected to prevent or reduce

possible interactions between the ICS/NNI and components receiving power from the ICS/NNI.

To summarize, reviews of past incidents and industry analyses indicate that power faults have generally been the cause of ICS/NNI related events. The severity of the incidents can be increased due to possible interactions between the ICS/NNI and the EFS, pressurizer PORV, and other components. Availability of control room indication of various parameters given ICS/NNI problems has also been a concern.

The ICS and NNI design improvements at ANO-1 are expected to reduce or eliminate many of the problems discussed above. The increased redundancy of the ICS/NNI bus power supplies should significantly reduce the probability of a complete loss of power at a bus. The power supply monitors should prevent spurious or erroneous component actuation by ensuring that both 24 V DC output supplies are tripped when one is lost. Finally, the implementation of an independent EFS actuation and control system (EFIC) should eliminate observed ICS/EFS and NNI/EFS interactions. For these reasons, ICS and NNI failures were not considered as individual initiating events since they are expected to cause failure of the power conversion system only. These failures are therefore included as part of the T(PCS) initiating event.

4.2.2.6 Heating, Venting, and Air Conditioning System Analysis

The heating, venting, and air conditioning system (HVAC) at ANO-1 supplies room cooling for various plant systems. Room cooling is modeled explicitly in the fault trees for the two electrical switchgear rooms and the two battery rooms. (Refer to discussion of battery and

switchgear emergency cooling system in Section 6.3.5 and Appendix B13.) The HVAC system at ANO-1 has two safety grade trains, each of which cools one battery room and one switchgear room. In addition to these safety grade cooling trains, each room has a non-safety grade cooler. The non-safety grade room cooling is used during normal operation.

An analysis of the HVAC system indicates that during normal operation, it would take at least two failures to cause a complete loss of room cooling to the battery and switchgear rooms. Therefore, HVAC faults were not analyzed further as potential initiating events.

4.2.2.7 Emergency Feedwater Initiation and Control System (EFIC) Analysis

The EFIC is currently in the design stage. Because of this, not all information required to conduct a thorough initiating event analysis was available. We did, however, review available information and are able to make the following observations.

Besides performing the functions of startup and control of the emergency feedwater system (EFS), EFIC performs the function of steam generator isolation following steam generator depressurization and approach to overfill. Since main feedwater, as well as the EFS are isolated from the steam generators, we placed particular emphasis upon the postulation of faults which could simultaneously cause the reactor trip, main feedwater isolation and EFS isolation (i.e., these types of initiating events have occurred at other B&W plants, see Section 4.2.2.5). This fault postulation included power bus failures within the EFIC, NNI and ICS, as well as EFIC controller failures. While failures were identified which

could cause simultaneous reactor trip and main feedwater isolation, none were found which could cause sustained isolation of the EFS. The latter finding stems from the fact that the EFIC logic automatically bypasses EFS isolation signals when the need for the EFS exists (see Appendix B14). Since EFIC-related failures are only expected to cause failure of the power conversion system, they were not considered as individual initiating events. These failures are therefore included as part of the T(PCS) initiating event.

4.2.2.8 Engineered Safeguards Actuation System (ESAS) Analysis

The ESAS performs the function of safety system actuation following a low RCS pressure signal or high containment pressure signals. If these signals are inadvertently generated, or if other ESAS malfunctions occur, the HPIS would actuate, and ultimately lead to a reactor trip. (The HPIS could also inadvertently actuate after reactor trip.) This does not present a safety problem unless operation of the HPIS is allowed to continue until the pressurizer SRVs are demanded. If a valve fails to reclose an unisolatable LOCA would result. The frequency of a LOCA caused by an inadvertent HPIS actuation can be estimated as:

$$(8)(.02)(.015)(.04) + (.07)(.015)(.04) = 1.4\text{x}10^{-4}$$

where

8 = number of ANO RX trips/yr

.02 = probability an inadvertent actuation of the HPIS will occur <u>after</u> Rx trip[10]

.015 = probability the operator will not terminate HPIS before challenging the SRVs[10]

.04 = probability that one of two SRVs do not reclose

.07 = number of RX trips <u>caused by</u> an inadvertent HPIS actuation (Table 4-4, entry 9).

Since the value of 1.4×10^{-4} is about an order of magnitude smaller than other stuck open SRV LOCA sequences explicitly modeled, inadvertent HPIS actuation resulting from ESAS problems was not considered a separate initiating event.

4.3 Description of the ANO-1 Initiating Events

The accident initiating events used in the ANO-1 analysis are those discussed in the previous sections and are summarized in Table 4-7. When the initiating events are combined with the appropriate system fault and success trees, unique ANO-1 accident sequences are produced. An alternate way to display the ANO-1 initiating events is with a logic diagram. This is done in Figure 4-1.

The initiating events define the initial conditions for accident sequences and may, in themselves, affect the availability of front line systems. The dependencies found between the ANO-1 initiating events and the mitigating systems are shown in Tables 3-4 and 3-5.

Table 4-7

Initiating Events Used in the ANO-1 Analysis

Designator	Initiating Event Description	Frequency Per Reactor Year
B(1.2)	LOCA with a .38 to 1.2 inch equivalent diameter break	2.0×10^{-2}
B(1.66)	LOCA with a 1.2 to 1.66 inch equivalent diameter break	3.1×10^{-4}
B(4)	LOCA with a 1.66 to 4 inch equivalent diameter break	3.8×10^{-4}
B(10)	LOCA with a 4 to 10 inch equivalent diameter break	1.6×10^{-4}
B(13.5)	LOCA with a 10 to 13.5 inch equivalent diameter break	1.2×10^{-5}
B(>13.5)	LOCA with an equivalent diameter break greater than 13.5 inches	7.5×10^{-5}
T(LOP)	Loss of offsite power transient	3.2×10^{-1}
T(PCS)	Transient initiated by a total interruption of main feedwater	1.0
T(FIA)	All other transients which do not affect front line systems significantly	7.1
T(A3)	Transient initiated by a failure of AC power bus A3	3.5×10^{-2}
T(B5)	Transient initiated by a failure of AC power bus B5	3.5×10^{-2}
T(D01)	Transient initiated by a failure of DC power bus D01	1.8×10^{-2}
T(D02)	Transient initiated by a failure of DC power bus D02	1.8×10^{-2}
T(LOSW)	Transient initiated by failure of Service Water Valve CV-3824	2.6×10^{-3}

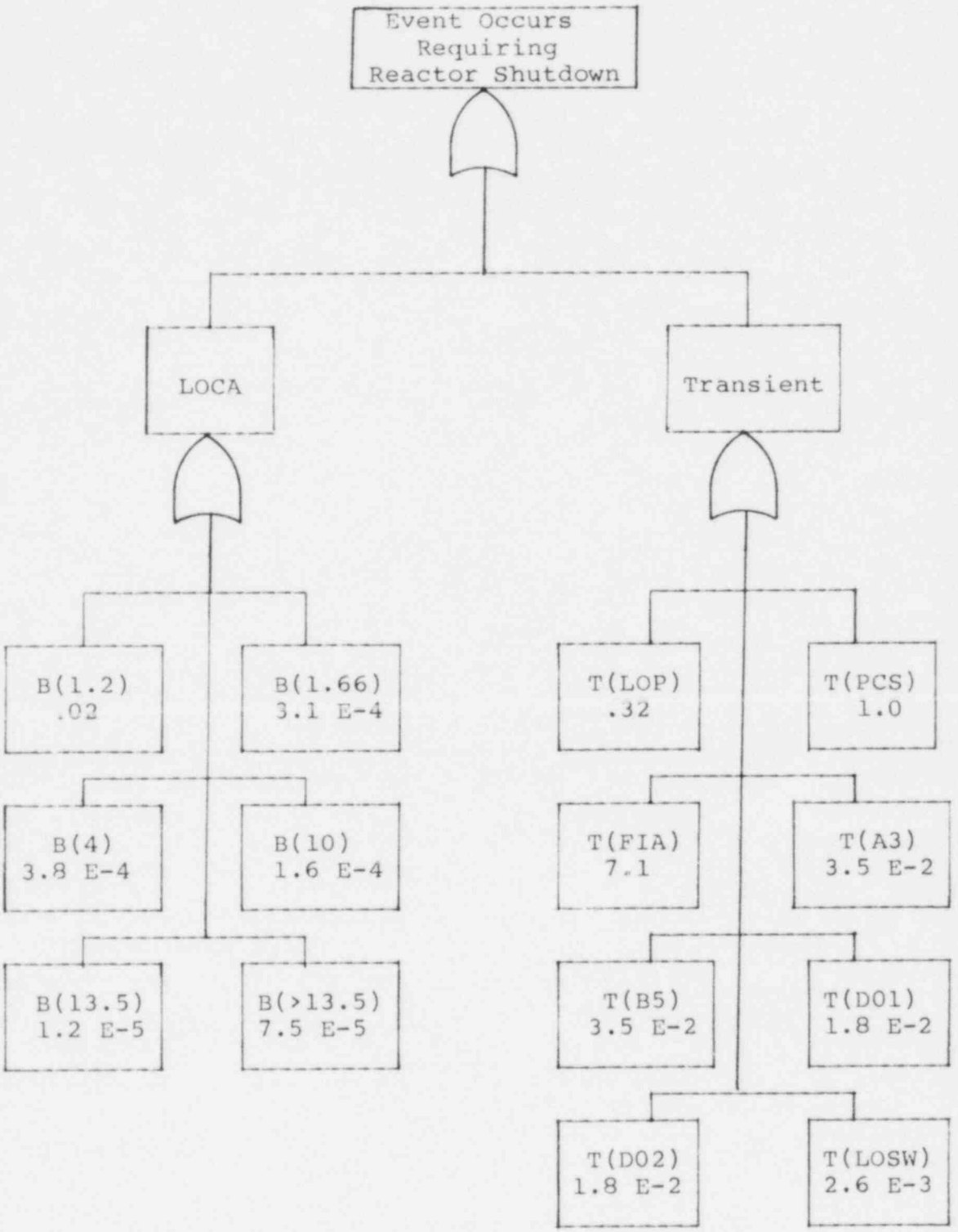


Figure 4-1. ANO Unit 1 Initiating Event Logic Diagram

CHAPTER 5

ACCIDENT SEQUENCE DELINEATION

5.1 Introduction

The type of reactor accidents of concern for the ANO-1 IREP study are core meltdown accidents initiated by the LOCAs and transients defined in Chapter 4. It is a goal of the study to quantify the frequency of these core meltdown accidents and to estimate their severity, expressed in terms of radioactive material released from containment. The severity of a core melt accident depends on the initiating event, on which plant safety functions/systems defined in Chapter 3 succeeded or failed during the accident, and on the approximate time at which they failed; i.e., the accident sequence.

Event trees are the logic models from which accident sequences are derived. Two types of event trees were implemented to delineate accident sequences. The functional event tree interrelates the initiating event and the plant safety function failure events and results in functional accident sequences. The systemic event tree interrelates the initiating event and safety system failure events and results in system accident sequences. The ANO-1 functional event trees are described in Section 5.2. The ANO-1 systemic event trees are briefly described in Section 5.3. A more detailed discussion can be found in Appendix A.

5.2 ANO-1 Functional Event Trees

5.2.1 LOCA Functional Event Tree

The ANO-1 LOCA functional event tree is depicted in Figure 5-1. This tree was drawn by (1) making the

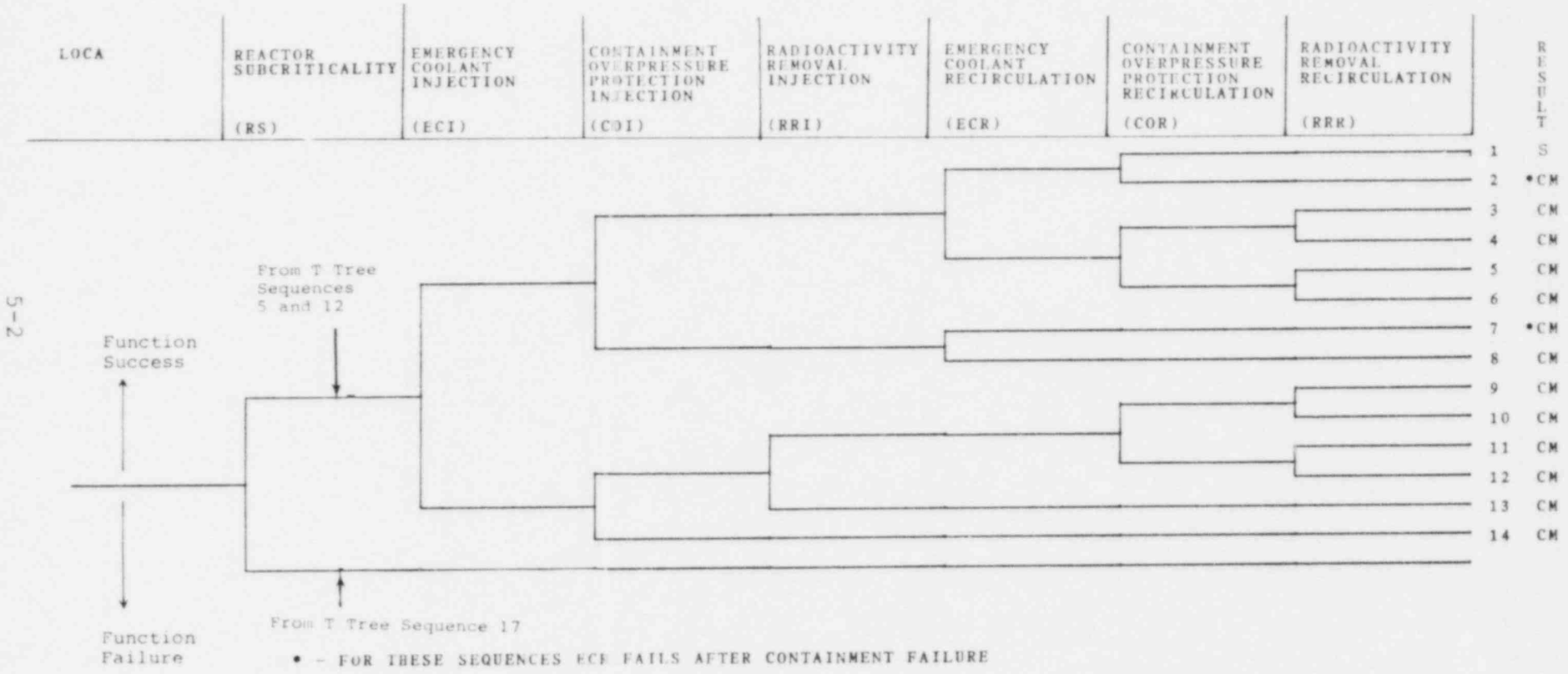


Figure 5-1. ANO-1 LOCA Functional Event Tree

plant LOCA functions described in Section 3.2.1 the event tree headings, (2) placing the event tree headings in the approximate chronological order they will be called upon following the LOCA, and (3) incorporating the functional interdependencies into the event tree structure. The interdependencies were incorporated into the event tree structure by removing success/failure decision branches at appropriate places in the tree.

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

1. If containment overpressure protection during the injection phase (COI) fails, then radioactivity removal during the injection phase (RRI) fails since the system which performs RRI is a subset of the systems performing COI.

2. If emergency core cooling during the injection phase (ECI) fails, then emergency core cooling during the recirculation phase (ECR) fails since ECR cannot prevent a core melt caused by ECI failure and operation of ECR is not expected to significantly affect the accident consequences. (Reference 2 indicates that for B&W type plants, there is a strong correlation between core melt frequency and accident consequences; i.e., all core melts have at least a 20 percent chance of leading to severe accident consequences).

3. If COI fails, then containment overpressure during the recirculation phase (COR) fails since the systems performing COI and COR share most of the same equipment and failure modes of COI would most likely fail COR.

4. If RRI fails, then radioactivity removal during the recirculation phase (RRR) fails since the systems performing RRI share most of the same equipment and failure modes of RRI would most likely fail RRR.

5. If reactor subcriticality (RS), ECI, and COI succeed, a core melt is prevented during the injection phase. A decision branch for RRI is not given for non-core melts since the success of this function would not significantly affect accident consequences.

6. If ECR and COR succeed, a core melt is prevented during the recirculation phase. A decision branch for RRR is not given for non-core melts since the success of this function would not significantly affect accident consequences.

7. With one exception, a decision branch for RRR is given for all sequences leading to core melt in which RRI succeeds. (As discussed in Chapter 3, radioactivity removal is only important in core melt sequences.) This exception is represented by Sequence 2. In this sequence a containment overpressure failure occurs which causes a failure of ECR and failure of the RRR function simultaneously. Upon failure, the containment would undergo a rapid depressurization. This would cause the superheated water in the sump to partially flash to steam and boil vigorously. The pumps which provide core cooling and radioactivity removal during the recirculation phase are not designed to pump two-phase water and are assumed to fail due

to cavitation. (It can be noted that in this sequence core melt occurs after containment failure.)

8. If COI succeeds and RRI fails, no decision branch is given for COR, since COR succeeds by definition. COI success and RRI failure implies that the reactor building cooling system (RBCS) was the system performing COI (refer to COI and RRI system success definition in Table 4-1). Since the RBCS performs both COI and COR, it was assessed that if the system is successful during the injection phase, it will most likely remain successful throughout the recirculation phase.

9. As can be noted on the event tree, no event tree structure was developed following failure of the RS function. This was done for purposes of simplification since core melt accident sequences involving LOCAs and failure of the RS function are probabilistically insignificant, i.e., less than 10^{-7}/Ryr.

5.2.1.1 LOCA Functional Accident Sequence Descriptions

The following paragraphs will discuss the sequences shown on the LOCA functional event tree.

Sequence 1 -- Sequence 1 is the LOCA sequence when all functions work as expected. In this sequence, the core is cooled, the containment pressure is kept within acceptable limits and no significant radioactivity is released to the environment.

Sequence 2 -- In Sequence 2 the COR function is unavailable. As a result, the containment will

overpressurize and fail due to steam generated during the accident. Upon failure, the containment will undergo a rapid depressurization and cause water in the containment sump to boil vigorously. This boiling is assumed to fail the pumps performing the functions of ECR and RRR due to cavitation. The core will melt due to ECR failure and radioactivity will be released to the atmosphere.

Sequence 3 -- In Sequence 3 the ECR function is unavailable which causes a core melt. The COR and RRR functions are available, however, to potentially reduce accident consequences. As discussed in Chapter 3, the COR function can delay or prevent a post core melt overpressure failure. The effectiveness of the COR and RRR functions in reducing accident consequences therefore depends on how long COR can delay overpressure or if overpressure can be prevented.

Sequence 4 -- Sequence 4 is similar to Sequence 3 except the RRR function is also unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 4 due to failure of RRR.

Sequence 5 -- In Sequence 5 the ECR and COR functions are unavailable. ECR failure will cause the core to melt and COR failure may lead to a containment overpressure failure. The RRR function is available and acts to scrub the containment atmosphere of radioactivity prior to overpressure failure.

Sequence 6 -- Sequence 6 is similar to Sequence 5 except the RRR function is also unavailable. The

radioactive material release following containment overpressure would be more severe for Sequence 6 due to failure of RRR.

Sequence 7 -- In Sequence 7 the COI and RRI functions are unavailable. COI failure will cause the containment to breach due to overpressure. As in Sequence 2, ECR failure is assumed to occur during containment depressurization following the breach. The core will melt due to ECR failure and radioactivity will be released to the atmosphere.

Sequence 8 -- In Sequence 8 the COI, RRI, and ECR functions are unavailable. As in Sequence 7, the core will melt and the containment will breach due to overpressure. In this sequence, however, the core may begin to melt prior to containment failure. This would allow some of the radioactive material released during the meltdown to plate out inside containment and thus reduce the release to the atmosphere.

Sequence 9 -- In Sequence 9, ECI fails, which causes a relatively rapid core melt and, thus, precludes success of the ECR function. Containment overpressure protection and radioactivity removal are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 10 -- Sequence 10 is similar to Sequence 9 except the RRR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 10 due to failure of RRR.

Sequence 11 -- In Sequence 11 the ECI and COR functions are unavailable. ECI failure will cause the

core to melt and COR failure may lead to containment overpressure failure. The RRR function is available and acts to scrub the containment atmosphere of radioactivity prior to overpressure failure.

Sequence 12 -- Sequence 12 is similar to Sequence 11 except the RRR function is also unavailable. The radioactive material release following containment overpressure would be more severe for Sequence 12 due to failure of RRR.

Sequence 13 -- In Sequence 13 ECI and RRI are unavailable. Containment overpressure protection is available during both the injection and recirculation phase to delay or prevent containment overpressure failure.

Sequence 14 -- In Sequence 14 all functions except reactor subcriticality are unavailable. Because of this, the core will melt relatively quickly and the containment may fail due to overpressure. Radioactive material present in the atmosphere would not be scrubbed at the time of containment breach due to failure of RRI.

5.2.2 Transient Functional Event Tree

The ANO-1 transient functional event tree is depicted in Figure 5-2. The tree was drawn by (1) making the plant transient functions described in Section 3.2.2 the event tree headings, (2) placing the event tree headings in the approximate chronological order they will be called upon following the transient initiating event, and (3) incorporating the functional interdependencies into the event tree structure by removing success/failure decision branches at appropriate places in the tree.

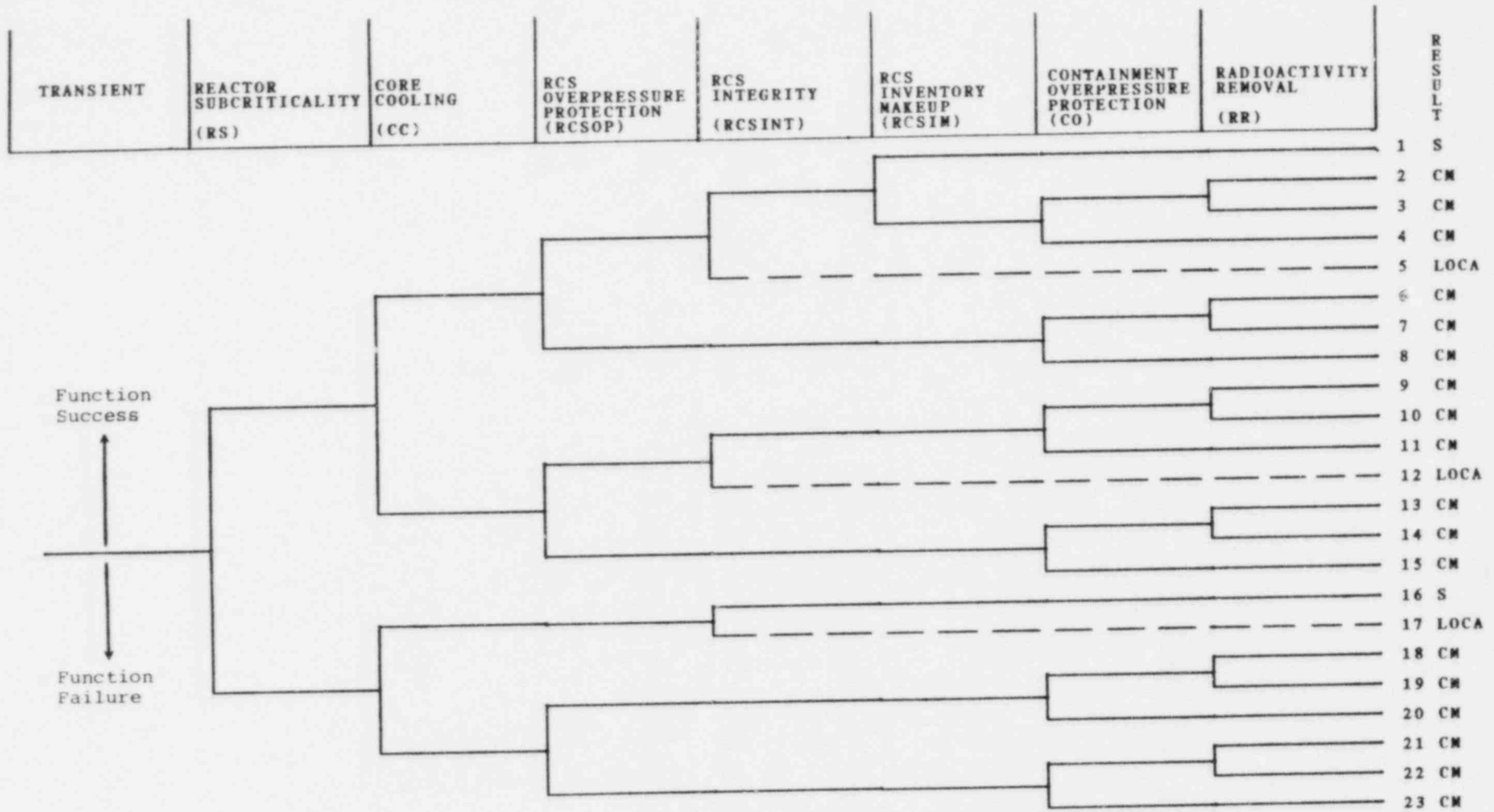


Figure 5-2. ANO-1 Transient Functional Event Tree

Dependencies incorporated into the transient functional event tree are the following.

1. If reactor subcriticality (RS), core cooling (CC), reactor coolant system overpressure protection (RCSOP), reactor coolant system integrity (RCSINT), and reactor coolant system inventory makeup (RCSIM) are successful, a core melt is prevented. Given success of these functions, decision branches for containment overpressure protection (CO) and radioactivity removal (RR) are not given since CO and RR are important for mitigating the consequences of core melt accidents only. (It should be noted that CO could conceivably be required if CC is provided by the "feed and bleed" core cooling method described in Chapter 3 since steam is released to the containment. Analysis presented in Reference 2 indicates that if it is assumed that the CO function fails, it takes approximately 70 hours to overpressurize the containment during feed and bleed. This should be more than ample time to establish other means of providing CC which do not eject steam to the containment.)

2. If CO fails, then RR fails since the system which forms RR is a subset of the systems performing CO.

3. If the relief valves performing the function of RCSOP fail to open they logically cannot fail to close, i.e., failure of RCSINT. No decision branch for RCSINT is therefore given following failure of RCSOP.

4. If RS and CC fail and RCSOP succeeds, no decision branch is given for RCSINT because it is assumed that the relief valves will remain open through core meltdown due to high RCS pressure.

5. Accident sequences involving failure of the RCSINT function are classified as a LOCA. Transient sequences involving failure of the RCSINT function are developed to completion on the LOCA functional event tree. (See Figure 5-1).

6. If CC fails, then RCSIM fails since the system which performs RCSIM is a subset of the systems performing core cooling.

7. If RCSOP fails, a core melt is assumed to occur and no decision branch is given for RCSIM because this function is not expected to significantly affect accident consequences. (It is conservatively assumed that RCSOP failure will lead to an uncoolable core via distortions and failures of RCS components.)

8. If RS fails and CC succeeds, then no decision branch is given for RCSOP and RCSIM because these functions succeed by definition. This is because following RS failure, successful CC requires the same systems which perform RCSOP and RCSIM.

9. If RS fails, but CC and RCSINT succeed, a core melt is assumed to be prevented and thus decision branches for CO and RR are not given since CO and RR are important for mitigating the consequences of core melt accidents only. (Reference 1 states that peak RCS pressures in the neighborhood of

4000 psi may occur during this type of accident sequence. B&W has assessed that the RCS will survive this pressure transient.(12) However, these types of sequences are an unresolved safety issue at the NRC. This analysis will adopt the B&W assessment but will treat this sequence as a sensitivity issue (see Chapter 8.) It should be noted that CC success following RS failure will eventually render the reactor subcritical since CC requires borated water to be injected into the core.

5.2.2.1 Transient Functional Accident Sequence Descriptions

The following paragraphs will discuss the sequences shown on the transient functional event tree:

Sequence 1 -- Sequence 1 is the transient when all functions work as expected. In this sequence, the core is cooled, inventory lost through small RCS leaks is replaced, the containment pressure is kept within acceptable limits and no significant radioactivity is released to the environment.

Sequence 2 -- In Sequence 2, the RCSIM function fails. If the transient involves reactor coolant pump seal leaks, failure of RCSIM will cause the core to uncover within several hours and an eventual melt. The functions of CO and RR are available to delay or prevent containment overpressure and reduce accident consequences.

Sequence 3 -- Sequence 3 is similar to Sequence 2, except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 3 due failure of RR.

Sequence 4 -- In Sequence 4, the RCSIM, CO and RR functions are unavailable. RCSIM failure accompanied by reactor coolant pump seal leaks will cause core melt, and CO failure may lead to containment overpressure failure.

Sequence 5 -- In Sequence 5, the RCSINT function fails. Failure of RCSINT creates a small LOCA which requires the LOCA functions described in Chapter 3 for mitigation. Sequence 5 is therefore transferred to sequences on the LOCA functional event tree in which RS has succeeded.

Sequence 6 -- In Sequence 6, the CC function is initially available, but during its implementation a requirement for the function of RCSOP occurs. In this sequence RCSOP fails and it is conservatively assumed that this causes damage to the reactor vessel and/or core such that the core can no longer be successfully cooled. The core will melt due to failure of core cooling. The functions of CO and RR are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 7 -- Sequence 7 is similar to Sequence 6 except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 7 due to failure of RR.

Sequence 8 -- In Sequence 8 the RCSOP, CO, and RR functions are unavailable. RCSOP failure is assumed to cause core melt and CO failure may lead to containment overpressure failure.

Sequence 9 -- In Sequence 9, failure of the transient function CC and success of RCSINT cause a core melt (failure of RCSINT would cause the RCS to depressurize and thus allow the possibility of cooling the core via the LOCA function of ECI). The functions of CO and RR are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 10 -- Sequence 10 is similar to Sequence 9 except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 10 due to failure of RR.

Sequence 11 -- In Sequence 11 the functions of CC, CO, and RR failed and the function of RCSINT succeeded. Failure of CC and success of RCSINT cause a core melt. Failure of CO may lead to containment overpressure failure.

Sequence 12 -- In Sequence 12 the functions of CC and RCSINT fail. Failure of RCSINT creates a small LOCA which requires the LOCA functions described in Section 3.2.1 for mitigation. Sequence 12 is therefore transferred to sequences on the LOCA functional event tree in which RS has succeeded. (It can be noted that Sequence 12 is not a core melt unless the LOCA core cooling functions fail. Even though the transient function of CC failed in this sequence, this does not imply failure of the LOCA core cooling function of ECI. This is because one method of CC failure is failure of the operator to manually initiate feed and bleed core cooling (refer to CC discussion in Section 3.2.2). This failure mode does not apply to ECI following failure of RCSINT since the

primary system will depressurize and cause automatic core cooling initiation.)

Sequence 13 -- In Sequence 13 failure of the CC function causes a requirement for the function of RCSOP. In this sequence RCSOP fails, and it is conservatively assumed that this causes damage to the reactor vessel and/or core such that a core melt ensues. The functions of CO and RR are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 14 -- Sequence 14 is similar to Sequence 13 except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 14 due to failure of RR.

Sequence 15 -- In Sequence 15 the CC, RCSOP, CO, and RR functions are unavailabble. CC and RCSOP failure is assumed to cause core melt and CO failure may lead to containment overpressure failure.

Sequence 16 -- In Sequence 16 RS fails but all other functions are available to mitigate the transient. Even with success of the function of RCSOP, analysis presented in Reference 1 indicates that excessively high RCS pressures may occur. This sequence assumes that the core will remain coolable following the pressure transient,[12] and a core melt will be prevented.

Sequence 17 -- In Sequence 17 the functions of RS and RCSINT fail. Failure of RCSINT creates a small LOCA which requires the LOCA functions described in Section 3.2.1 for mitigation. Sequence 17 is therefore transferred to sequences on the LOCA functional event tree in which RS has failed.

Sequence 18 -- In Sequence 18 the functions of RS and CC are unavailable. Failure of these two functions cause a core melt. The functions of CO and RR are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 19 -- Sequence 19 is similar to Sequence 18 except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 19 due to failure of RR.

Sequence 20 -- In Sequence 20 the RS, CC, CO, and RR functions are unavailable. RS and CC failure cause core melt and CO failure may lead to containment overpressure failure.

Sequence 21 -- In Sequence 21 failure of the RS causes a requirement for the function of RCSOP. In this sequence failure of RCSOP along with CC will cause a relatively fast core melt. The functions of CO and RR are available to delay or prevent containment overpressure failure and reduce accident consequences.

Sequence 22 -- Sequence 22 is similar to Sequence 21 except the RR function is unavailable. If a containment overpressure occurs, the radioactive material release to the atmosphere would be more severe for Sequence 22 due to failure of RR.

Sequence 23 -- In Sequence 23 all mitigating functions are unavailable. Failure of RS, CC, and RCSOP cause a relatively fast core melt and CO failure may lead to containment overpressure failure.

5.3 ANO-1 Systemic Event Trees

5.3.1 LOCA Systemic Event Trees

Six LOCA systemic event trees were constructed to represent the plant front line system response to the six LOCA break size ranges defined in Chapter 4. Six event trees were drawn because the front line systems required to perform the LOCA functions and/or the interdependencies between the systems were different for each break size range. These event trees are:

LOCA Initiating Event	LOCA Systemic Event Tree
1. .38"D < Breaks $\leq$ 1.2"D	Figure 5-3
2. 1.2"D < Breaks $\leq$ 1.66"D	Figure 5-4
3. 1.66"D < Breaks $\leq$ 4"D	Figure 5-5
4. 4"D < Breaks $\leq$ 10"D	Figure 5-6
5. 10"D < Breaks $\leq$ 13.5"D	Figure 5-7
6. 13.5"D < Breaks $\leq$ 36"D	Figure 5-8

Each event tree was drawn by (1) making the front line systems, which perform the LOCA mitigating functions in response to a particular break size range, the event tree headings (these systems were given as a function of break size range in Chapter 4, Table 4-1), (2) placing the event tree headings in the approximate chronological order they will be called upon following the LOCA, and (3) incorporating into the event tree structure interdependencies between the systems and the functions they perform.

The definitions for the events depicted on the six event trees are given in Table 5-1. The reader should refer to Section A.1.1 of Appendix A for a detailed discussion of these events and the interdependencies between them.

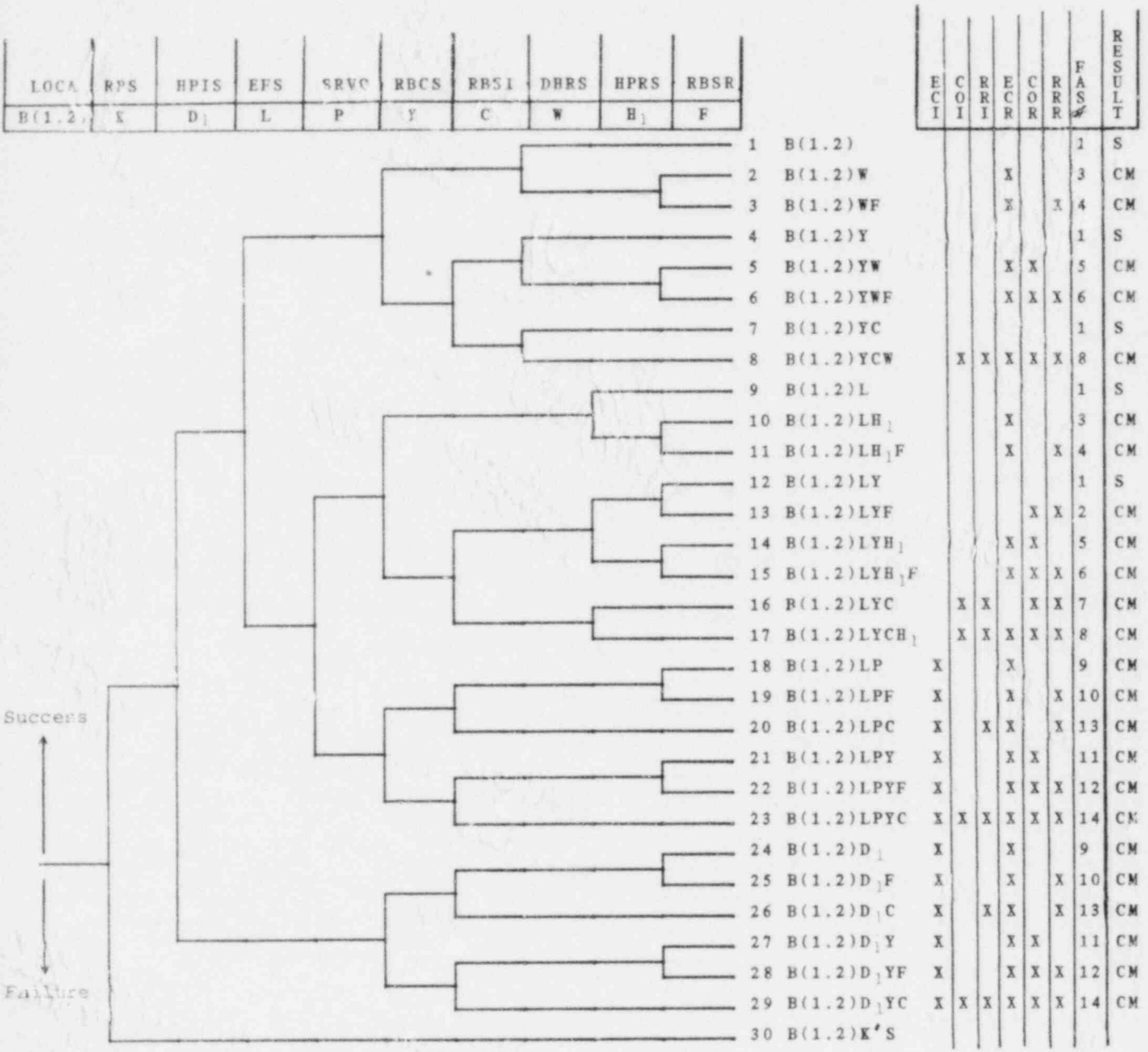
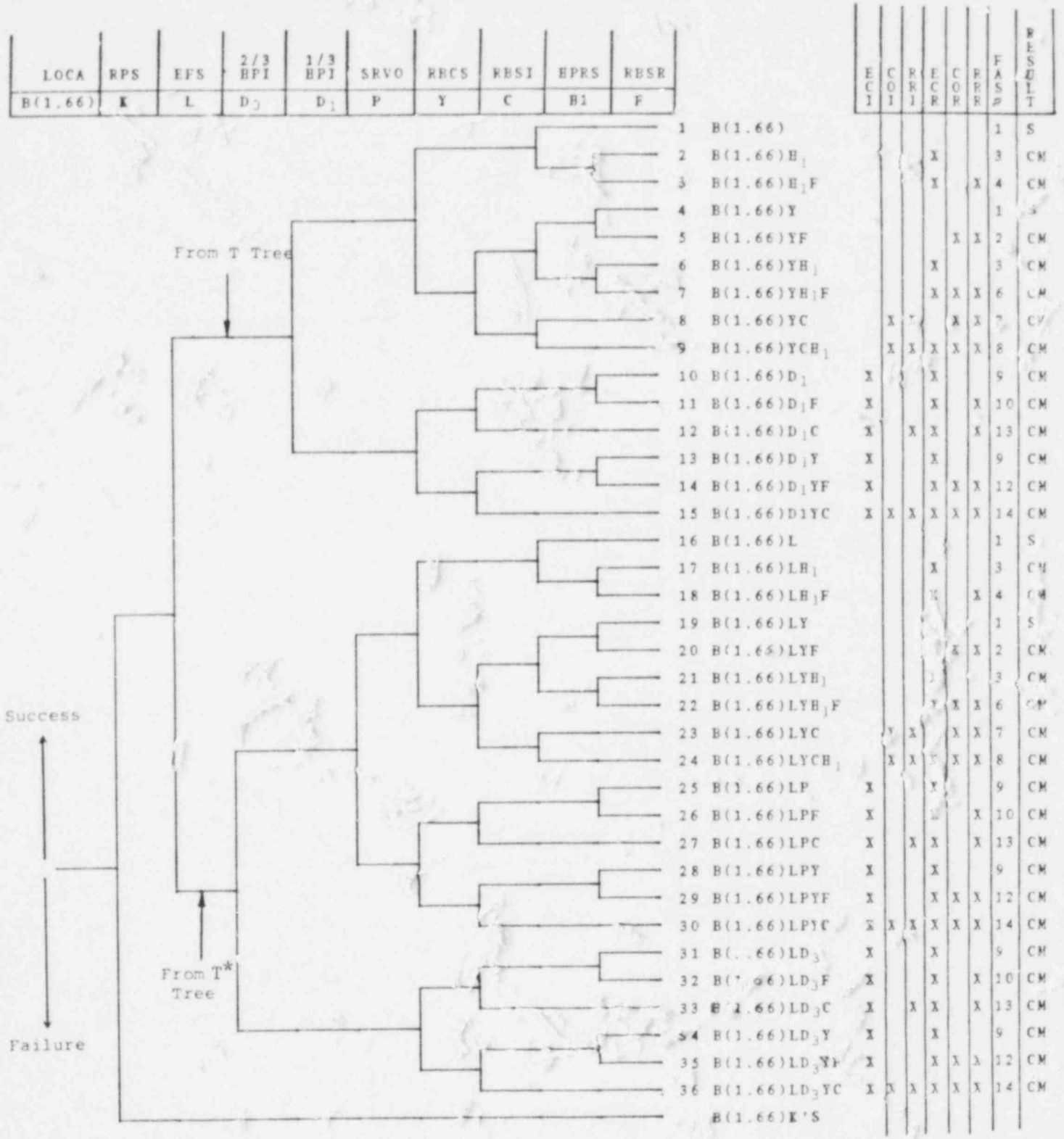


Figure 5-3. ANO-1 LOCA Systemic Event Tree for Breaks .38"<D≤1.2"



*Note: For transient induced LOCAS, sequences 25 through 30 do not apply.

Figure 5-4. ANO-1 LOCA Systemic Event Tree for Breaks $1.2" < D \leq 1.66"$

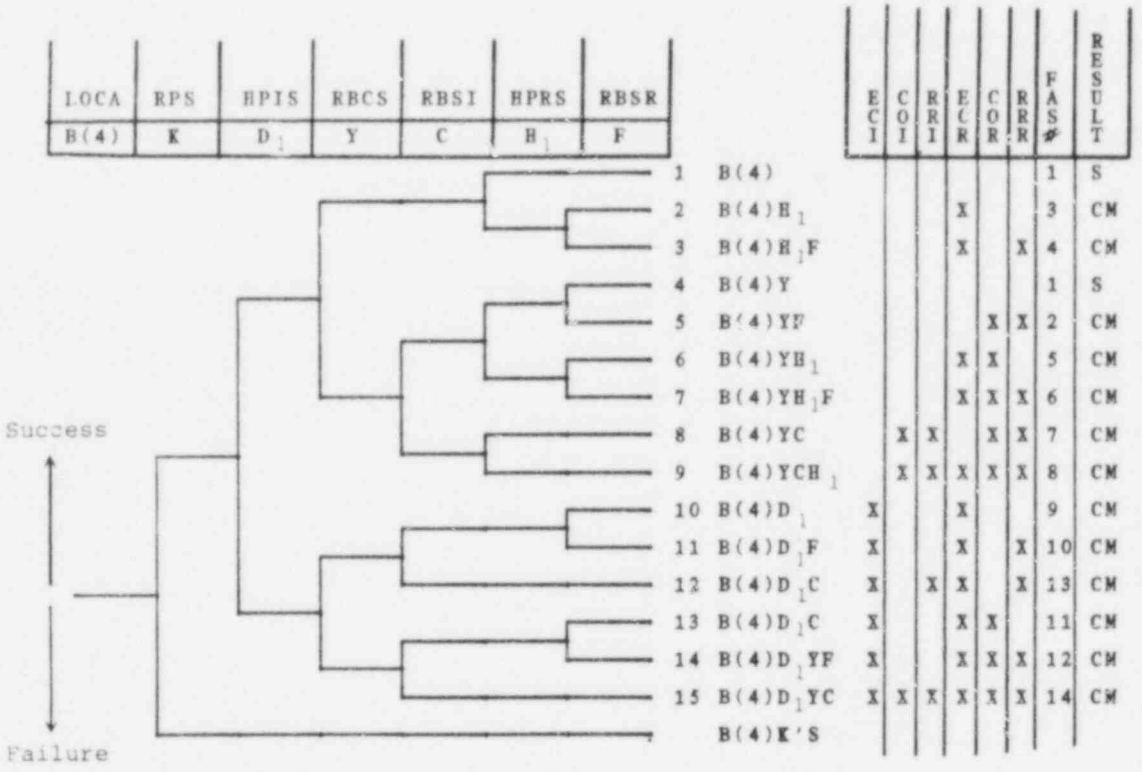


Figure 5-5. ANO-1 LOCA Systemic Event Tree for Breaks $1.66" < D \leq 4"$

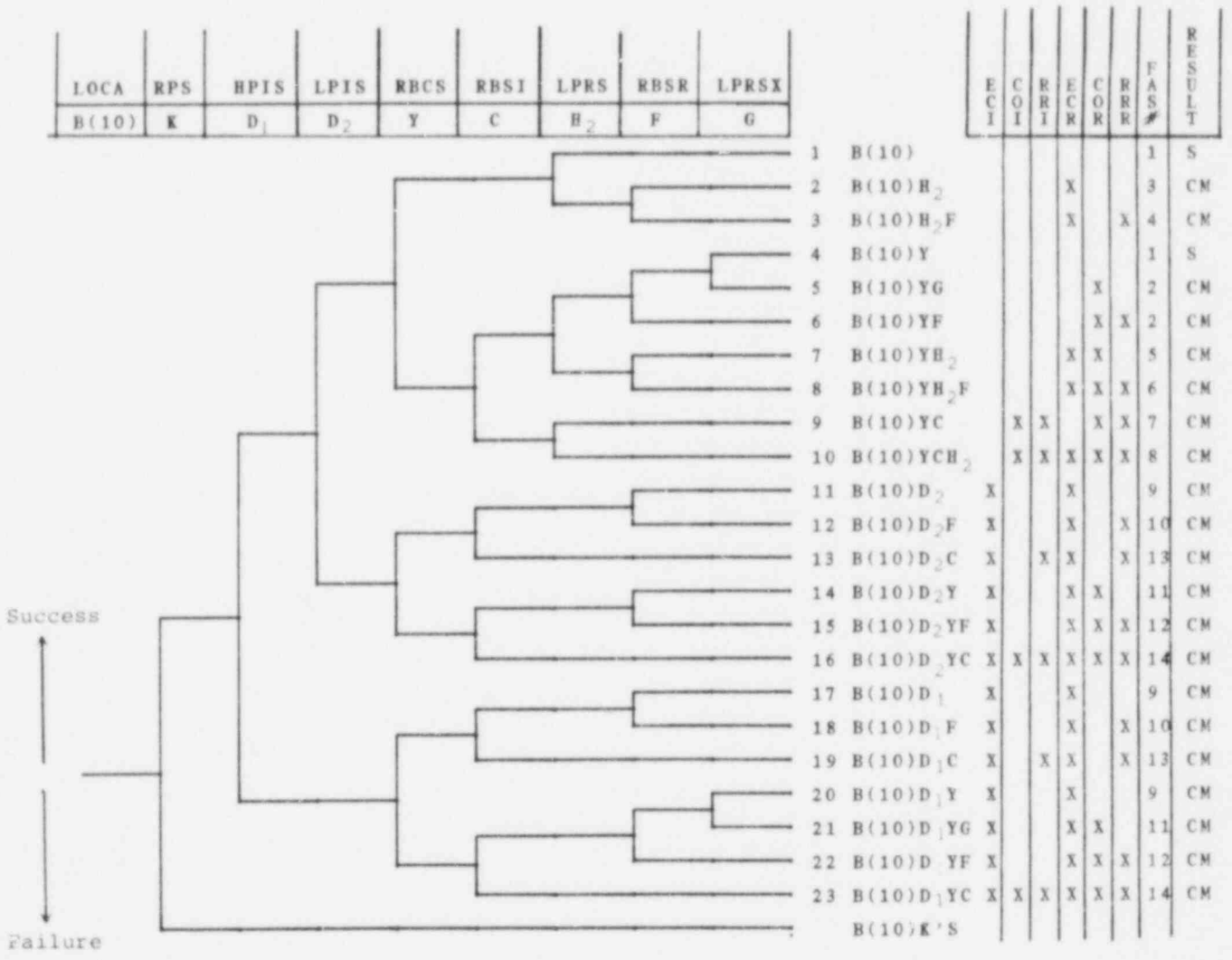


Figure 5-6. ANO-1 LOCA Systemic Event Tree for Breaks $4" < D \leq 10"$

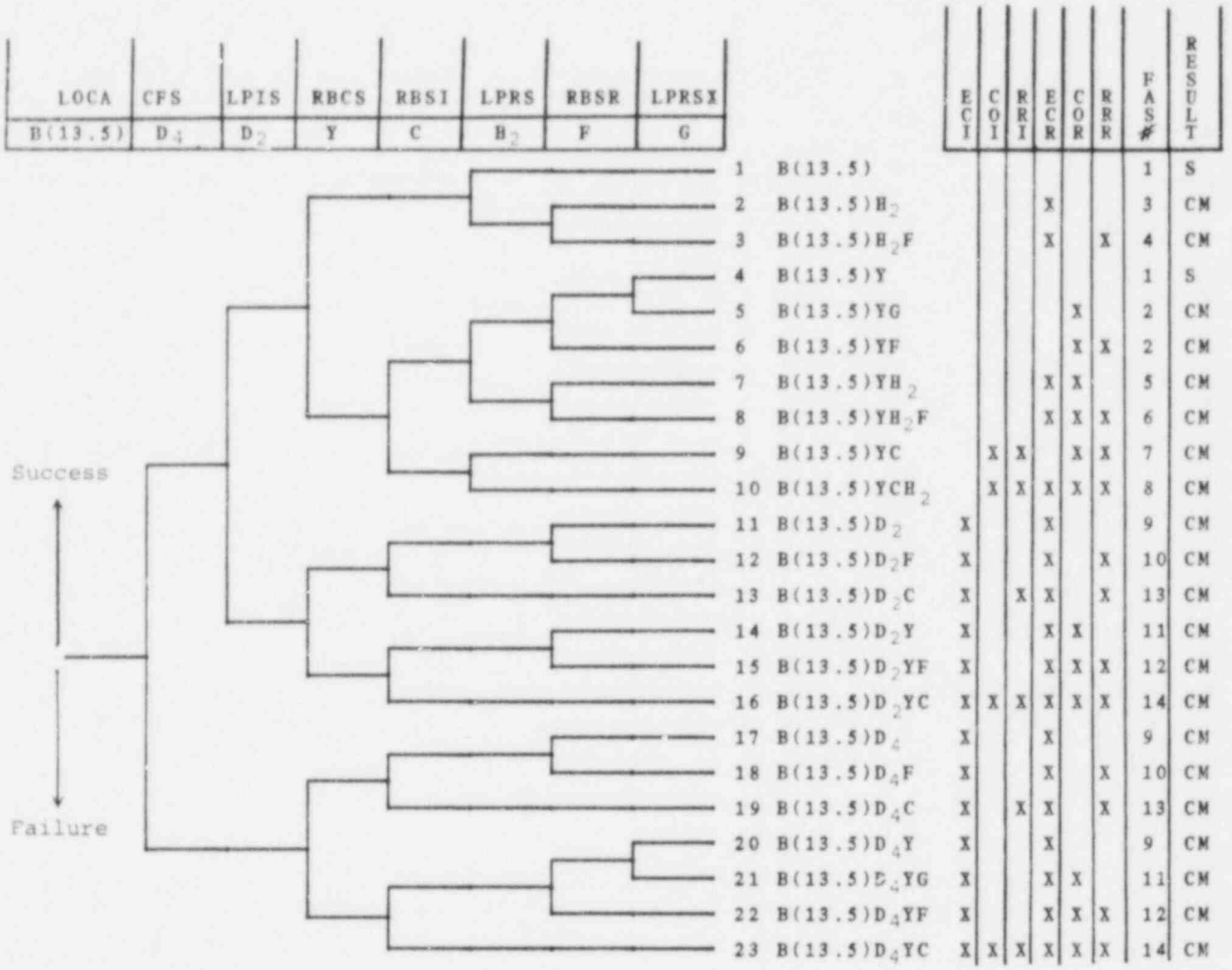


Figure 5-7. ANO-1 LOCA Systemic Event Tree for Breaks 10"<D≤13.5"

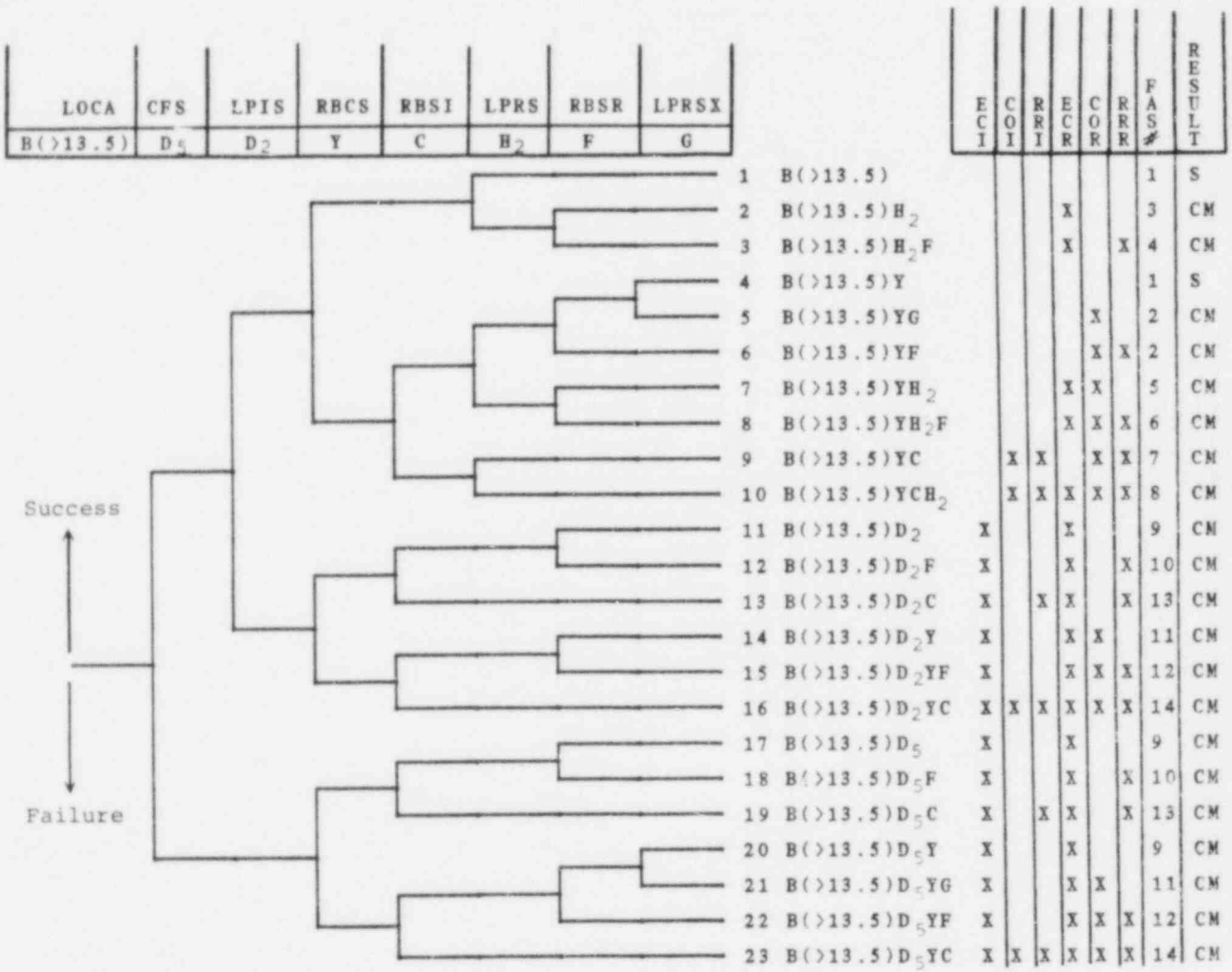


Figure 5-8. ANO-1 LOCA Systemic Event Tree for Breaks D<13.5"

Table 5-1

Event Definitions for LOCA Event Trees

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

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

B(13.5) 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" $\geq$ D > 10").

B(10) Medium 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" $\geq$ D > 4").

B(4) Small LOCA - a breach of the RCS with a flow area greater than .015 ft^2 and less than or equal to .087 ft^2 (4" $\geq$ D > 1.66").

B(1.66) Small LOCA - a breach of the RCS with a flow area greater than .008 ft^2 and less than or equal to .015 ft^2 (1.66" $\geq$ D > 1.2").

B(1.2) Small-Small LOCA - a breach of the RCS with a flow area greater than 7.6×10^{-4} ft^2 and less than or equal to .008 ft^2 (1.2" $\geq$ D > .38").

C Reactor Building Spray Injection System - 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.

D_1 High Pressure Injection System (HPIS) - Failure to provide flow to the reactor vessel from at least 1 of 3 high pressure pumps, taking suction from the BWST.

D_2 Low Pressure Injection System (LPIS) - Failure to provide flow to the reactor vessel from at least 1 of 2 low pressure pumps, taking suction from the BWST.

Table 5-1 (Continued)

D_3 High Pressure Injection System (HPIS) - Failure to provide flow to the reactor vessel from at least 2 of 3 high pressure pumps, taking suction for the BWST.

D_4 Core Flood System (CFS) - Failure to inject the contents of 1 of 2 tank trains into the reactor vessel.

D_5 Core Flood System (CFS) - Failure to inject the contents of 2 of 2 tank trains into the reactor vessel.

F Reactor Building Spray Recirculation System (RBSR) - 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.

G Low Pressure Recirculation System Heat Exchange (LPRSX) - Failure to provide sufficient cooling of containment sump water by at least 1 of 2 LPRS heat exchangers.

H_1 High Pressure Recirculation System (HPRS) - Failure to provide flow to the reactor vessel from at least 1 out of 3 high pressure trains with its associated low pressure train, taking suction from the reactor building sump.

H_2 Low Pressure Recirculation System (LPRS) - Failure to provide flow to the reactor vessel from at least 1 out of 2 low pressure trains, taking suction from the reactor building sump.

K Reactor Protection System (RPS) - Failure of the automatic reactor scram system to insert at least 6 shutdown rod groups into the core.

L Emergency Feedwater System (EFS) - Failure to provide steam generator cooling via 1 of 2 emergency feedwater pump trains.

Table 5-1 (Concluded)

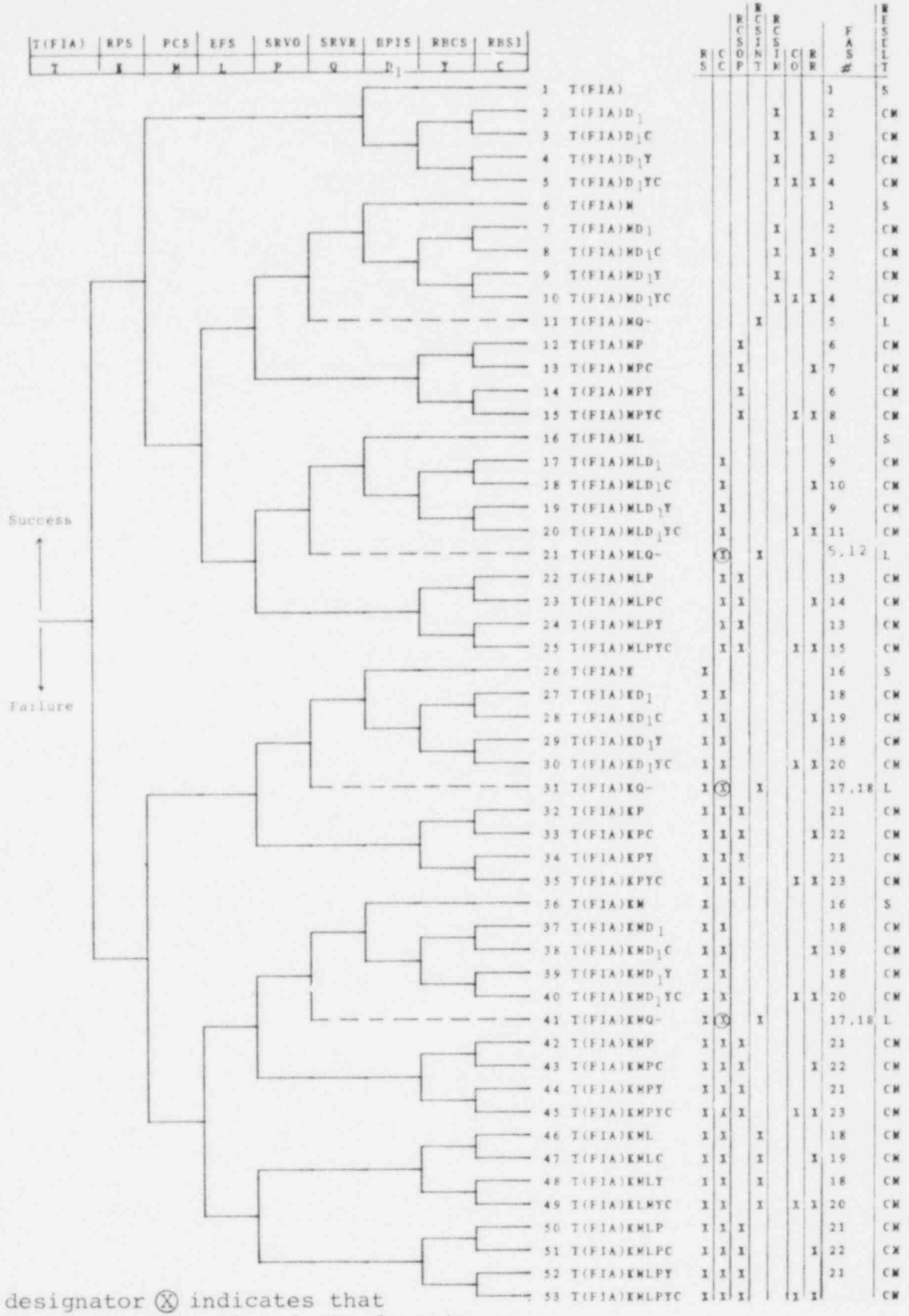
P	Safety/Relief Valves Open (SR/VO) - Failure to relieve excess primary pressure via 1 of 2 pressurizer safety valves.
W	Decay Heat Removal System (DHRS) - Failure to provide cooled flow to the reactor vessel with at least 1 of 2 low pressure trains, taking suction from the RCS hot leg.
Y	Reactor Building Cooling System (RBCS) - Failure to remove steam (heat) from the containment atmosphere by at least 1 out of 3 reactor building cooling fans.

Each event tree contains a table that lists the LOCA mitigating functions which have failed for each system accident sequence. The tables also contain the appropriate functional accident sequence number defined in Figure 5-1 which applies to each system accident sequence.

5.3.2 Transient Systemic Event Trees

Three transient event trees were constructed to represent the plant front line system response to the eight transient initiating event groups defined in Chapter 4. For each of the eight initiating event groups, one of the three event trees is appropriate.

Transient Initiating Event	Transient Systemic Event Tree
1. Requirement for reactor trip (RRT) with the power conversion system initially available	Figure 5-9
2. RRT due to a loss of offsite power	Figure 5-10
3. RRT due to complete interruption of the power conversion system	Figure 5-10
4. RRT due to failure of engineered safeguards (ES) bus A3 (4160V AC)	Figure 5-10
5. RRT due to failure of ES bus B5 (480V AC)	Figure 5-10
6. RRT due to failure of ES bus D01 (125V DC)	Figure 5-10
7. RRT due to failure of ES bus D02 (125V DC)	Figure 5-10
8. RRT due to failure of the service water system	Figure 5-11



Note: The designator (X) indicates that for the first FAS# listed the function succeeds, and for the second FAS# listed the function fails.

Figure 5-9. ANO-1 "All Front Line Systems Initially Available" Transient Systemic Event Tree

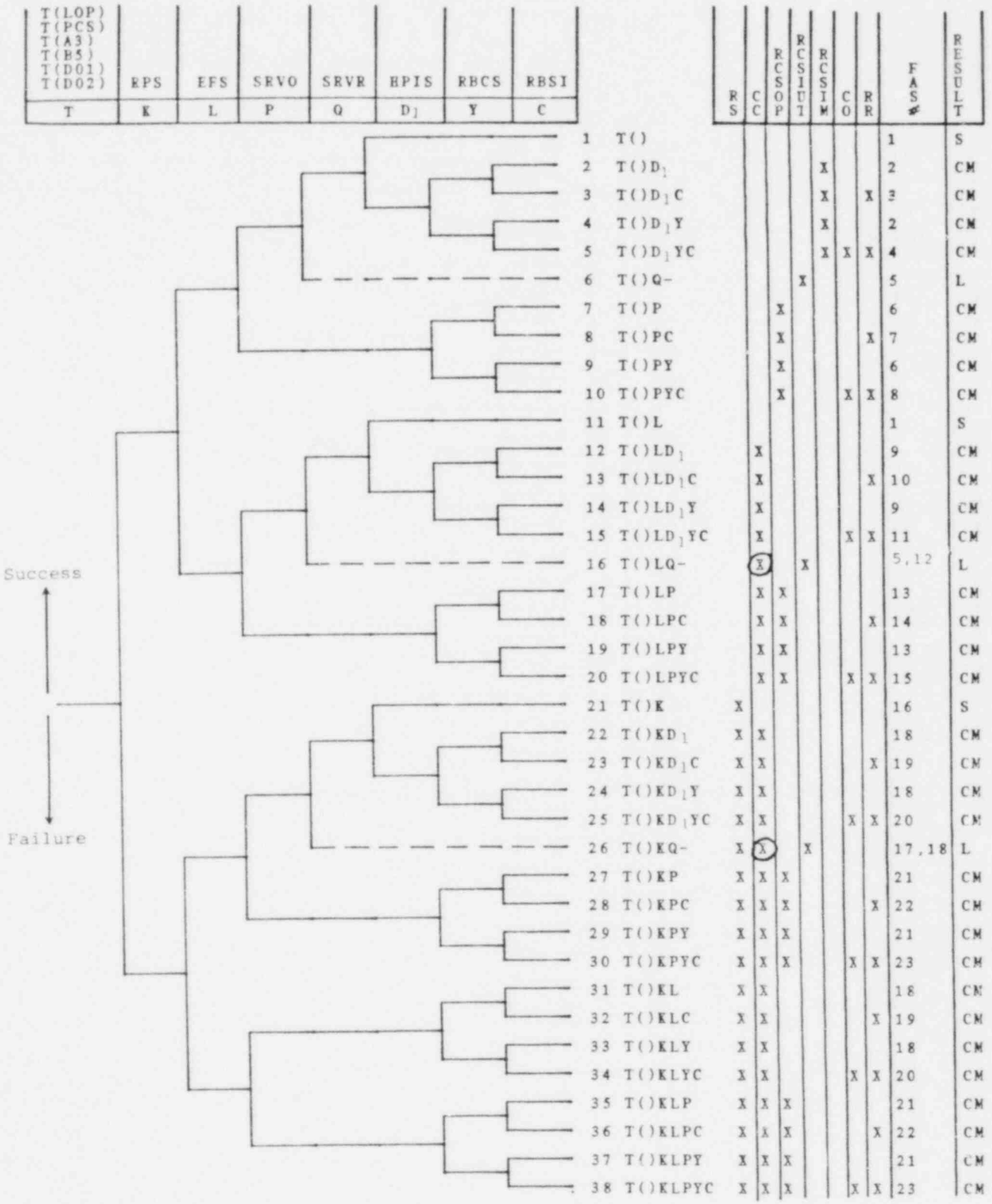


Figure 5-10. ANO-1 "Power Conversion System Initially Unavailable" Transients Systemic Event Tree

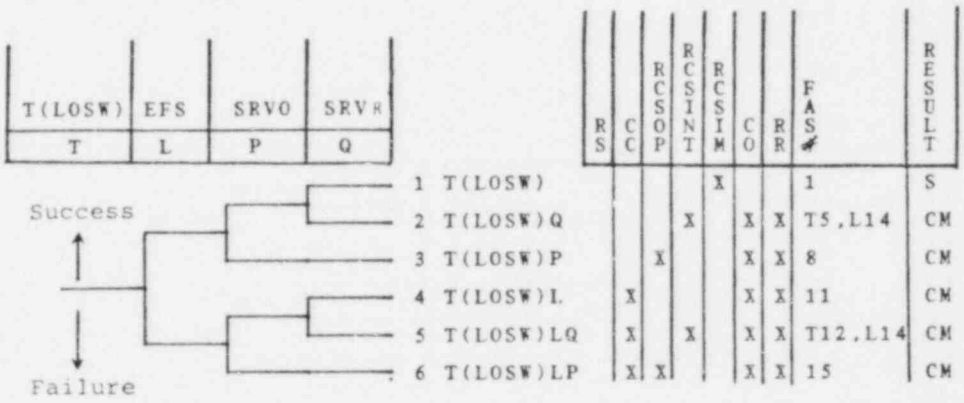


Figure 5-11. ANO-1 "Loss of Service Water System" Transient Systemic Event Tree

Each event tree was drawn by (1) making the front line systems, which perform the transient mitigating functions in response to the particular transient, the event tree headings, (2) placing the event tree headings in the approximate chronological order they will be called upon following the transient, and (3) incorporating into the event tree structure interdependencies between the systems and the functions they perform.

The definitions for the events depicted on the three event trees are given in Table 5-2. The reader should refer to Section A.2.1 of Appendix A for a detailed discussion of these events and the interdependencies between them.

Table 5-2

Event Definitions for the Transient Event Tree

Transient - Any abnormal condition in the plant which requires that the plant be shut down, but does not directly breach RCS integrity. There are eight transient categories.

T(FIA) Shutdowns with all front line systems initially available.

T(LOP) Shutdowns initiated by a loss of offsite power.

T(PCS) Shutdowns initiated by a failure of the power conversion system.

T(A3) Shutdown initiated by failure of the engineered safeguards (ES) bus A3 (4160V AC).

T(B5) Shutdown initiated by failure of ES bus B5 (480V AC).

T(D01) Shutdowns initiated by failure of ES bus D01 (125V DC).

T(D02) Shutdowns initiated by failure of ES bus D02 (125V DC).

T(LOSW) Shutdowns initiated by failure of the plant service water system.

C Reactor Building Spray Injection System (RBSI) - 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.

K Reactor Protection System (RPS) - Failure of the automatic reactor scram system to insert at least 6 shutdown groups into the core.

L Emergency Feedwater System (EFS) - Failure to provide steam generator cooling via 1 of 2 emergency feedwater pump trains.

Table 5-2 (Continued)

Event Definitions for the Transient Event Tree

M — Power Conversion System (PCS) - Failure to provide steam generator cooling via 1 train of main feedwater portion of the PCS.

P — Safety/Relief Valves Open (SR/VO) -

a) For sequences involving success of event K -- failure to relieve excess primary pressure via 1 of 2 pressurizer safety valves.
b) For sequences involving failure of event K -- failure to relieve excess primary pressure via 2 of 2 pressurizer safety valves.

Q — Safety/Relief Valves Close (SR/VC) - Failure of any SRV which opened to reseat.

D_1 — High Pressure Injection System (HPIS) - Failure of the operator to manually establish flow from the BWST to the reactor vessel using at least one high pressure injection pump.

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

CHAPTER 6

SYSTEMS ANALYSIS

The probabilistic risk assessment of ANO-1 necessitated a thorough comprehension of the systems at the plant which could be used to mitigate the effects of a LOCA or transient. This chapter briefly presents the methodology and several assumptions used in this task. Furthermore, summaries of the systems, both front-line and support, are given. Detailed system descriptions and fault trees are presented in Appendix B. Also given in Appendix B are the fault summary sheets used in the quantification process, which is discussed in Chapter 7.

6.1 Methodology and General Assumptions

6.1.1 Methodology

The methodology used in the ANO-1 systems analysis is that presented in SAND81-0062, "Fault Tree Analysis Procedures for the Interim Reliability Program."(13) Basically, the methodology presented in the report is a modular logic approach to the development of detailed fault tree models for the various studied systems.

The application of this IREP methodology was to concentrate the fault tree development on the hardware in the plant systems. The fault trees represented system failures in terms of component faults. In addition, human error effects were assessed in the evaluation of the trees. Concentrating on the mechanistic part of the problem provided a set of basic fault trees that have broad utility for different kinds of analyses.

To apply the modular fault tree development approach, fluid systems were divided into piping segments (electrical and actuation systems were divided into wiring segments), and the fault logic for the systems was developed in terms of failures of the piping segments as defined by a set of rules presented in the methodology report. Detailed fault logic for the piping segments was developed by the use of standardized sub-trees which were adjusted to properly represent the specific characteristics of each segment.

6.1.1.1 Systems and Success Criteria

The front-line systems which were analyzed are those identified in the event trees that were discussed in Chapter 5. In addition, the initiating events (Chapter 4) and the event tree development determined the success criteria for those systems for a particular accident sequence, and these criteria dictated the top failure logic for the front-line system fault trees.

In addition to the front-line system success, accident mitigation also requires the successful functioning of support systems upon which the front-line systems depend. Shown in Table 3-4 is a front-line system -- support system dependency matrix. The support systems listed in the matrix were also analyzed. Table 3-5 shows the interrelationships among the support systems. Although not listed in either matrix, the operators are a support system for all systems.

6.1.1.2 System Information

Information for the systems analysis was gathered from a number of sources. The Final Safety Analysis Report and Technical Specifications for ANO-1 were

used.[7] The plant was visited. AP&L also supplied complete operational and emergency procedures for ANO-1 as well as all the relevant piping and instrumentation diagrams, electrical one-line and control drawings, functional logic diagrams, and all the licensee event reports (LERs). Most importantly, AP&L personnel were available, as needed, for discussions, including the full-time participation during the systems analysis task of a former ANO-1 assistant superintendent of operations.

6.1.1.3 Systems Analysis

The systems analysis team assimilated the systems information from the sources given above in Section 6.1.1.2. The overall configuration of each system was understood as well as its instrumentation and control and any operator actions affecting the system. Testing and maintenance of the system components was investigated, and the normal and emergency operation of the system was studied. In addition, a failure modes and effects analysis was conducted for each system in relation to its support system dependencies. These steps were undertaken to develop as complete an understanding of the system as possible.

A detailed fault tree for each front-line system was then constructed with the top event being that determined from the event tree analysis. Several systems have different success criteria, depending on the specific event tree application. In these cases, a top level fault tree was developed for each event-tree failure definition. The system was decomposed into piping segments (wiring segments for electrical or actuation systems), and the top level tree was developed to the extent necessary to portray all the pipe segments whose failure was sufficient to fail the system for the given application. Local faults were

analyzed within each pipe segment, and support system interfaces were identified.

It must be noted that not all front-line systems were analyzed to this detail. As will be described in Section 6.2, a simpler model was used for some systems.

Support system models were developed for all the interfaces identified by the front-line system fault trees and for interfaces with other support systems. Not all support systems were developed in full detail. For example, the instrument air system is needed to fill some charging tanks. It was assumed, however, that the tanks were full (or else shutdown is required), so that the instrument air system was not analyzed further. The overall support system study was similar to that described above for the front-line systems.

The systems analysis resulted in an a very detailed model for ANO-1 systems which not only logically described hardware faults but also included test and maintenance unavailabilities. In addition, possible operator error inputs to the models were analyzed. These errors were of two types. The first considered operator actions in response to an accident. An example of this type of error is the failure of the operator to manually change ECCS pumps from injection alignment to recirculation alignment. The second type considered the failure of the operators to properly restore a component after test and maintenance. An example of this type of human error is the miscalibration of pressure sensors in the Engineered Safeguards Actuation System. Because of the detailed nature of the analysis, hardware and human common mode failures, within the scope of the analysis, were readily identified. Hardware examples were shared

components, and human examples included common testing and maintenance activities.

6.1.2 General Assumptions

General assumptions for the analysis were of three classes: fault tree development and quantification, system fault postulation and consideration, and inclusion of operator action. System specific assumptions are discussed in Sections 6.2 and 6.3 and Appendix B.

6.1.2.1 Fault Tree Development and Quantification

Two systems and portions of another were not modeled in detail. Main feedwater system fault trees were only developed in those areas which interfaced with other systems defined as front line or support systems. All other MFWS faults were grouped as local faults and loss of main feedwater generic industry data were applied as appropriate.

In addition, the ERV was not analyzed in detail. At the time of the study, the block valve at ANO-1 was closed. The failures of the safety valves to both open and close were examined and found to be independent of other systems. To quantify these failures, generic industry data were used.

Finally, portions of the Emergency Feedwater Initiation and Control (EFIC) system were not analyzed to the detail of other portions of the system. This is described further in Section 6.3.6.

6.1.2.2 System Fault Postulation and Consideration

Four general assumptions of this nature were made:

1. System fault events which could also be accident initiators (e.g., loss of off-site power) were

explicitly included as appropriate in each system fault tree.

2. Passive failures, which were accident initiators, were included in each system fault tree. In addition, single passive failures which could fail the entire system were included.

3. Flow diversion paths were considered as potential system failure modes for fluid delivery systems. However, each potential diversion path was included on the fault tree only if it resulted in failure of the system and its likelihood was comparable to other system faults. That is, a possible diversion path had to have a diameter not less than one-third (approximately 10 percent of the area) of the diameter of the intended path, and probability discrimination was used in diversion development.

4. Spurious control faults of components after successful initial operation were considered only in those cases where the component was expected to receive an additional signal during the course of the accident to readjust or change its operating state.

6.1.2.3 Inclusion of Operator Action

As mentioned in 6.1.1.3, operator actions were an integral part of the models of the systems. Three general assumptions were made regarding operator actions. The first two concern the first type of operator action discussed above, and the third is of the fail-to-restore type. The assumptions were:

1. Operator errors of commission which misposition valves or fail other components in response to the accident were only included for those components which are specifically identified in procedures as requiring operator manipulation.

2. Consideration of operator action as a successful operating mode for systems was only done in those cases where a written procedure for system operation exists which specifies the required operator actions. That is, operator recovery actions were not explicitly considered in the fault tree, but were treated following the screening calculations for accident sequence frequencies. "Verify" statements in procedures were treated as recovery operations.

3. Mispositioning of valves prior to the accident was not considered in those cases where valve position is indicated in the control room and monitored each shift. Nor was it considered if the valves receive an automatic signal to return to their operable state under accident conditions.

6.2 ANO-1 Front Line Systems

Presented in this section are brief descriptions of the front line systems at ANO-1. More detailed discussions of these systems can be found in Appendix B. The rationale for which systems, either front-line or support, which are described in this chapter was discussed in Chapter 3.

6.2.1 High Pressure Injection/High Pressure Recirculation

The high pressure (HP) system is utilized during those LOCAs where the reactor coolant pressure remains high (i.e.,

above about 150 psig where the low pressure (LP) pumps are ineffective). This condition will typically exist during small breaks and during the early stages of medium breaks. The High Pressure Injection System is, like most other engineered safeguards (ES) systems, actuated upon receiving an engineered safeguards actuation system (ESAS) signal which signifies either a 1500 psig RCS pressure or a 4 psig reactor building pressure. During the injection mode, the HP system draws borated water from the borated water storage tank (BWST) via a common tank outlet header shared with the LP and reactor building spray (RBS) systems. When switched to the recirculation mode (which requires manual operator actions) the water is drawn from the reactor building sump by the LP pumps through the decay heat coolers whose discharge is aligned to the HP pump suction which then injects into the reactor vessel. Figure 6-1 is a simplified schematic of the HP system (the discharges of the decay heat coolers to the HP pumps is through pipe segments DH7A and DH7B) with valve positions shown prior to injection.

The HP system is a two train, three pump system which injects water into the reactor pressure vessel via four injection headers (one for each cold leg of the RCS). The injection headers are cross connected such that each pump has an open flow path to all four RCS cold legs.

During normal operation, one of three HP pumps is kept running in order to provide normal makeup to the reactor coolant system. Upon receiving an ES signal a second HP pump is started and the running HP pump is realigned from normal makeup to HPI. The realignment is accomplished by opening the suction of the HP pumps to the BWST, isolating the normal makeup (MU) tank and by realigning the discharge

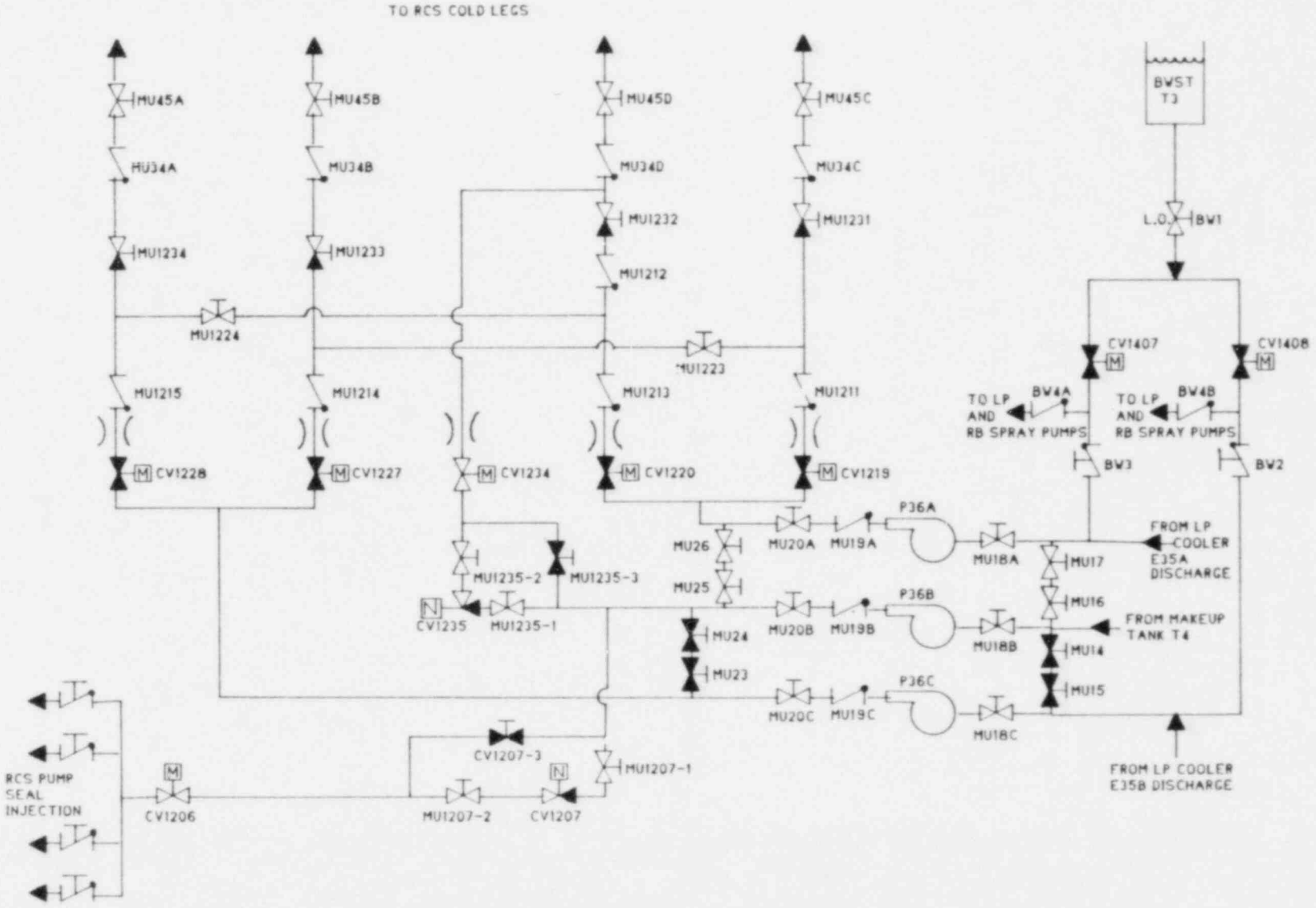


Figure 6-1. High Pressure Injection System.

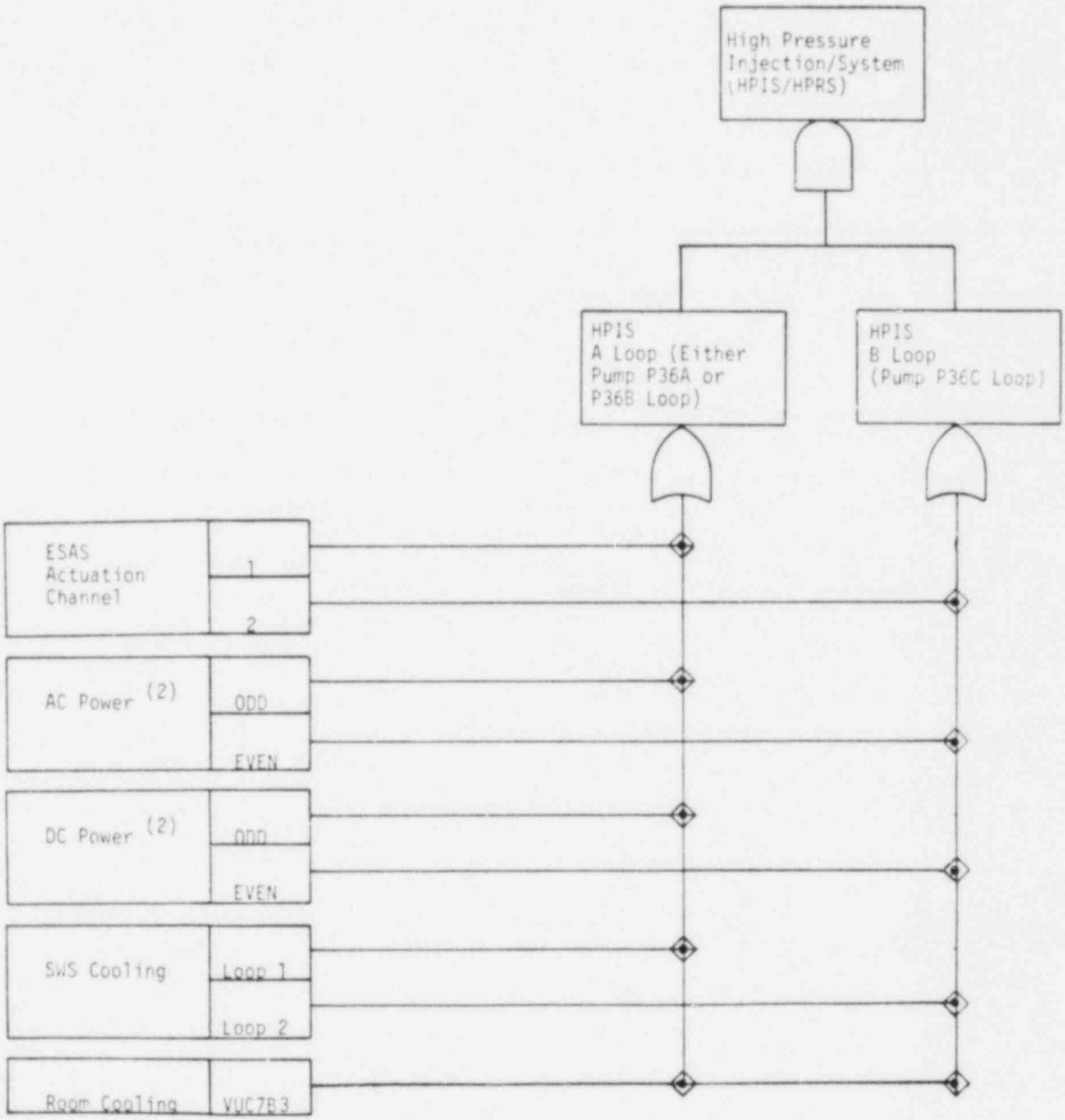
from the normal MU to the HPI piping. Although there are three pumps in the HP system, only two can be run at any one time, since there are only two electrical power source busses and each can power only one pump. The A and C pumps are each connected to a different electrical bus and pump B can swing between the two busses. During normal operation, pump B is aligned to the bus powering the normal MU pump. The like-aligned pump is then configured as an automatic backup to the operating MU pump and the opposite-aligned pump is the ES pump.

Another function of the HPIS is to provide cooling water to the reactor coolant pump seals. The service water system provides a backup method of seal cooling through the intermediate cooling water system (ICWS). The ICWS, however, is isolated upon an ESAS signal.

The success criteria for the system are dependent on the initiating event. For example, for some LOCA sizes, only one pump is necessary, but for other sizes, two are. Further discussion of specific success criteria is presented in Chapter 4 of this report.

An important system assumption is that the failure of decay heat coolers to cool the recirculation water during HPR will fail the HP pumps as they are designed to pump water which is no hotter than 200°F. The system dependencies of the high pressure system are shown in Figure 6-2. (It must be noted that humans are a dependency for all systems, as discussed in Section 6.3.7.)

An insight gained from this study is that, without recovery, single failures exist for the HP system. During the recirculation phase of a LOCA, the HP pumps are kept below their design operating temperature by a single room



(1) The success criteria here assumes one HP pump has to go into 1 of 4 headers.
(2) For all dependency diagrams, the AC and DC references include their necessary room cooling.
(3) Needed for HPRS only.

Figure 6-2. HPSI/R Support System Dependency Diagram.

cooler. Two other nonoperating coolers could potentially be used, but they must be started by the operator outside the control room.

6.2.2 Low Pressure Injection/Low Pressure Recirculation

The LPI/LPR System serves a number of functions during both accident conditions and normal operations. Along with providing decay heat removal and filling and draining of the fuel transfer canal during plant outages and refueling, the system also provides emergency core cooling (ECC) during a LOCA. Although the system is actuated by an ES signal (i.e., 1500 psig RCS pressure or 4 psig RB pressure), it is not until the reactor coolant system (RCS) pressure drops to about 150 psig (as during a large break LOCA) that the system is able to overcome the RCS pressure and inject borated water into the RCS. In addition to LP recirculation from the reactor sump, the system is utilized during the recirculation phase of a small break LOCA (i.e., RCS pressure remains high). This is the DHRS mode of recirculation discussed in Section 3.2.1. During HPRS recirculation, the system is required to feed cooled (via the decay heat coolers) water from the RB sump to the HP system for injection into the pressure vessel. Lastly, the LPRS in conjunction with spray recirculation provides long-term cooling to the containment as described in Section 3.2.1. A simplified drawing of the system is presented in Figure 6-3. The system dependencies of the low pressure system are shown in Figure 6-4.

The LPI/LPR system consists of two independent trains which draw water via a common header from the BWST. This header pipe also provides water to the HP and RBS systems. Each train of the LP system consists of a LP pump, a

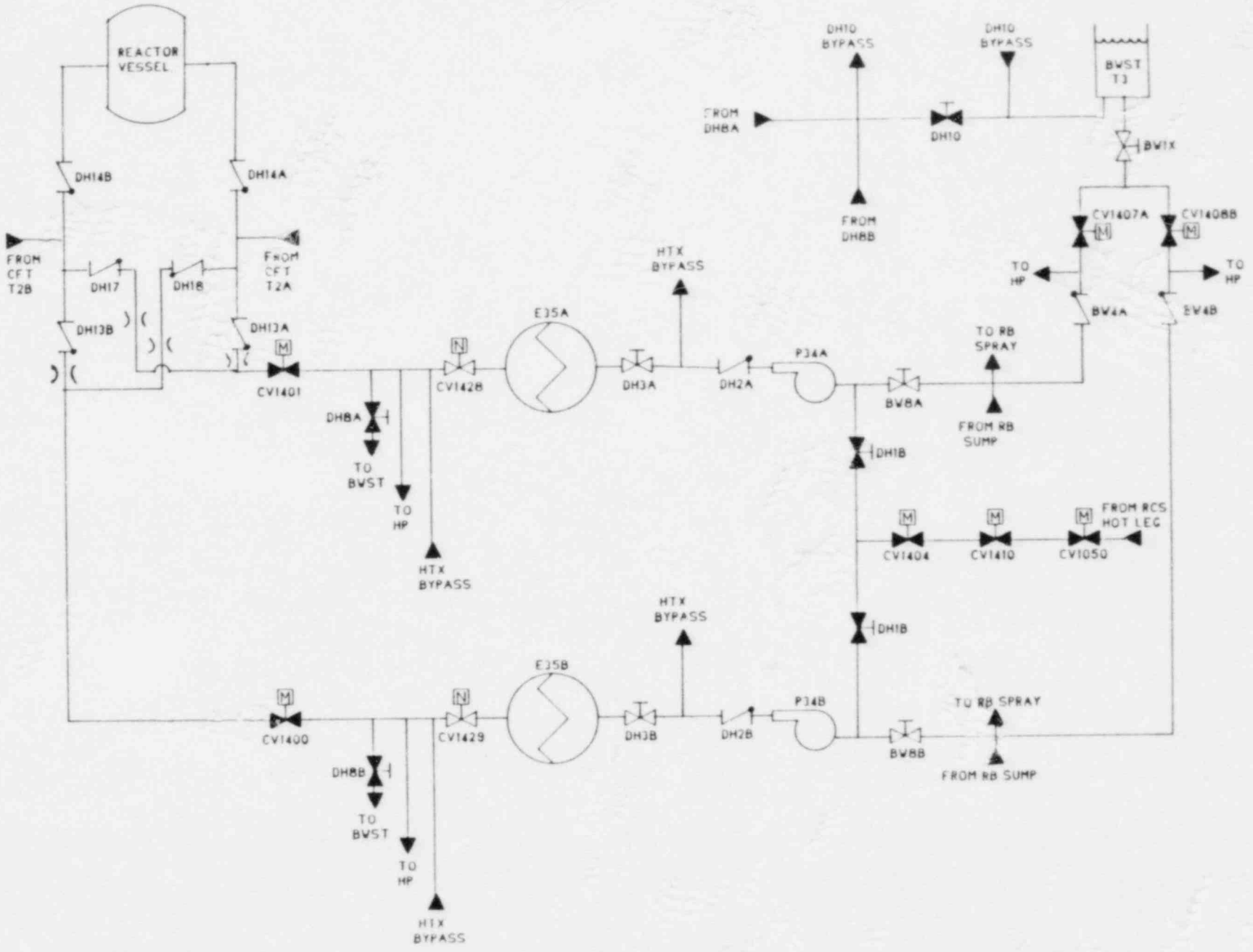
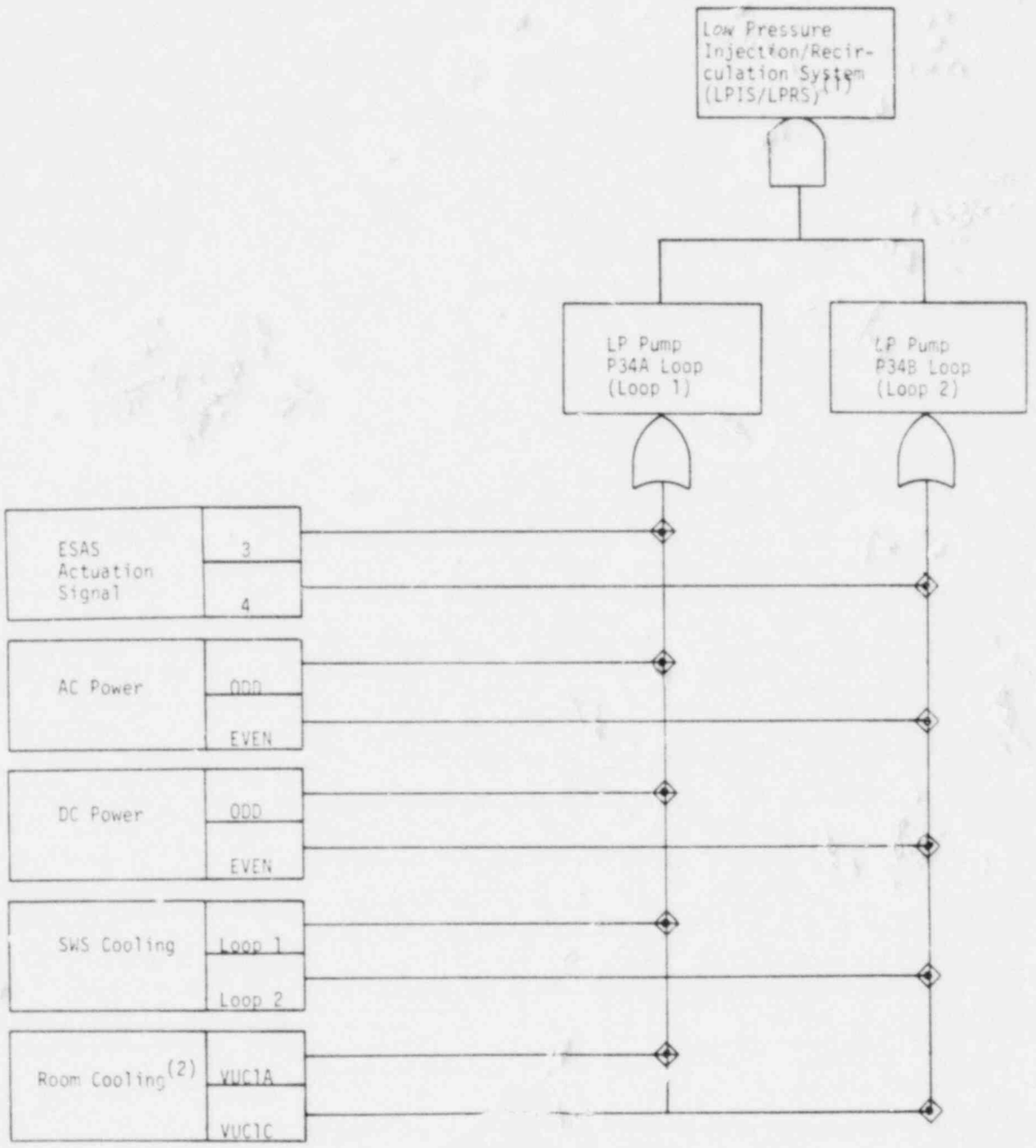


Figure 6-3. Low Pressure Injection System



(1) Success criteria here is one of two low pressure loops are required
(2) Needed for LPRS only

Figure 6-4. LPSI/R Support System Dependency Diagram.

decay heat cooler, piping and valves. The water is injected directly into the pressure vessel through two LP injection headers which are cross-tied and contain flow restricters such that each train injects 50 percent of its flow through each injection header. These injection headers are also used by the core flood system, with the tanks being isolated from the pressure vessel by two check valves, one in the LP injection line, one in the CFT header.

The system is realigned for recirculation manually by the operators. This is done by opening the motor operated isolation valves which allow flow from the RB sump to the LP pump suction. Flow is also manually aligned from the DH cooler discharge to the HP pump suction during HPR. This is accomplished by opening two manual valves (one in each train) in the cross-tie piping.

The success criteria of the LP system is that for LOCAs, one of two pumps is necessary. In addition, during the recirculation phase of the accident sequences, one of two pumps is required. More detailed information on the success criteria is presented in Chapter 4.

For this system cavitation of the LP pumps due to the nonclosing of CV1407 and CV1408, when switching to recirculation, was assumed to be negligible in the analysis for two reasons. Both the BWST and RB sump are at higher elevations than the LP pumps, and the pumps are gravity fed at their suction, and secondly, discussions with ANO-1 personnel revealed that cavitation of the pumps was not of concern if the valves were left open.

6.2.3 Core Flooding System

The Core Flooding System serves during the early phase of a large LOCA those ECC requirements that are beyond the capacity of the high pressure system but not yet within the pressure range of the low pressure system. The CFS fulfills its function by injecting a large volume of borated water into the pressure vessel when the RCS pressure drops to 600 psig or below. The system is passively operated, relying solely on check valves to keep it isolated from the RCS during normal operations. These check valves remain closed as long as the RCS pressure remains above the 600 psig maintained in the CFTs.

The CFS as shown in Figure 6-5 consists of two tanks or accumulators and the associated piping and valves which connect the tanks to the pressure vessel. Each CF line contains a normally locked open valve and two check valves. Sensors in the tanks actuate alarms in the control room to alert operators if the tanks are low on pressure or water level. The system dependencies of the core flooding system are shown in Figure 6-6.

The CFS shares its injection headers with the LPS. The check valve closest to the pressure vessel is part of the piping that is shared with the LP system.

Depending on the LOCA size, either one or both of the tanks is necessary for system success. This is discussed in Chapter 4.

6.2.4 Reactor Building Spray Injection/Reactor Building Spray Recirculation

For the purposes of this analysis, the reactor building spray system (RBSS) performs two functions. These functions are to (1) during injection reduce the post-accident pressure to nearly atmospheric pressure

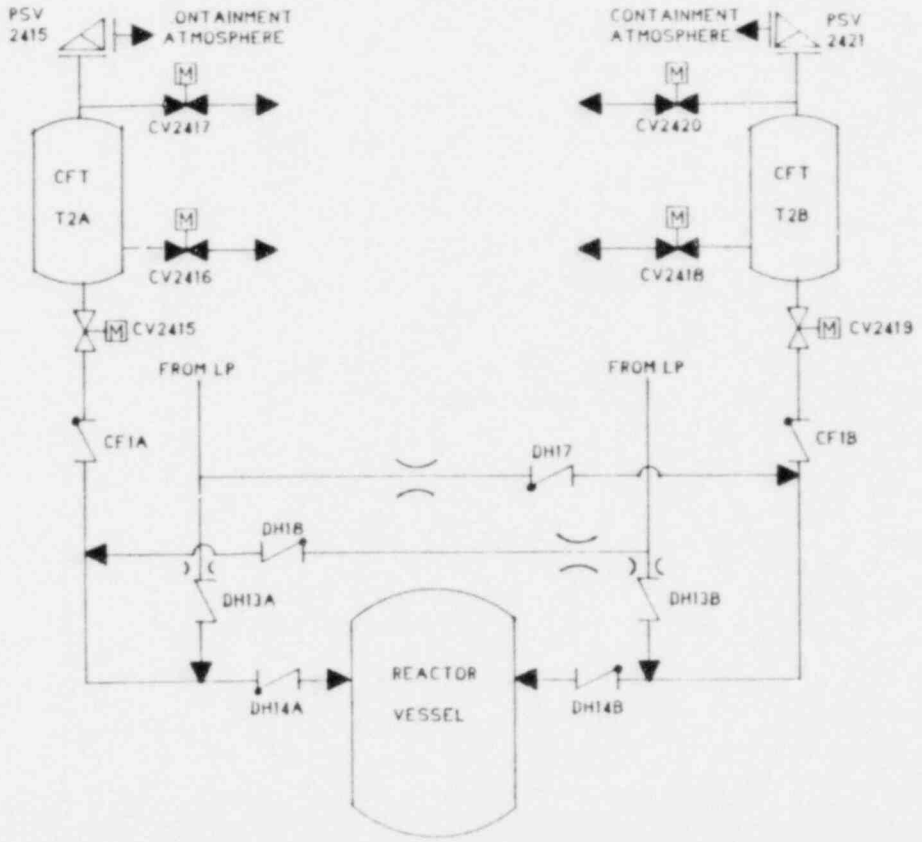
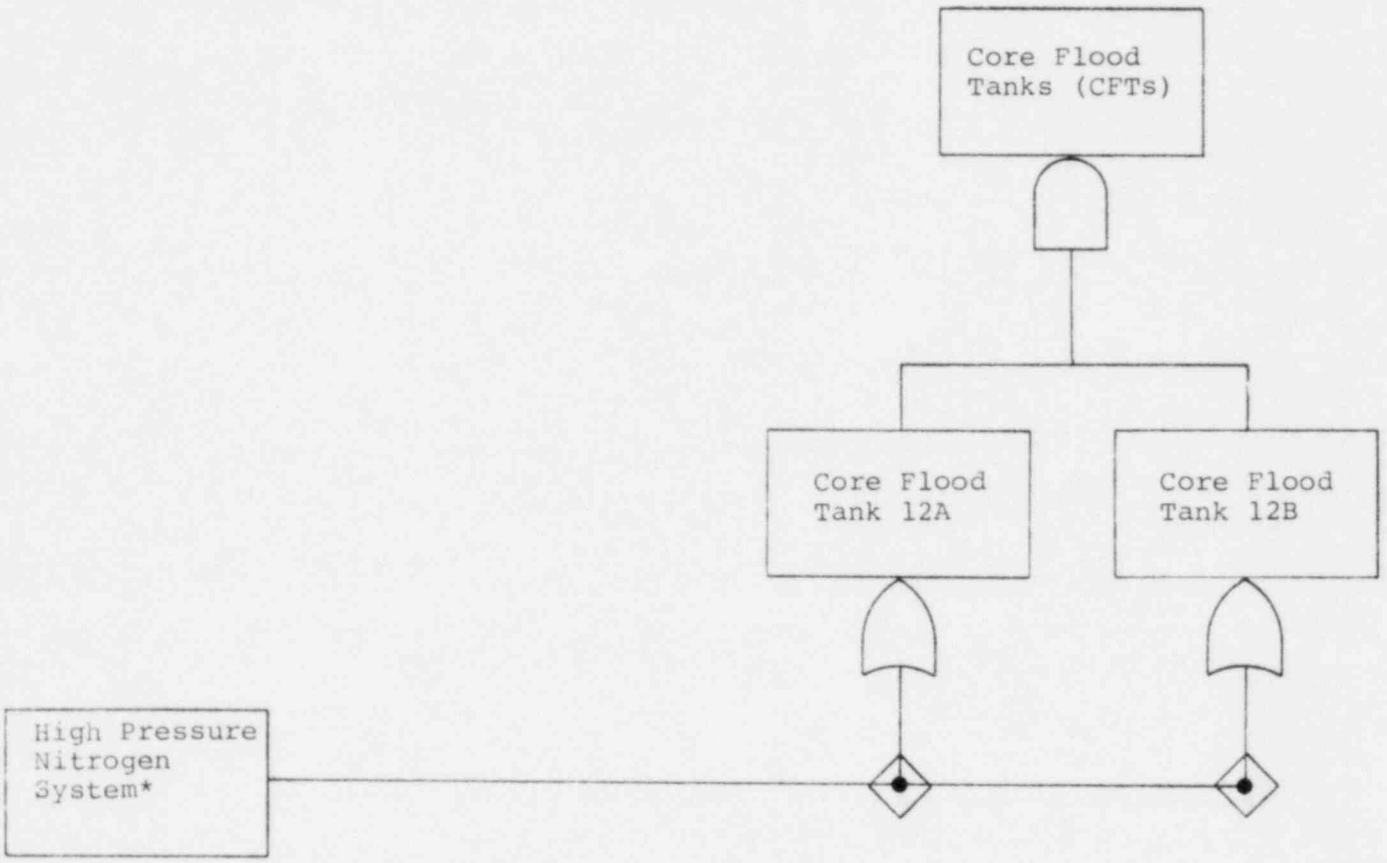


Figure 6-5. Core Flooding System.



*The analysis assumes the tanks are pressurized per Technical Specification requirement.

Figure 6-6. CFT Support System Dependency Diagram

and during recirculation act in conjunction with the low pressure recirculation system to remove heat from the containment and (2) remove radioactivity from the containment atmosphere.

The RBSS serves only as an engineered safeguard system and performs no normal operating function. It consists of two independent trains. In the event of a loss-of-coolant accident (LOCA) that results in a reactor building pressure of 30 psig, the RBSS is actuated by the ESAS and takes water from the low pressure injection lines that come from the borated water storage tank (BWST) and sprays it into the reactor building. Once the BWST reaches a low level, the RB spray pump suction is transferred to the reactor building sump. This first phase is called reactor building spray injection (RBSI) and the second phase is called reactor building spray recirculation (RBSR). A simplified schematic of the RBSS is shown in Figure 6-7.

The RBSS interfaces with the low pressure (LP) system in both the injection and recirculation phases. During the injection phase, in order for the water source to be available it is necessary that the outlet manual valve (BW-1) from the BWST and the motor operated valves (MOVs) (CV1407 and CV1408) in the low pressure line be open. (The manual valve BW-1 is normally locked open; however, MOVs CV1407 and CV1408 receive an ESAS to open on either of a 4 psig building pressure or 1500 psig coolant pressure. Thus, these valves should be open by the time the RBSS requires injection water.) The RBSS also requires LP valve action for recirculation. The operation of the injection and recirculation valves is discussed in the low pressure system description of Appendix B, and system dependencies are presented in Figure 6-8.

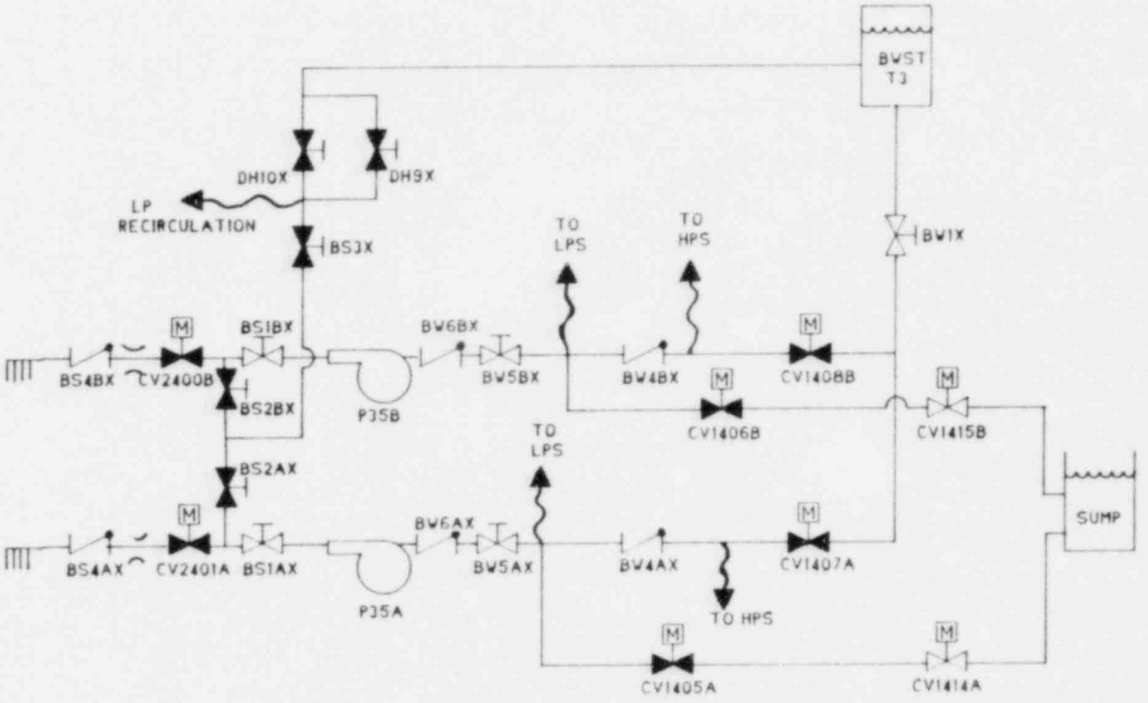


Figure 6-7. Reactor Building Spray System.

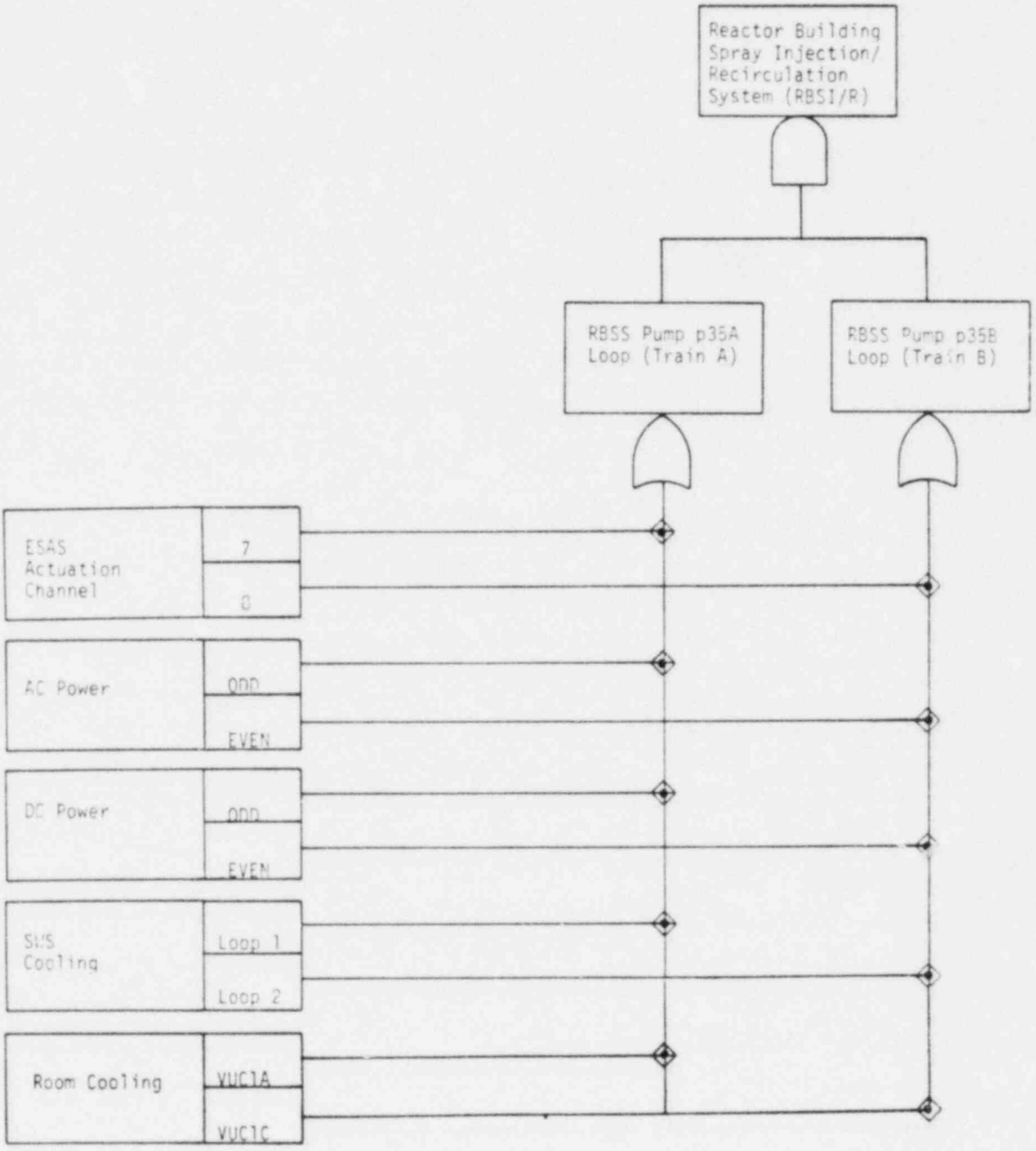


Figure 6-8. RBSI/R Support System Dependency Diagram.

For the two functions of the RBSS mentioned above, the success criteria is that one of the two trains must function.

Two system specific assumptions were made. First, the plugging of the spray nozzles was ignored. Second, the addition of sodium hydroxide to the spray was not modeled. The first assumption was deemed as being of low probability relative to other system failures. The second assumption results from the knowledge gained in previous studies.[2] The chemical addition to the spray does not significantly mitigate the offsite consequences of an accident.

6.2.5 Emergency Feedwater System

The emergency feedwater (EFW) system analyzed in this study is not the system in existence at ANO-1 at the time of the study. Changes to the system, however, have been approved by the NRC and are scheduled for implementation in 1982. Reasons for the upgrade are discussed in Section 4.2.2.5.

The purpose of the EFWS is to backup the main feedwater system (MFS) in removing post-shutdown decay heat from the reactor coolant system via the steam generators. During normal shutdowns the MFS is throttled down to a level capable of removing decay heat and the EFWS is not utilized. However, if the plant shutdown is caused by a loss of the MFS or the reactor coolant pumps, or if the MFS is lost subsequent to the plant shutdown, then the EFW system is put into operation. It is important to note that at some other PWRs the MFS is not throttled down during normal shutdowns as at ANO-1. Instead, the MFS is tripped and the backup feedwater system at these

plants, the "auxiliary" feedwater system, is put into operation during all shutdowns. This note is made to explain why the backup feedwater system at ANO-1 is labeled emergency rather than auxiliary.

The EFW system consists of two interconnected trains, capable of supplying emergency feedwater (EFW) to either or both steam generators (SGs) from either of two water sources under automatic or manual initiation and control. A simplified piping diagram is included as Figure 6-9. The system pumps take suction from either the condensate storage tank (CST) or from the service water system and discharge to the SGs. In the flow path between the EFW pumps and the SGs there are isolation valves, check valves, control valves, flow instrumentation, and pressure instrumentation to control the flow of EFW to the SGs. The EFW system is designed to provide a minimum of 500 gpm of EFW to the SGs at 1050 psig within 50 seconds of a system initiation signal.

Train A contains a motor-driven pump, and the pump of train B is turbine-driven. Except for electric motive and control power and actuation signals, the pumps, pump motor, and turbine are self-contained entities without support system dependencies. If AC power is not available, the B train can still provide complete system function relying solely on DC power. (System dependencies of the emergency feedwater system are presented in Figure 6-10.)

The success criteria of the system is to remove reactor coolant system decay heat from one of two steam generators. Either pump can supply sufficient feedwater for this purpose to either steam generator.

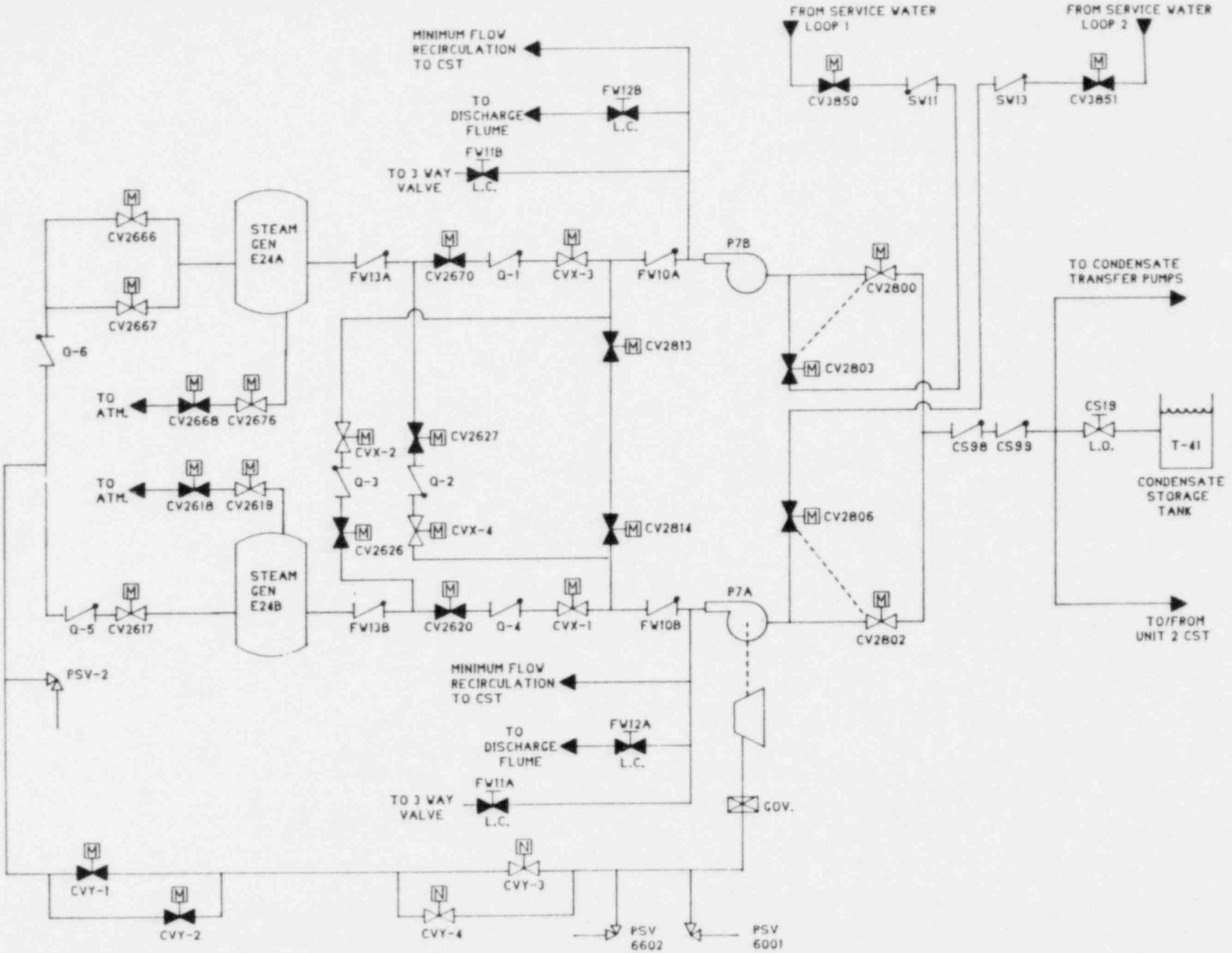
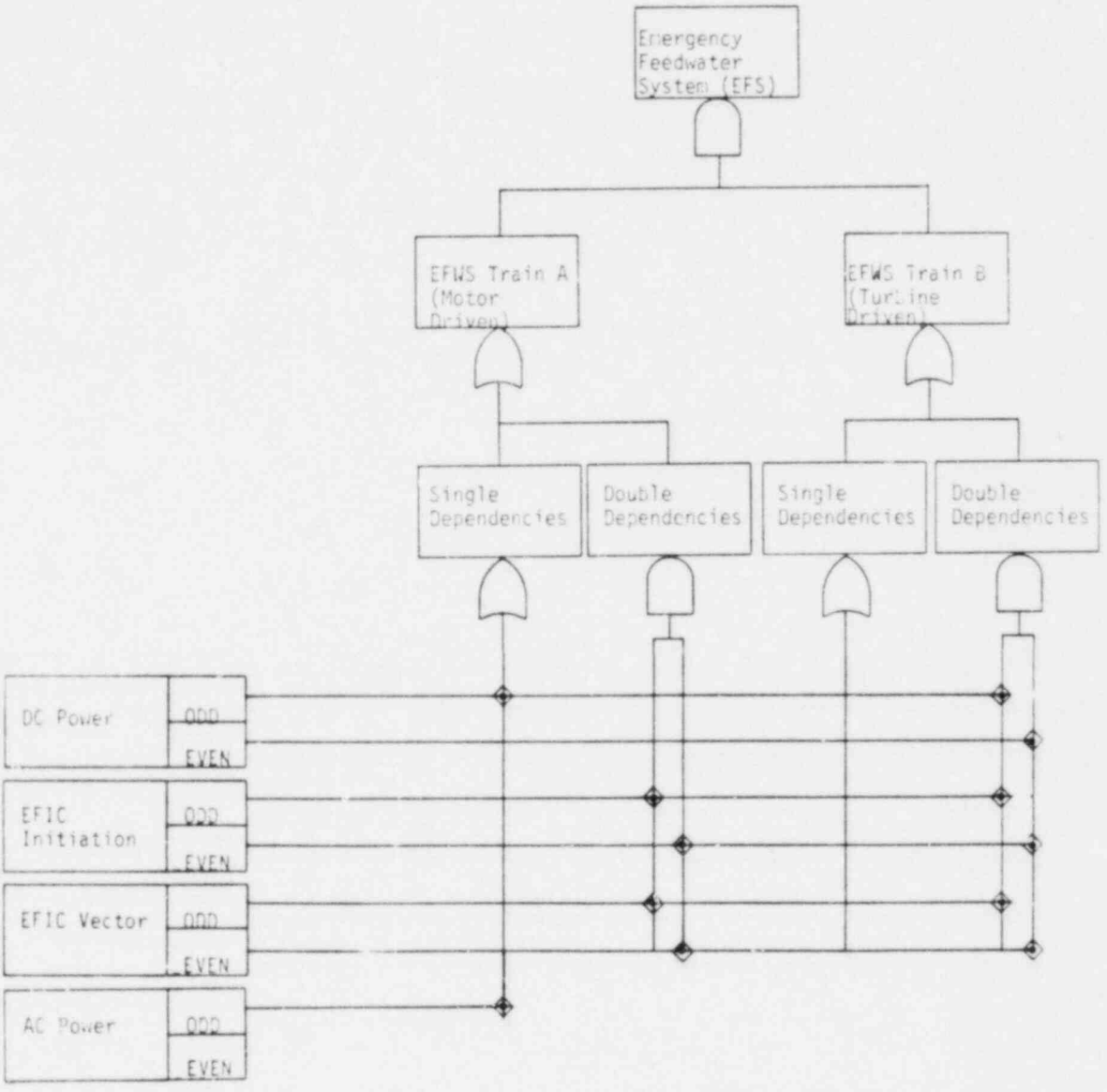


Figure 6-9. Emergency Feedwater System.



Dependency diagram assumes no ES signal is present.

Figure 6-10. EFS Support System Dependency Diagram.

A specific assumption of the analysis of this system is that the testing, maintenance, and circuitry for the system currently existing at ANO-1 are the same as that analyzed. In addition, it is assumed that the EFW pumps would fail by cavitation, if the CST source was unavailable, before the operator could realign the suctions of the pump to service water. This latter assumption is discussed in further detail in Appendix B-5 and also in the sensitivity analysis of Chapter 8.

6.2.6 Reactor Building Cooling System

The Reactor Building Cooling System (RBCS) is provided to limit post-accident reactor building pressure to the design value during steam evolution within the building due to an accident.

Emergency and normal cooling of the reactor building are performed with the same basic cooler units. Each unit contains normal and emergency cooling coils and a single speed fan. During normal plant operation, chilled water from the plant main water chillers is circulated through the normal cooling coils of the fans which are running. For emergency cooling all units operate under postaccident conditions with the heat being rejected to the service water system. ESAS-actuated dampers open to alter the flow from the normal to the emergency path.

The schematic flow diagram of the reactor building cooling system and associated instrumentation is shown in Figure 6-11. The reactor building atmosphere enters each of the fan coolers at the fan locations. All four fans discharge into a supply air plenum which distributes cooled air throughout the reactor building. One pair of units (VSFM1A and VSFM1B) is cooled by Service Water Loop 1 while the other pair (VSFM1C and VSFM1D) is cooled by

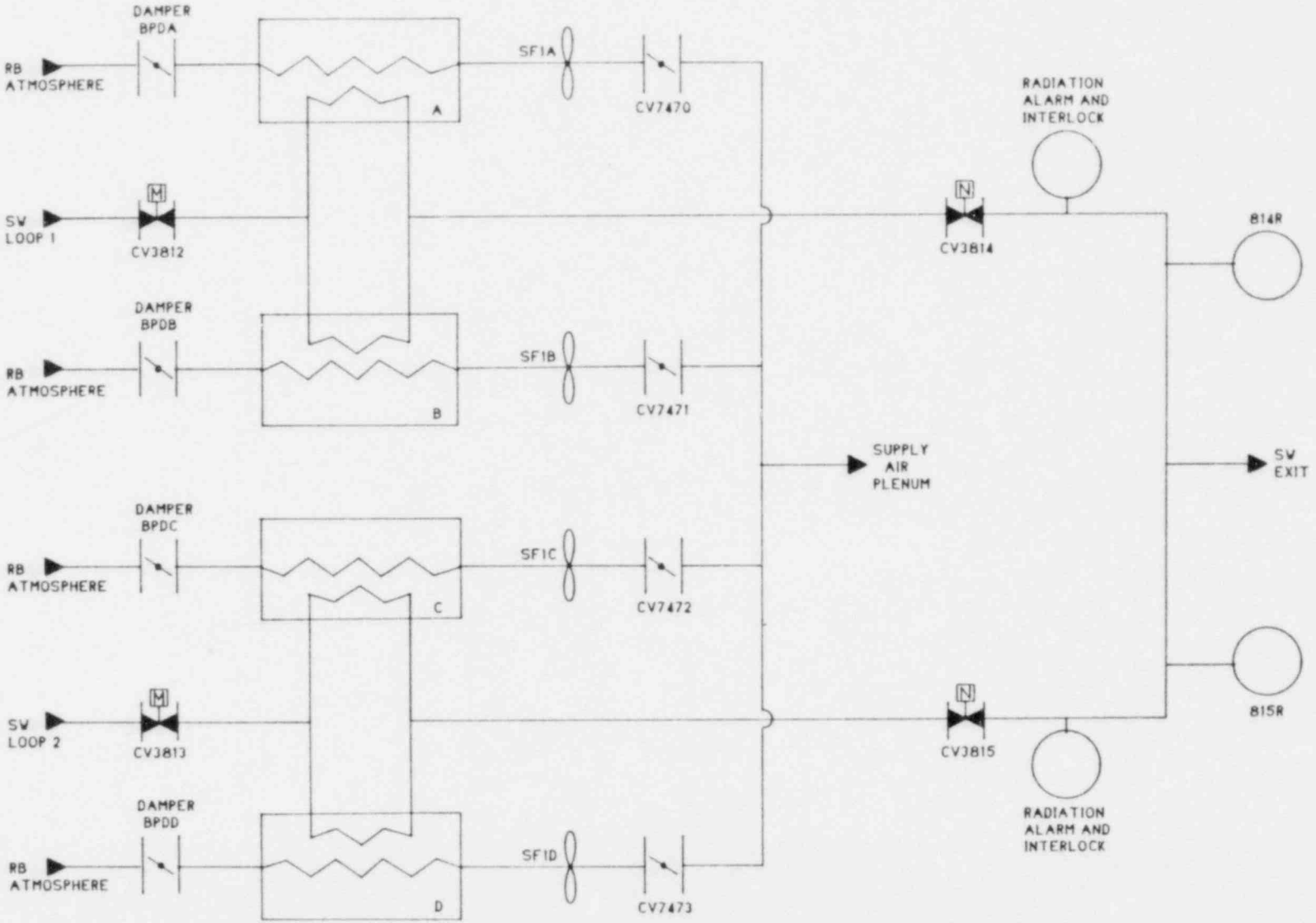


Figure 6-11. Reactor Building Cooling System.

Service Water Loop 2. The reactor building is normally isolated from the service water system by two ESAS-actuated, pneumatically operated valves and two ESAS-actuated motor operated valves. A safeguards actuating signal, generated by 4 psig pressure in the reactor building, will cause the valves to open. After the service water exits the reactor building, it is monitored for high radiation. High radiation in the service water closes the service water isolation valves and overrides any existing ES signal.

As with the service water and actuation signals, the four fans are divided as to motive power. The A and B fans are supplied from the odd emergency AC train, and the C and D fans from the even. Similarly, the associated valving is powered from the odd or even AC train, respectively, or the odd or even DC power train. The system dependency diagram for the RBCS is given in Figure 6-12.

Based on earlier studies, such as the NUREG/CR-1659,[2] the success criterion of the RBCS is that one of the four fan coolers must operate to fulfill the function of the RBCS.

6.2.7 Reactor Protection System

The Reactor Protection System (RPS) consists of redundant sensors, relays, logic, and other equipment necessary to monitor selected nuclear steam supply system conditions and to effect a reliable and rapid reactor shutdown (reactor trip) if any, or a combination of, monitored conditions reach specified safety system settings. Successful RPS operation protects the nuclear

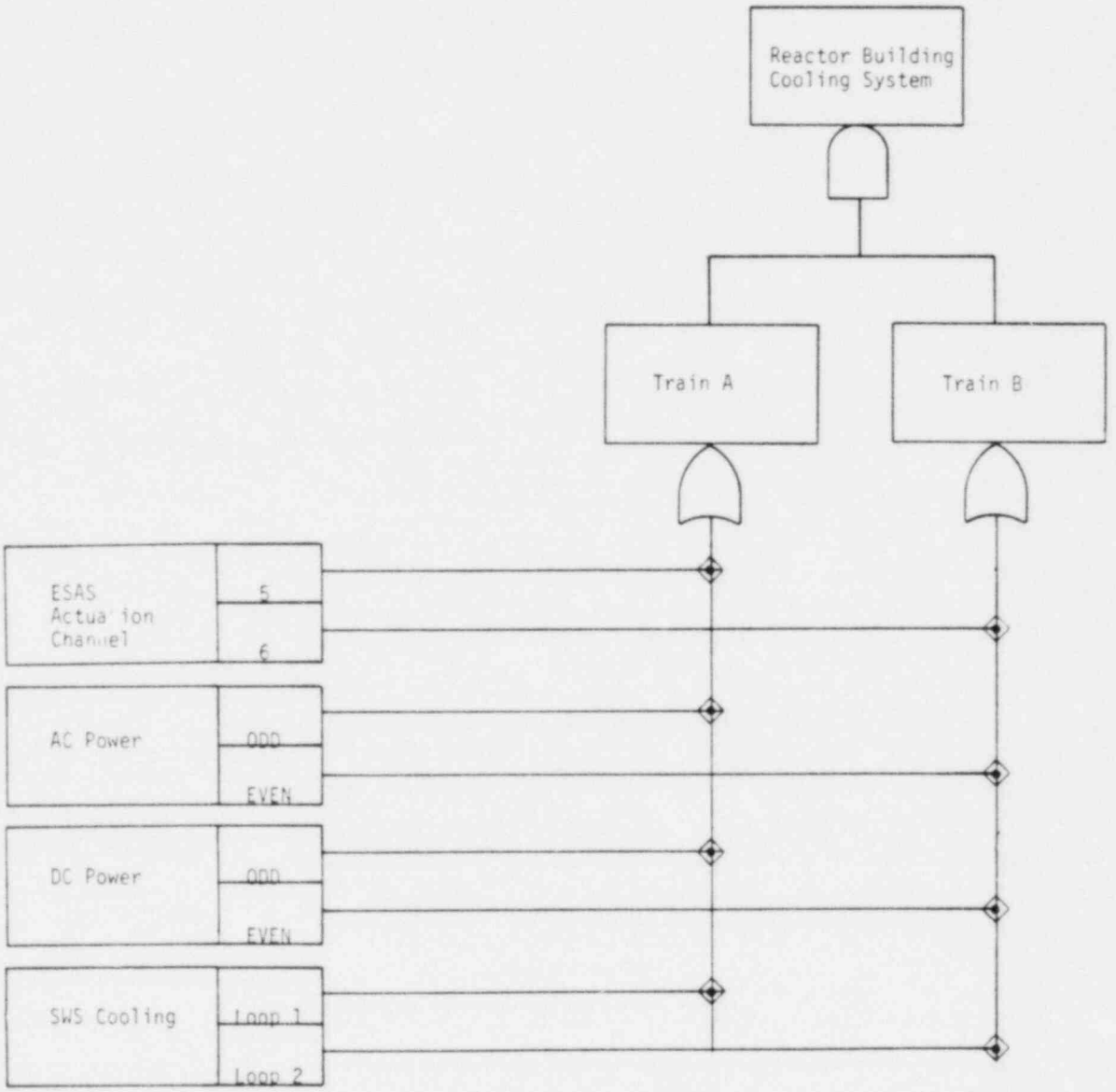


Figure 6-12. RBCS Support System Dependency Diagram.

fuel from cladding damage and helps prevent reactor coolant system overpressure by limiting energy input.

An overview of the reactor trip system is shown in Figure 6-13, and a more detailed system description is presented in Appendix B7. The trip parameters in four independent channels feed a bistable trip string with an output to the reactor trip module which includes a two-out-of-four logic interaction with the other channels. Trip signals interrupt main and secondary power to the power supplies for four safety rod groups and three regulating rod groups. Removal of holding power from the windings for the Control Rod Assemblies (CRA) allows the rods to drop into the core.

The trip parameters include high reactor coolant temperature, high and low reactor coolant pressure, high reactor building pressure, and various power comparisons. Two trip parameters recently added are loss of main feedwater and turbine trip. If automatic trip does not occur when required, a manual trip switch is provided which is independent of the automatic trip logic.

In addition, all modules are interlocked to trip the affected channels if removed. A manual bypass is provided to allow one channel to be bypassed without trip. If an attempt is made to bypass a second channel, a physical interlock will prevent the bypass.

The only system interaction of import for the RPS is that of humans. A procedural error could allow one channel to be left in the bypass mode after a test which would leave the RPS in a two-of-three system configuration. No dependency diagram is given because the only RPS dependency is the human element.

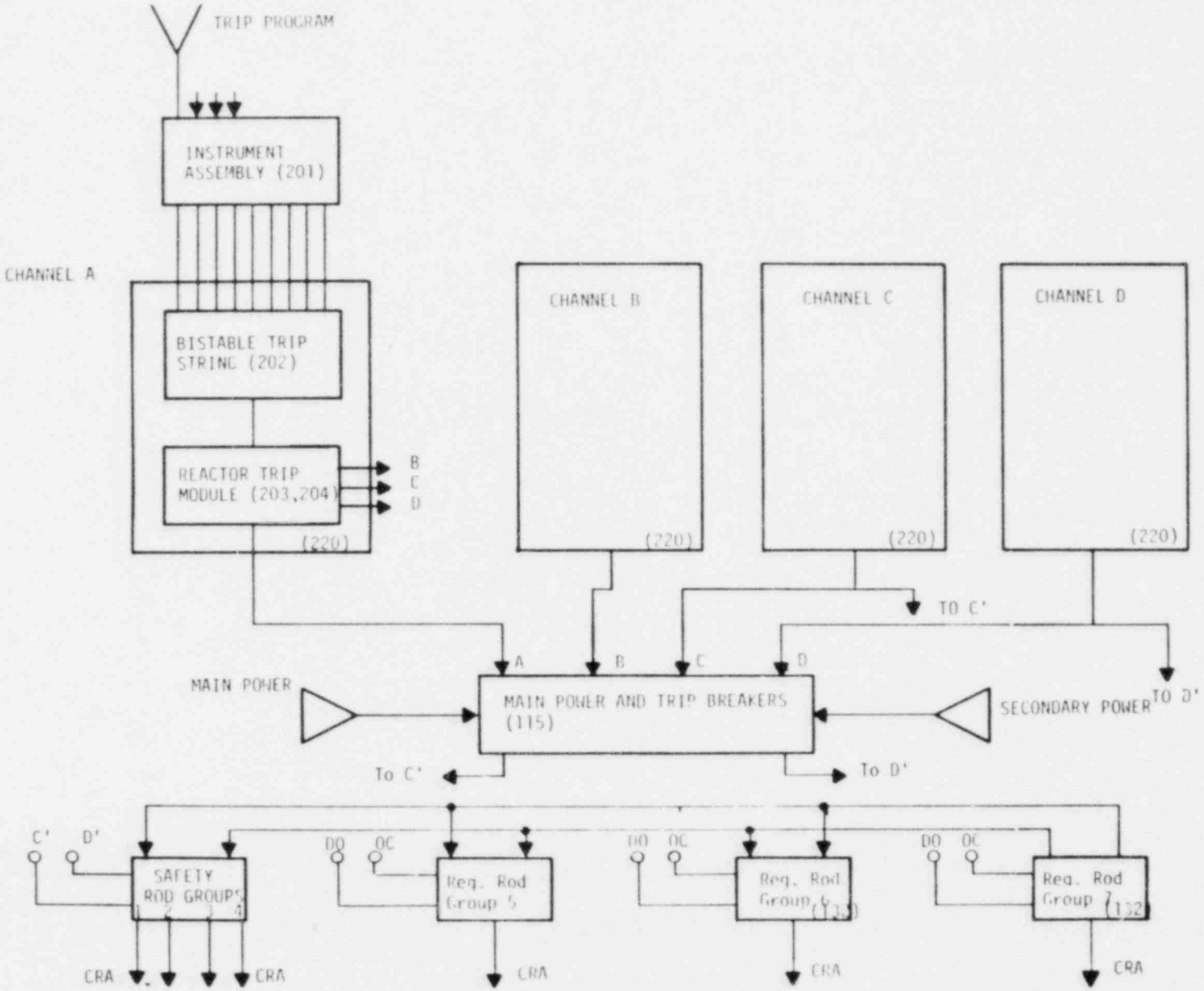


Figure 6-13. Reactor Trip System

The success criterion for the RPS is that it is required after transient initiators and small LOCAs and succeeds with one stuck rod group. For larger LOCAs, it is assumed that the vessel depressurizes through the break and the removal of moderator is sufficient to achieve reactor subcriticality. The RPS consists of eight groups of control rods, seven of which comprise the emergency part of the system. For transients and small LOCAs, successful RPS operation requires that six of the seven emergency groups be inserted into the reactor core.

Another assumption is that, in the fault tree development, no detailed modeling was done on the various reactor trip parameters. Instead, individual parameter unavailabilities were used as inputs to the bistable logic modules.

6.2.8 Power Conversion System

The Power Conversion System (PCS) at ANO-1 is designed to provide feedwater to the secondary side of the steam generators which, in turn, transfers energy to the turbine generator system. Following a reactor trip, the PCS is also capable of delivering feedwater to the steam generators at a reduced rate to provide for decay heat removal. This is accomplished by throttling the PCS feedwater flow to a level commensurate with decay heat and allowing this water to boiloff to the condenser or atmosphere. This section will describe the PCS and will also discuss the operation of the system after a reactor trip.

Figure 6-14 shows a simplified schematic of the PCS; the system dependencies are shown in Figure 6-15. The feedwater portion of the PCS consists of two pump

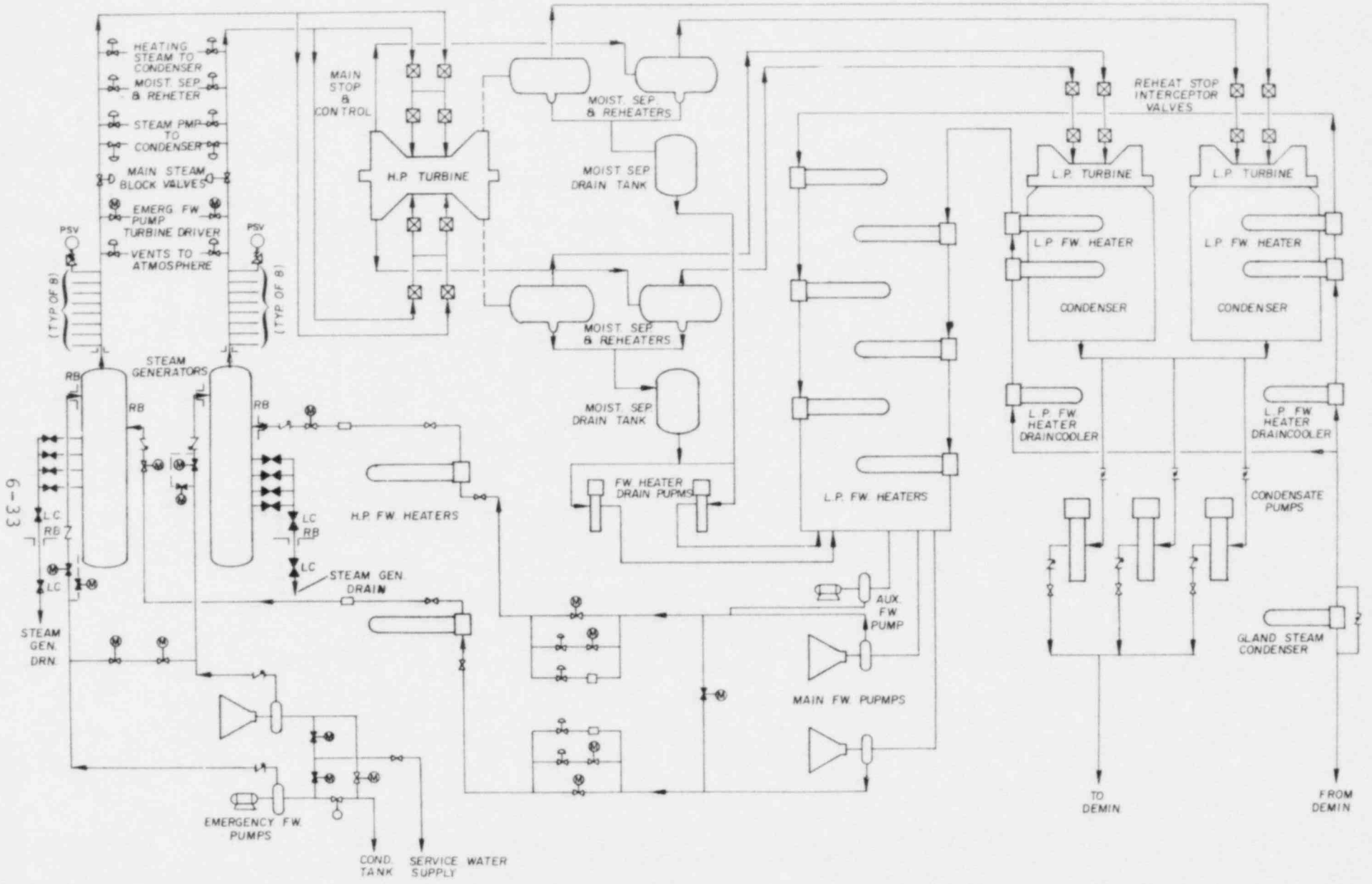


Figure 6-14. Schematic of Power Conversion System

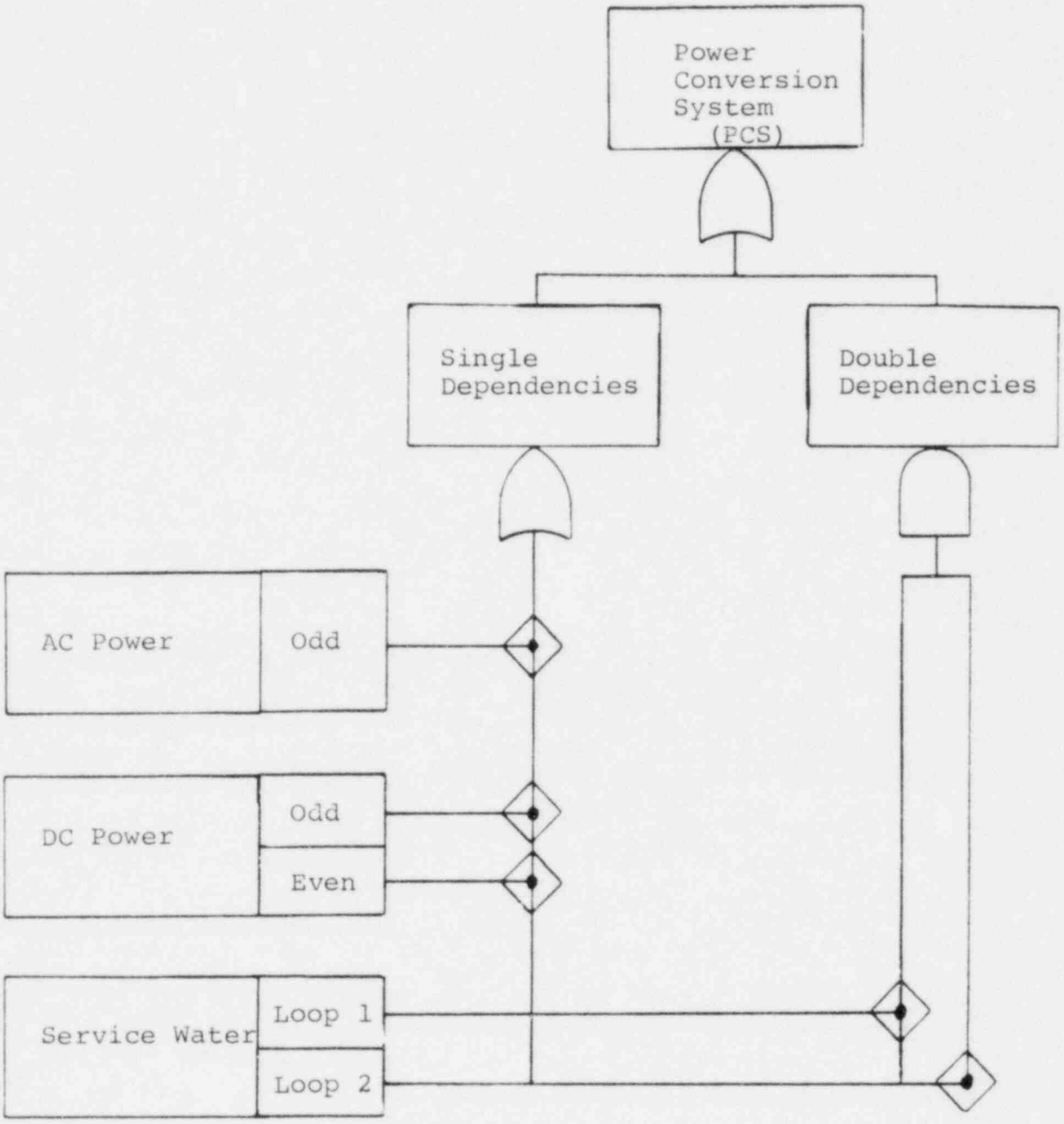


Figure 6-15. PCS Support System Dependency Diagram

trains. Three low-pressure motor driven condensate pumps feed two high-pressure steam driven main feedwater pumps and one high pressure motor driven auxiliary feedwater pump. These latter three pumps in turn feed both steam generators via two injection lines. The injection lines are interconnected by a line which contains a motor operated valve. Each injection line also includes three parallel lines, two with control valves for startup and low load modulation and one with a motorized gate valve for full load; one high pressure feedwater heater; one flow-tube type flow measuring device; isolation valves; and one check valve (containment isolation valve) just outside the reactor containment.

A detailed fault tree of the PCS was not constructed. Instead, industry data were used which represent the PCS unavailability due to independent causes not associated with the initiating events or systems modeled in the fault trees. Also, a review of all support systems interfacing with the PCS was made to determine which component failures already modeled in the fault trees would cause total interruption of the system.

6.3 ANO-1 Support Systems

The ANO-1 support systems are described in this section. More detailed descriptions of these systems are presented in Appendix B.

6.3.1 Engineered Safeguards Actuation System

The engineered safeguards actuation system (ESAS) monitors parameters associated with a major loss of reactor coolant accident and initiates operation of the proper engineered safeguards systems, i.e., emergency core

cooling, reactor building isolation and cooling, and reactor building spray, dependent on the severity of the accident.

In addition, ESAS starts the diesel generators but does not connect them to the emergency AC electrical system.

ESAS is composed of three redundant analog subsystems and two redundant digital subsystems as shown in Figure 6-16. Each analog subsystem contains two channels which monitor reactor coolant pressure and reactor building pressure. Each of the two digital subsystems contains five logic channels for initiation of safety action when two of three analog subsystems indicate such action is required. The components actuated by the odd and even digital subsystems are generally different but complementary, e.g., the pump in an odd system train is actuated by the odd ESAS train and the even, by the even.

Each analog train has two pressure sensors, one for the reactor coolant and one for the reactor building atmosphere. Each sensor is connected to a buffer amplifier, which in turn feeds at least two bistables. Trip points for the sensors are less than 1500 psig for the coolant and greater than 4 psig (high) or 30 psig (high-high) for the atmosphere, depending on which digital train is to be tripped. The analog components fail safe, i.e., removal of, or loss of power to, a module causes the train output to initiate, which results in a 1 of 2 logic configuration remaining. During normal shutdown, the low reactor coolant pressure trip can be manually bypassed during the cooldown pressure interval of 1750 to 1500 psig.

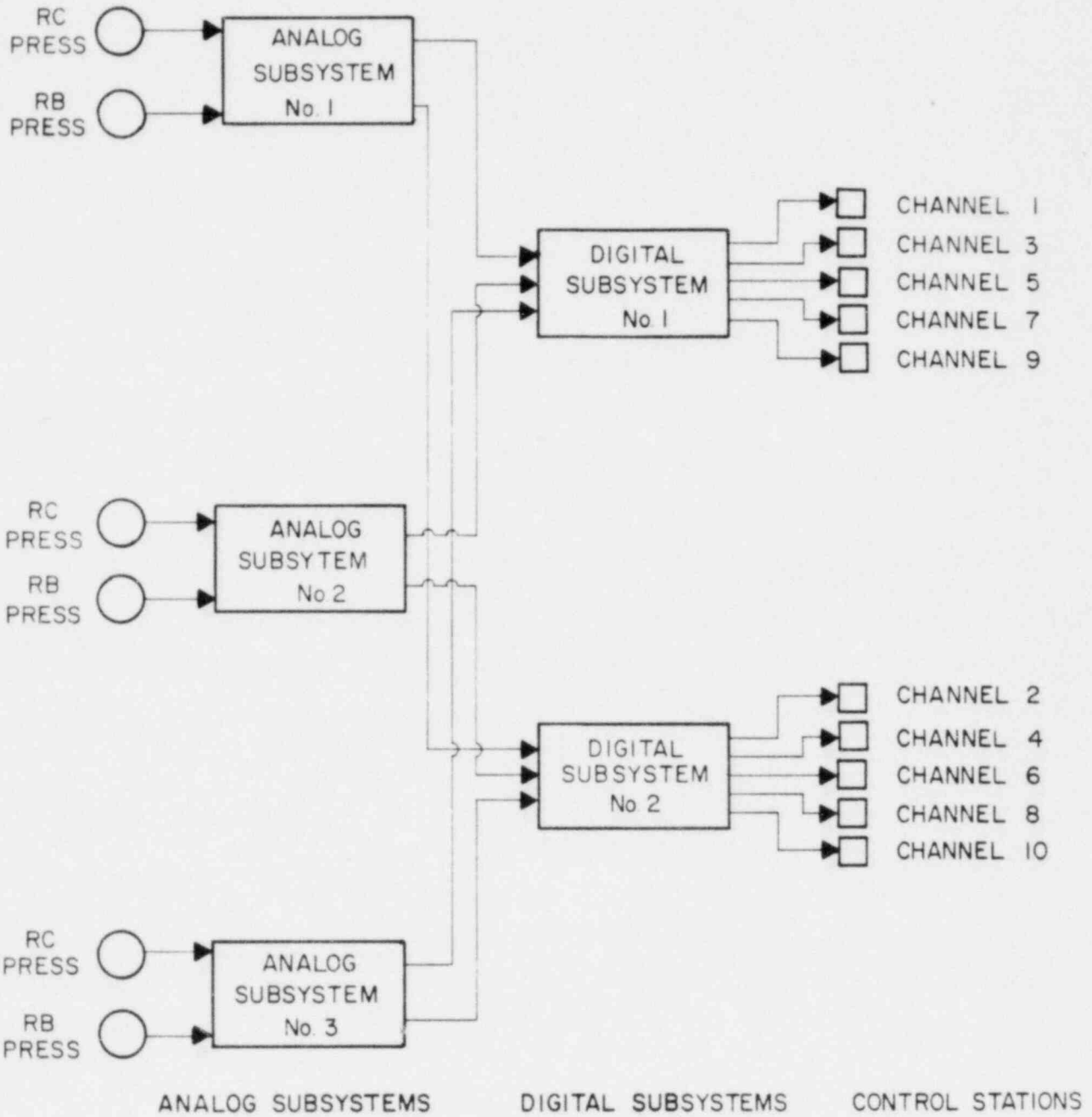


Figure 6-16. Simplified Schematic of Engineered Safeguards Actuation System.

For reasons explained in Appendix B-9, only eight of the ten digital channels are herein analyzed. Each channel can be tripped by one of two methods: two of three analog subsystems trip or manual action. Removal of, or loss of power to, a digital component module does not cause an actuation output signal. The modules in the digital portion can be tested on-line.

The success criteria of the eight logic trains is that each must send its signal to its actuated components when the specific accident sequence requires it. An insight gained in this study is that the human factor faults outweigh the hardware faults for this system. The miscalibration or misreading of instrumentation is as strong a contributor to system failure than is the hardware. This is discussed in more detail in Section 6.3.7 and in Appendix B-9.

6.3.2 Service Water System

The purpose of the Service Water System (SWS) is to provide cooling water for the following equipment during emergency conditions:

1. Reactor building cooling system cooling coils,
2. Diesel generator jacket heat exchangers,
3. High pressure pump lube oil coolers,
4. High pressure pump room coolers,
5. Circulating water pumps bearing lubrication,
6. Low pressure/building spray pump room coolers,
7. Low pressure pump(s) bearing coolers,
8. Low pressure system heat exchangers,
9. Building spray pump(s) bearing L.O. coolers,
10. Emergency feedwater system water sources.

The SWS consists of two redundant loops as shown in Figure 6-17. Normal cooling is supplied from Lake Dardanelle; however, an emergency pond is available in case of loss of flow from the lake. The service water is normally discharged back to the lake via the circulating water discharge flume. If the lake source is lost, the service water would be discharged back to the emergency pond.

There are three SW pumps. During normal operation, two of them are in use with the third pump in standby. All of the crossover valves in the common-pump-discharge header are open, but they close upon ESAS actuation. (The normal open position of the valves only recently became part of normal procedures.) No valve realignment occurs automatically unless there is an ESAS signal. The ESAS will only send an actuation signal to the two SW pumps that were already running in the normal mode. Success for the SWS is that all components requiring cooling in a specific accident sequence, receive sufficient SWS flow for that cooling. The success criteria of the SWS in this analysis are two-fold: that with an ESAS signal present and that without. With an ESAS condition, no credit is given for one loop backing up the other. That is, the loops are designed to isolate on an ESAS signal, and if they do not, the operator is trained to isolate them. In addition, any diversion from a loop subsequent to the ESAS signal, is assumed to fail that loop. For the case without an ESAS condition (or prior to one being initiated), credit is given for one loop backing up the other, and diversions to normal plant loads do not fail the SWS because the pre-ESAS loads are not as large.

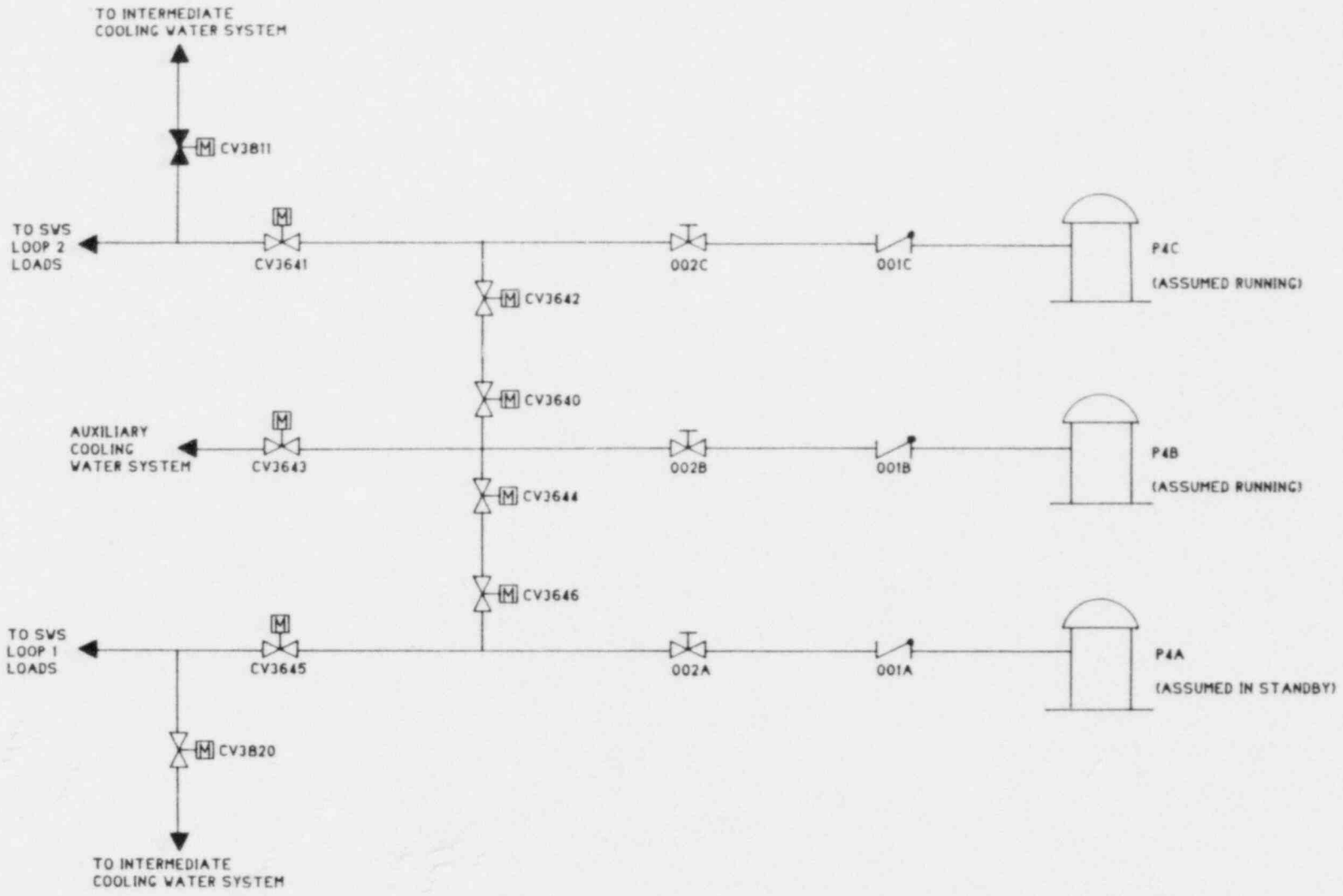


Figure 6-17. Service Water System.

The success criteria defined above are the major analysis assumptions for this system. The criteria are conservative in that any diversion in the post-ESAS alignment is a failure. These criteria are not those given by the plant. The criteria given by the plant were numerous because they were dependent on specific actions of sets of components. From the success criteria provided by the plant, the two criteria used in the analysis were identified as containing all the possibilities in an exact or conservative fashion. That is, the criteria used are the more general representation of those of the plant. Furthermore, the use of the developed success criteria aided the sequence analysis. With the criteria of the plant, not only would the specific criterion be dependent on the sequence, but it would also be dependent on the individual, minimal cut sets within a sequence.

6.3.3 Emergency AC Electrical System

The emergency AC electrical (EAC) system provides electric power to the ESF equipment of the mitigating systems. The EACS is composed of two trains (see Figure 6-18), each comprising a diesel generator, 4160 V switchgear, 480 V load centers and motor control centers, 120 V instrumentation panels, and associated transformers and circuit breakers. The normal power supply to the two trains is offsite, and each train has its own offsite connection at the 4160 V switchgear (A3 or A4).

There are three independent undervoltage sensing circuits per train. Two each are connected to A3 and A4, and one each to the 480 V load centers B5 and B6. Upon sensing an undervoltage condition, any of them will transmit a signal to open the 309 breaker for A3 (409 for A4), start the diesel in the train, and close breaker 308 (408 for A4).

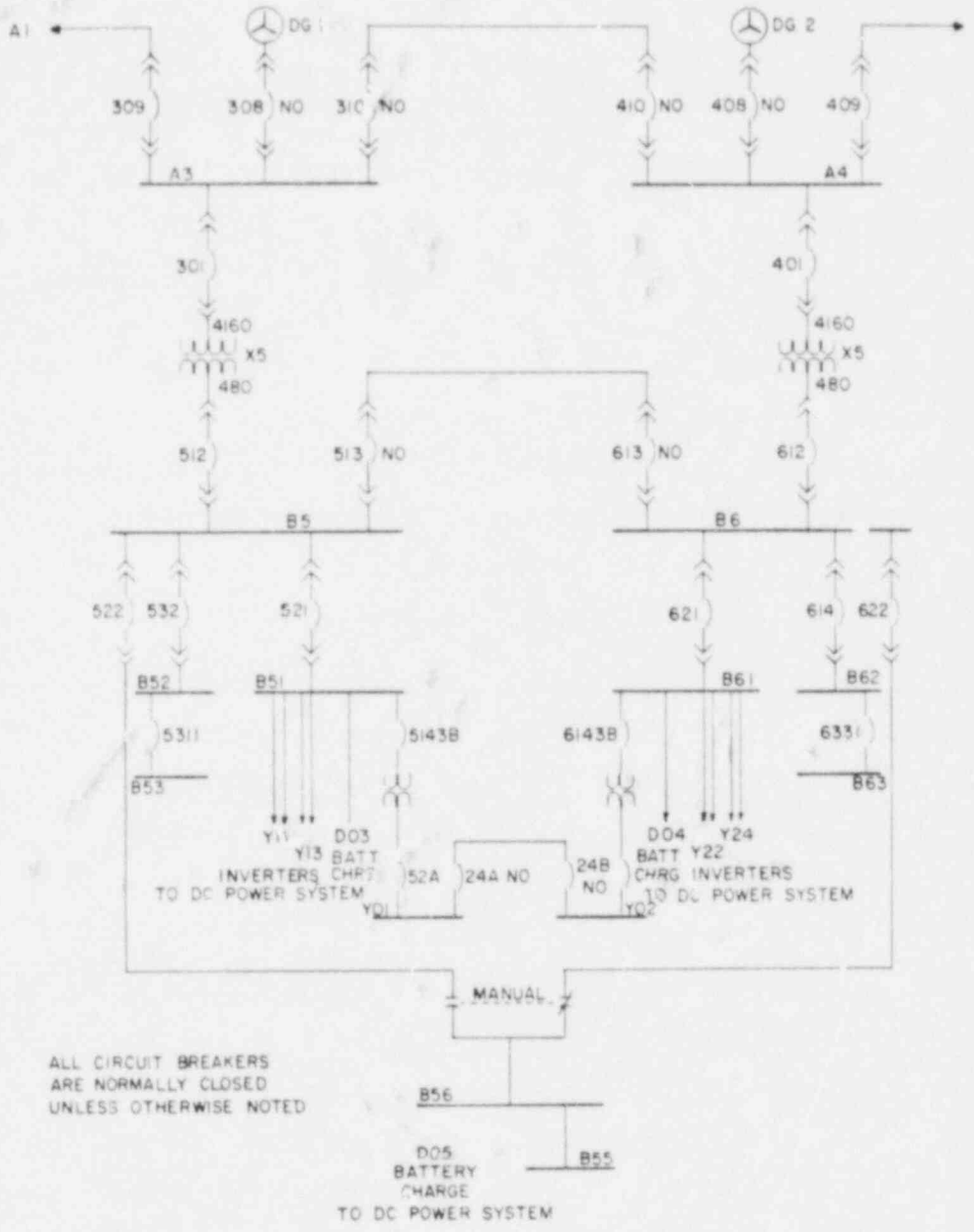


Figure 6-18. Emergency AC Electrical System.

Each diesel generator is equipped with a permanent magnet, and if the air start can crank a diesel to 300 rpm, it will start without field flashing from the DC power system. The diesels have a maximum rated starting time of fifteen seconds from the admission of the starting air. DC power is required, however, to open the solenoid valves in the lines connecting the air start tanks to the diesel. They cannot currently be manually opened. There are two, independent compressor tanks for each diesel. Subsequent to the start, DC power is required for diesel generator and circuit breaker control power.

As can be seen in Figure 6-18, A3 and A4 (and B5 and B6) are capable of being cross-tied. The cross-tie breaker sets are designed so that only three of the four can be closed at any time, and an undervoltage signal severs the tie, if it exists. Normal practice at ANO-1 is not to cross-tie the two trains, and the cross-ties are only considered here in the recovery portion of the analysis. In addition, an ESAS actuation signal from either channel 1 or 2 (see Section 6.3.1) will also open the crosstie breakers. Such a signal will also start the diesels, but it is not considered here for reasons explained in Appendix B.

Shift relief sheets at ANO-1 state that B56 is to be normally tied to B6. As explained in Section 6.3.4, this can result in having one DC train, and the complementing diesel air start valves, being dependent on the other train of the AC and DC systems. For conservatism, this dependent alignment was chosen for the analysis so that its effect could be ascertained.

At ANO-1, there is no load sequencing system, per se. Rather, ESAS sends out start signals to all components simultaneously, and the control circuitry of each major load component contains a time delay coil. Conservatively, for this analysis, it is assumed that a failure in these coils will cause the failure of the diesel which ultimately powers that coil. In addition to the ESAS time delay coils, each component has similar, parallel circuitry for an undervoltage signal.

It is assumed that the A3 and A4 switchgear rooms will eventually require cooling (see Section 6.3.5). This cooling is modeled as a support system fault of the longrunning equipment (e.g., pumps, fans) and not for the initially acting components (valves). The modeling of the service water cooling is the same. The reason is that these are failures of the electrical system after time has elapsed (five minutes for lack of service water, several hours for room cooling) which is not a failure mechanism for initially acting components.

The success criteria for this support system are that each bus is powered when ESF equipment requires it.

6.3.4 DC Power System

The 125 volt DC system provides continuous power for control, instrumentation, reactor protection and engineered safeguards actuation systems, and emergency safeguard actuation control (e.g., pumps) systems. In addition, it powers the control valves in the emergency feedwater system and provides control power for the diesel generators in the emergency AC electrical system.

The DC system is composed of two separate trains, each comprising a 125 volt battery, bus, and control panels (see Figure 6-19). In addition to the batteries, the DC system

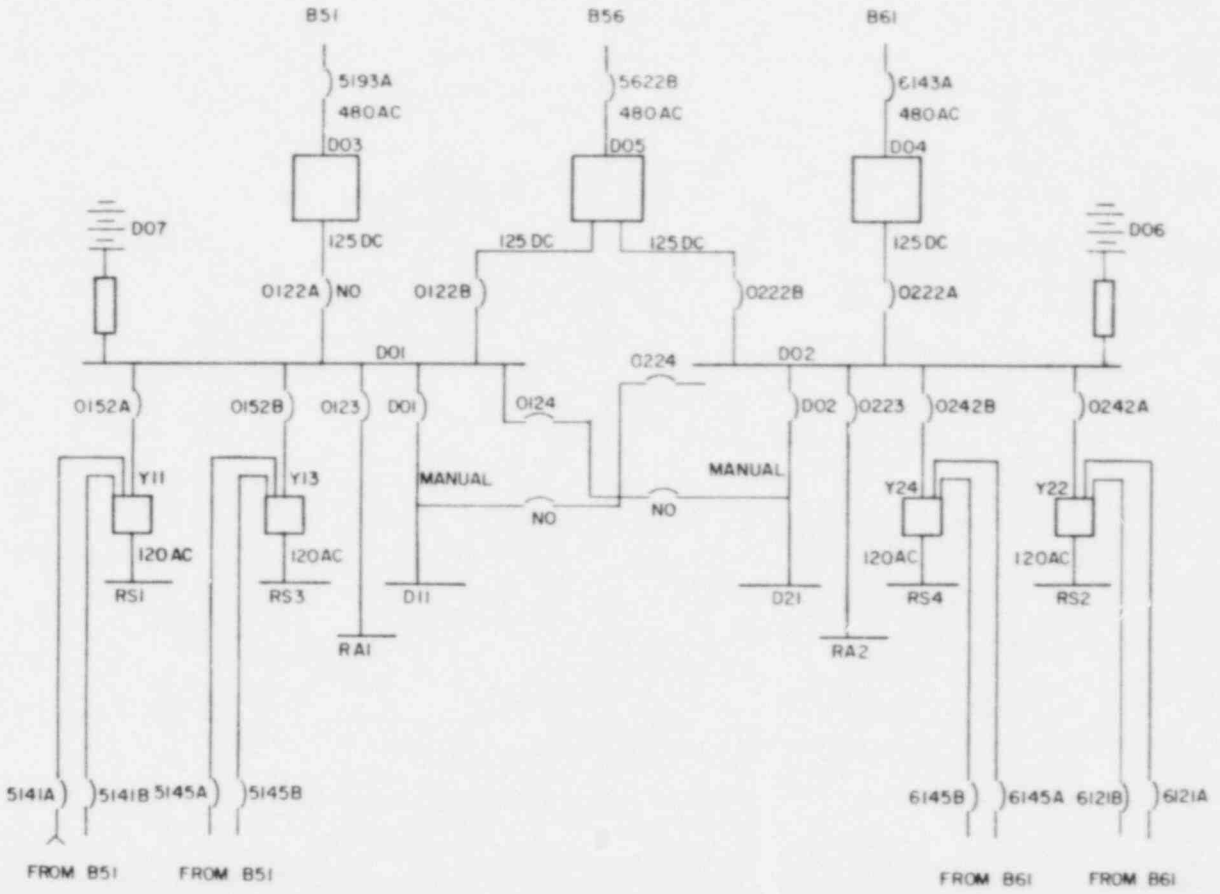


Figure 6-19. DC Power System.

is also supplied from the emergency AC electrical system via three battery chargers, with two in service at any given time. The charger alignment is rotated monthly.

The busses cannot be cross-tied. If maintenance is required on one train, its respective distribution panel can be manually aligned to receive power from the main bus of the other train. The inverters each have three sources of power: the respective DC bus, rectified and transformed 480 V AC from the emergency AC system, and transformed 480 V AC from the emergency AC system which does not actually pass through the inverter itself.

Each battery is designed to carry the continuous DC and vital AC loads for a minimum of two hours, following a station blackout. This time can be extended with the manual shedding of loads per the appropriate emergency procedure. Of crucial importance to system performance is the reliability of the batteries. Discharge tests are performed at the refueling shutdown, every eighteen months. The rest of the time, the batteries are floating on the chargers so that it cannot be precisely determined what the capability of the batteries is except at discharge. (Exceptions to this occur monthly when the chargers are rotated. Momentarily, the DC system is powered by the batteries alone so that severe degradation would be detected then). Other inspections include daily checks of the pilot cells, quarterly checks of all the cells and terminals, and an annual check of the cells as well as terminal cleaning. As a consequence of interim results of this study, the quarterly, and annual, tests are now staggered so as to lessen the human common mode inspection error possibility. Before this study, the tests were not staggered.

It is currently possible to have both battery chargers, which are in service, be receiving AC power ultimately from the same bus. B61 of the AC system is always fed from bus B6, and shift checklists stipulate that swing bus B56 should also be unless diesel generator 2 is undergoing maintenance (see Figure 6-18). This then results (see Figure 6-19) in both battery chargers receiving power from B6.

It is assumed that the battery rooms will eventually require cooling (see Section 6.3.5). This cooling is modeled the same as that for the switchgear rooms and the diesel generator service water cooling, which was discussed in Section 6.3.3.

The success criterion for the DC power system is that all components requiring either DC motive or control power receive it. An important assumption in this analysis is that the battery chargers can supply DC power without the batteries, i.e., they are an independent DC power source.

6.3.5 Battery and Switchgear Emergency Cooling System

The purpose of the battery and switchgear emergency cooling system (referred to as ECS) is to provide sufficient cooling to assure that electrical units which must operate during emergency conditions will not fail due to excessive heat. The rooms with electrical equipment in them, which could fail due to overheating, are the two battery rooms and the two switchgear rooms. The former inclusion is based on an APL analysis[25] which showed that after one hour without cooling the room temperature exceeded that of the duty ambient reading of the batteries. The cooling requirements for the switchgear rooms were not studied in the APL analysis, but for the sake of

completeness, the failure of such cooling is assumed in this study to fail the equipment in the switchgear rooms.

The ECS consists of two independent identically configured chilled water trains, which provide cooling to the rooms noted above, and two refrigerated air units which provide additional cooling capacity for the north and south battery rooms only. Each chilled water train comprises a chill water unit (CWU), three ventilation unit coolers (VUCs) and associated plumbing. A simplified schematic of chilled water train A is shown in Figure 6-20. The schematic for train B is similar. Additional cooling for the north and south battery rooms is provided by self-contained air cooled refrigeration units which are independent of the chilled water system (see Figure 6-21). A single refrigeration system is provided for each battery room. Each system consists of a condensor unit, an evaporator/blower unit and a thermostat. Each unit has sufficient capacity to accommodate 100 percent of the heat load in its associated battery room.

As an interim result of this study, the test procedures at ANO-1 have been changed to actually test the thermostats under a heat load. Until this time, they had never been tested.

For the chill water units, the odd ECS train cools odd components of the emergency AC and DC systems as well as is powered by them. Likewise, the even train cools and is powered by the even train. The refrigeration units, however, are both powered by the swing bus of the emergency AC system, which is normally aligned to be fed from

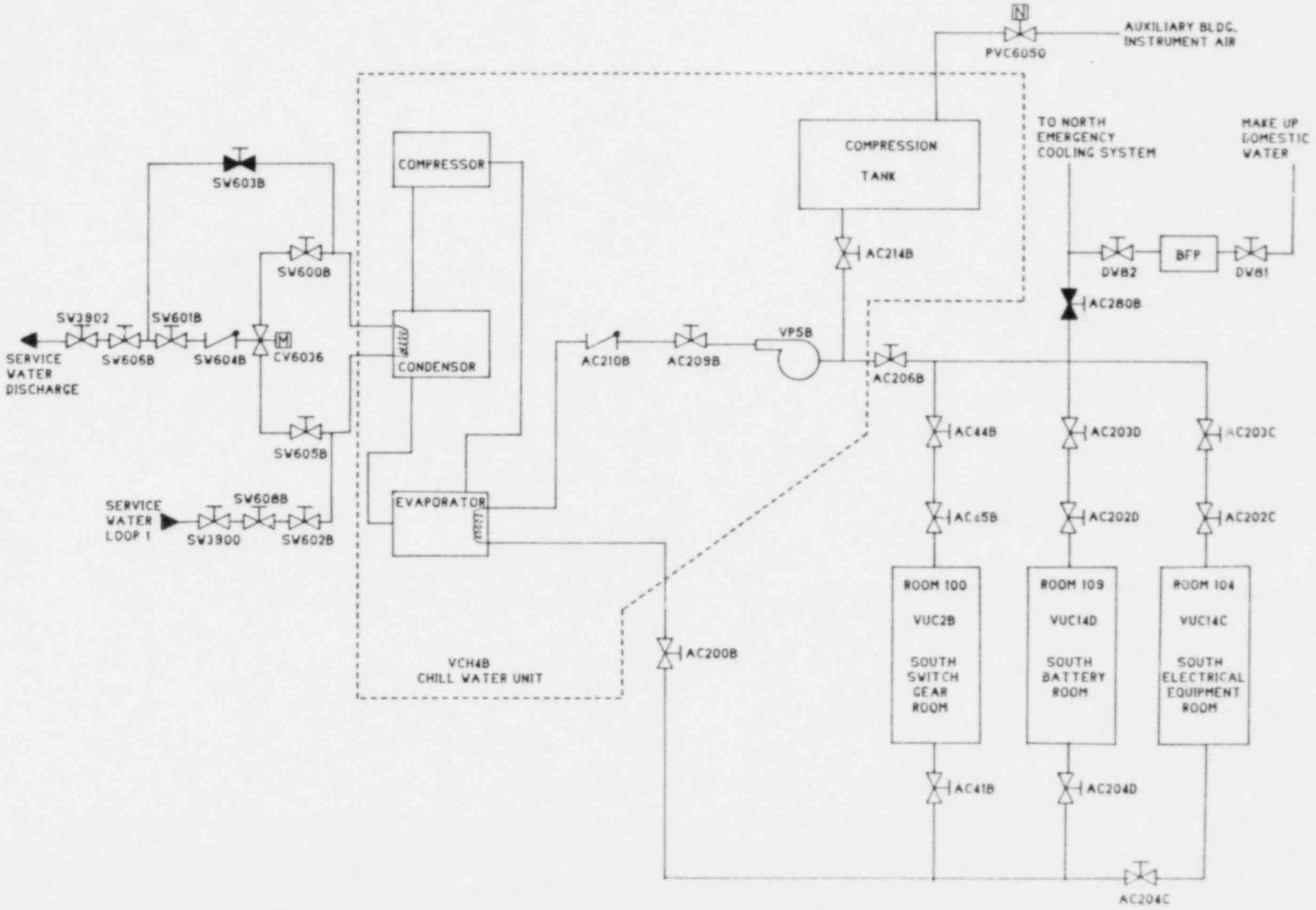


Figure 6-20. Chilled Water System, Train A.

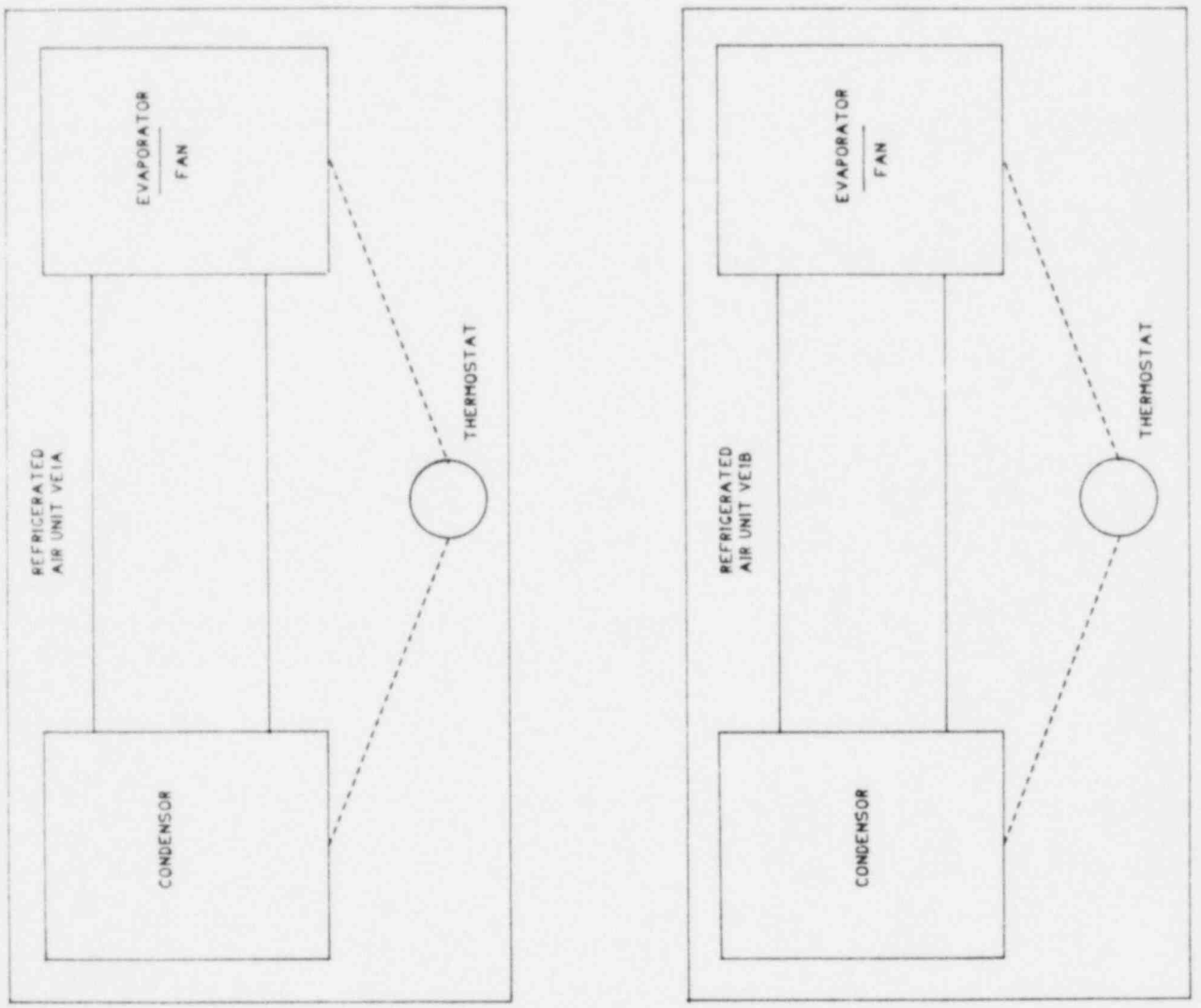


Figure 6-21. Schematic of Refrigeration Units.

B6. Thus, one of the cooling units for the odd train battery is normally powered by an even train component.

The success criteria of the ECS are four-fold: each of the four rooms, mentioned above, must have cooling. For each of the switchgear rooms, this means success of the associated chill water unit. For each of the battery rooms, these criteria mean that either the associated chill water unit or the refrigeration unit must succeed.

6.3.6 Emergency Feedwater Initiation and Control System

As mentioned in Section 6.2.5, the EFW system analyzed is not yet installed at ANO-1. This is also true of the Emergency Feedwater Initiation and Control (EFIC) system. EFIC is actually three systems: initiation, vector, and control. The latter was not studied in detail in this study due to a lack of sufficient specific information. The expected motive and control power dependencies were modeled, and in this analysis, it was assumed that the control function had to be operable throughout the accident.

6.3.6.1 EFIC Initiation

The purpose of the initiation system is to automatically initiate emergency feedwater when:

1. all four reactor coolant pumps are tripped,
2. both main feedwater pumps are tripped,
3. the level of either steam generator is low,
4. the pressure in either steam generator is low.

The system also provides for manual EFWS actuation and control after either automatic or manual actuation.

The EFIC initiation system consists of four channels of solid-state logic. Each of the four channels (A, B, C, and D) is provided with input and initiate logics. Channels A and B also contain trip logics. A simplified block diagram of the initiation system is shown in Figure 6-22.

Each channel monitors inputs by means of the input logic and ascertains whether action should be initiated by means of the initial logic. Channels A and B monitor signals from each of the four initial logics by means of the trip logics, and transmit signals to circuit breakers for EFW motor-driven pump P7B and for valves CVY1 and CVY2 which control steam flow to the EFW turbine-driven pump P7A (see Figure 6-9).

The trip logic is a two-of-four configuration. That is, at least two of the four input logic trains must generate an output signal before the trip logic will pass initiation signals to the EFWS equipment.

The EFIC initiation system succeeds when an actuation signal is given, when required, to the three components listed above. The analysis assumes that the input signal for system processing results from loss of main feedwater pumps and low steam generator levels and not from other possible initiators because not all initiators will occur in a given accident sequence. The assumption that the initiators are loss of MF pumps and low SG levels is conservative in that these encompass the components of the others. Additionally, no information on test and maintenance is known for this system. The test and maintenance experience of ESAS was examined for possible usage in EFIC.

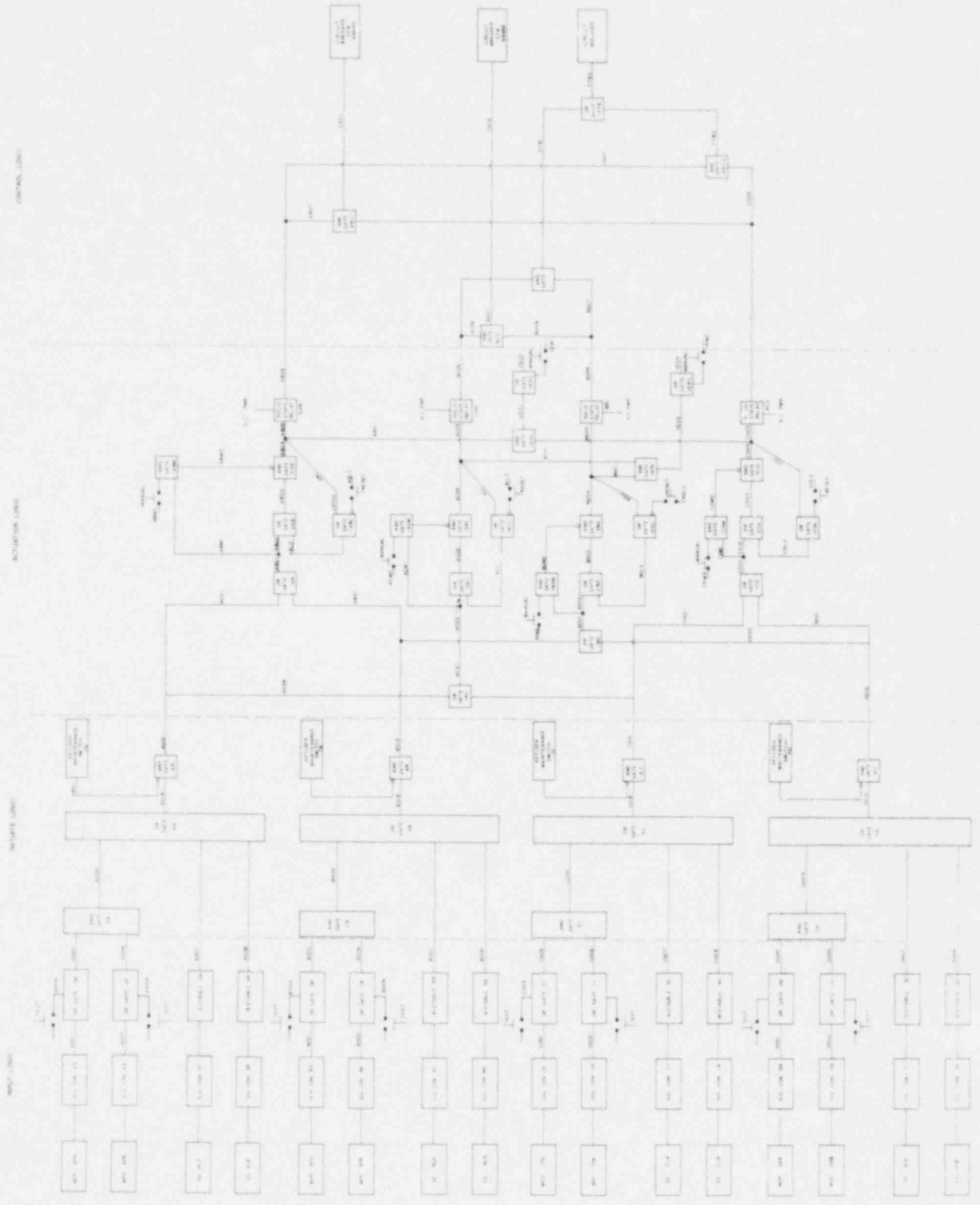


Figure 6-22: EFIC INITIATE SYSTEM

6.3.6.2 EFIC Vector

In this study, the detailed, fault tree analysis of the EFIC vector system is limited to one of its functions: to open the four normally-closed block valves (CV2620, CV2626, CV2627, and CV2670) in the EFWS which block discharge flow from the EFW pumps to the SGs (see Figure 6-23). The functions resulting from SG overfill or blowdown were also studied, but not to the same detail, because the overfill and blowdown faults were not significant contributors to the IREP sequences analyzed.

The EFIC vector system has four channels of solid state logic. Each of the four channels monitor steam generator pressures, steam generator levels, and the status of the EFIC initiation system. Each channel provides position signals to two valves in the lines between the emergency feedwater pumps and the steam generators. The position of the four block valves controlled by vector channels C and D determines whether emergency feedwater is directed to both steam generators, to one steam generator or to neither steam generator. A simplified block diagram of the vector logic system is shown in Figure 6-23.

The vector system functions only when the EFIC initiation system is activated. The assumption of manual control in the initiate system will return the block valves to manual control.

The vector system succeeds when each of the four block valves receives an actuation signal. As stated above, the failure mode of interest is the failure to open these valves. Test and maintenance were not available for the same reason as for the initiate portion, but ESAS experience was again examined. In addition,

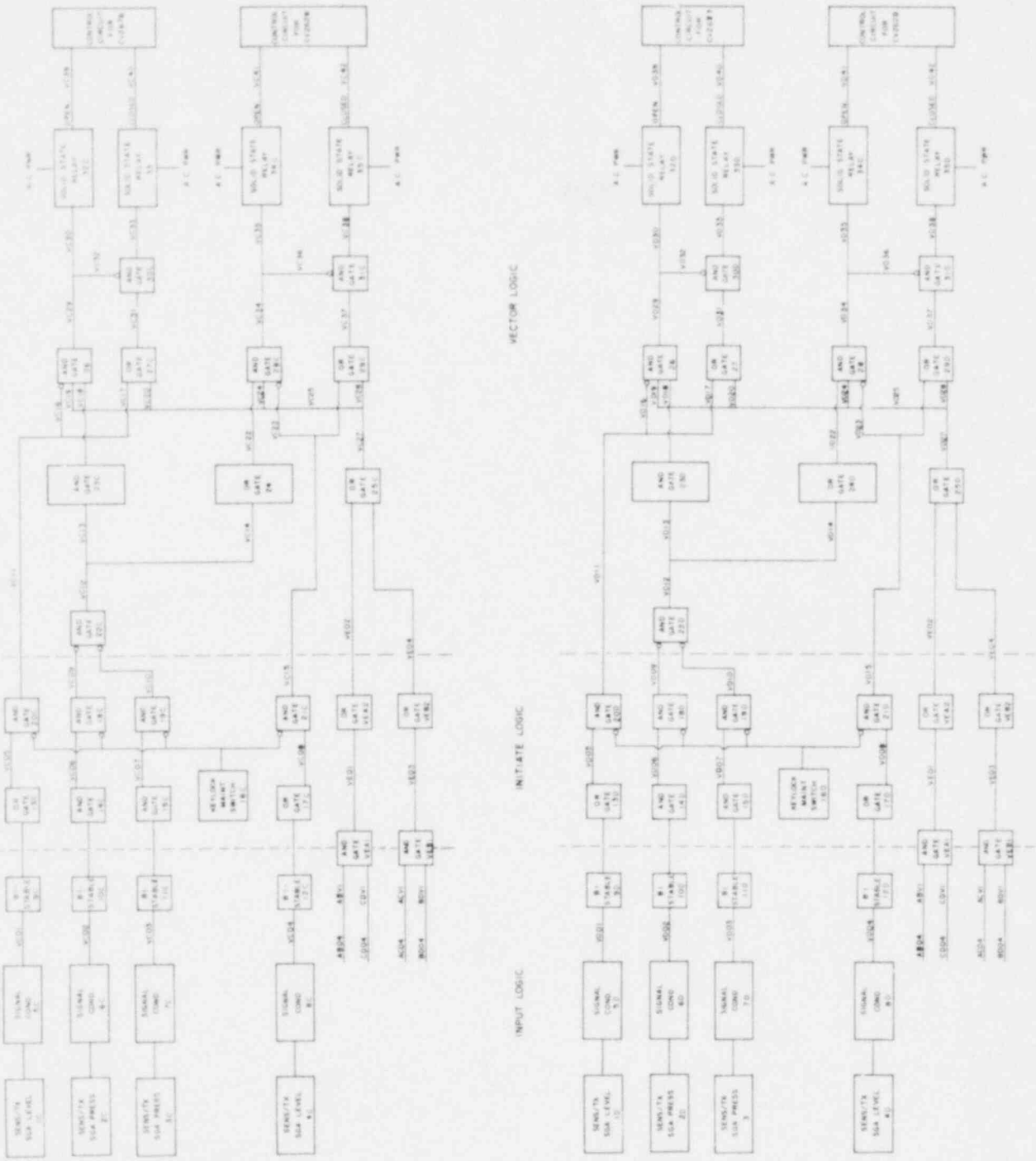


Figure 6-23: EFIC VECTOR SYSTEM

the analysis assumed that the presence of both "OPEN" and "CLOSE" signals from the vector system to a valve resulted in the valve opening from the design of the limit switches.

6.3.7 Human Interface System

Humans have an interface with all front-line and support systems discussed previously. The interface occurs during the operation, test, and maintenance of these systems. The humans involved are classified as operations personnel, maintenance technicians, or calibration technicians.

The operations personnel are responsible for operating the plant primarily from a specially designed control room to ensure maximum economic gain and minimum safety hazard or exposure to risk. This is accomplished by performing duties that include monitoring the status of the plant by observing or reading several of the plant status displays; keeping track of components involved in maintenance or test procedures; controlling the information collection, storage, and retrieval system; providing a primary source of system response following accidents or transients; and observing the general state of the plant by inspecting areas in and outside of the control room.

The maintenance technicians are responsible for performing the actual maintenance acts that are scheduled to prevent decreases in system or component reliability. The calibration technicians are charged with performing test or calibration operations on equipment to maintain their operating performances within prescribed tolerance limits.

The human reliability analysis, presented in Appendix B15, examined the various human interfaces in detail and assessed the probability of human errors during test and maintenance activities and accident situations. The following insights regarding the ANO human interface system were realized via this analysis:

1. Safety system/component unavailabilities caused by the failure of personnel to realign valves and circuit breakers to their safeguards positions after test and maintenance activities are generally small compared with other faults. There are several reasons for this including: (1) the component tagging procedure requires the operators to perform redundant checks of valve and circuit breaker alignment following test and maintenance, (2) most safety system valves and circuit breakers have alignment indication in the control room and are verified via a check list to be in the correct position every 8-hour shift, (3) required post-maintenance tests of components would, in general, inform the operator that valves and circuit breakers have not been aligned properly.

2. Operator errors committed during the course of an accident (i.e., LOCA or transient) are generally small contributors to accident sequence frequencies. One of the main reasons for the small contribution is due to the recent installation of the Safety Parameter Display System (SPDS) at ANO-1. The SPDS continuously plots the RCS temperature and pressure and compares them to operating envelopes and saturation

curves. We feel the SPDS is an excellent diagnostic tool and thus affords increased recovery potential from many types of operator errors. The SPDS also provides the type of information necessary to determine that a core damage accident is likely.

CHAPTER 7

ACCIDENT SEQUENCE ANALYSIS

The accident sequences discussed in Chapter 5 were analyzed to determine those core melt sequences with the highest frequency. The systems identified as failing or succeeding in the sequences were those which were discussed and modeled in Chapter 6. This chapter describes the methodology used in analyzing these accident sequences and presents an example calculation. More detailed information supplementing this chapter is given in Appendix C.

7.1 Methodology

The method used in analyzing the accident sequences was to first reduce the size of the fault tree models of the systems of Chapter 6 to a more computationally efficient size. Wherever possible, independent fault subtrees were formed, grouping those individual local faults associated with a given pipe or wire segment into single events. These reduced models were then combined appropriately for each accident sequence. This combination involved assembling the specific system models required in the sequence, as identified in Chapter 5 (e.g., the HPI system has several fault tree representations, and the one used depended on the specific sequence requirements). For each applicable system, the failure or success state of the system was chosen, as defined in the given sequence.

After combining the appropriate system models, a Boolean reduction was conducted via computer to produce sequence cut sets (i.e., the minimum combination of

component failures which produce an accident sequence), and the cut sets were quantified using the data base. A recovery model was applied to the cut sets of the sequences with the highest frequencies. Those sequences which still remained important after application of the recovery model comprised the dominant accident sequences.

Not all of the approximately 2000 possible sequences in the event trees were analyzed in the same manner. Several of the failure probabilities of systems were independent of all the failure probabilities of the other systems so that the independent ones could be removed from this part of the analysis, and their failure or success could be later manually multiplied into the final sequence frequency. The removal, from the computer part of the process, of systems whose failure probabilities were independent of failures of other systems geometrically reduced the number of computer runs necessary. Other sequences were not computer analyzed because examination of them showed the frequency of them to be very small in comparison to others.

The rest of this chapter will discuss the independent subtree creation, the candidate sequence selection, the data base, the computer analysis, and the recovery model.

7.1.1 Independent Subtrees

As described in Chapter 6, the front-line and support systems at ANO-1 were analyzed using Reference 13, "Fault Tree Analysis Procedures for the Interim Reliability Evaluation Program". These developed fault trees were extremely detailed. To achieve greater computational efficiency, the detailed trees were reduced in size, while retaining their information, by creating independent

subtrees. The independent events were those which were independent of all other systems.

The independent subtrees were formed by coalescing several faults which were local in the specific subsystems studied into a single local fault. The unavailability of the single local fault was simply the logical combination of the individual unavailabilities of the local faults comprising it. For example, a pipe segment could have many different ways by which flow through it could be stopped. Valves could plug or fail to operate when required. Pumps could fail to start or fail to run given start, etc. All of these failures and others, which are unique to a particular pipe segment can be combined together as local faults of that pipe segment if each original local fault is necessary and sufficient in and of itself to cause flow stoppage in the pipe segment. System interfaces in general cannot be so combined. In some cases, however, they can be, if and only if, the support system or subsystem only affects one particular pipe (or wire) segment. That is, if a fault is unique to a particular pipe segment, it can be logically combined with others which are unique to it into a single local fault while those which are not unique must be developed separately.

As a simplified example, Figures 7-1 and 7-2 show the process of creating independent subtrees. The first figure presents the fault tree for a pipe segment, which contains a check valve, a motor-operated valve, and a motor-driven pump. The check valve fails if it plugs, a local fault to the check valve. The MOV fails

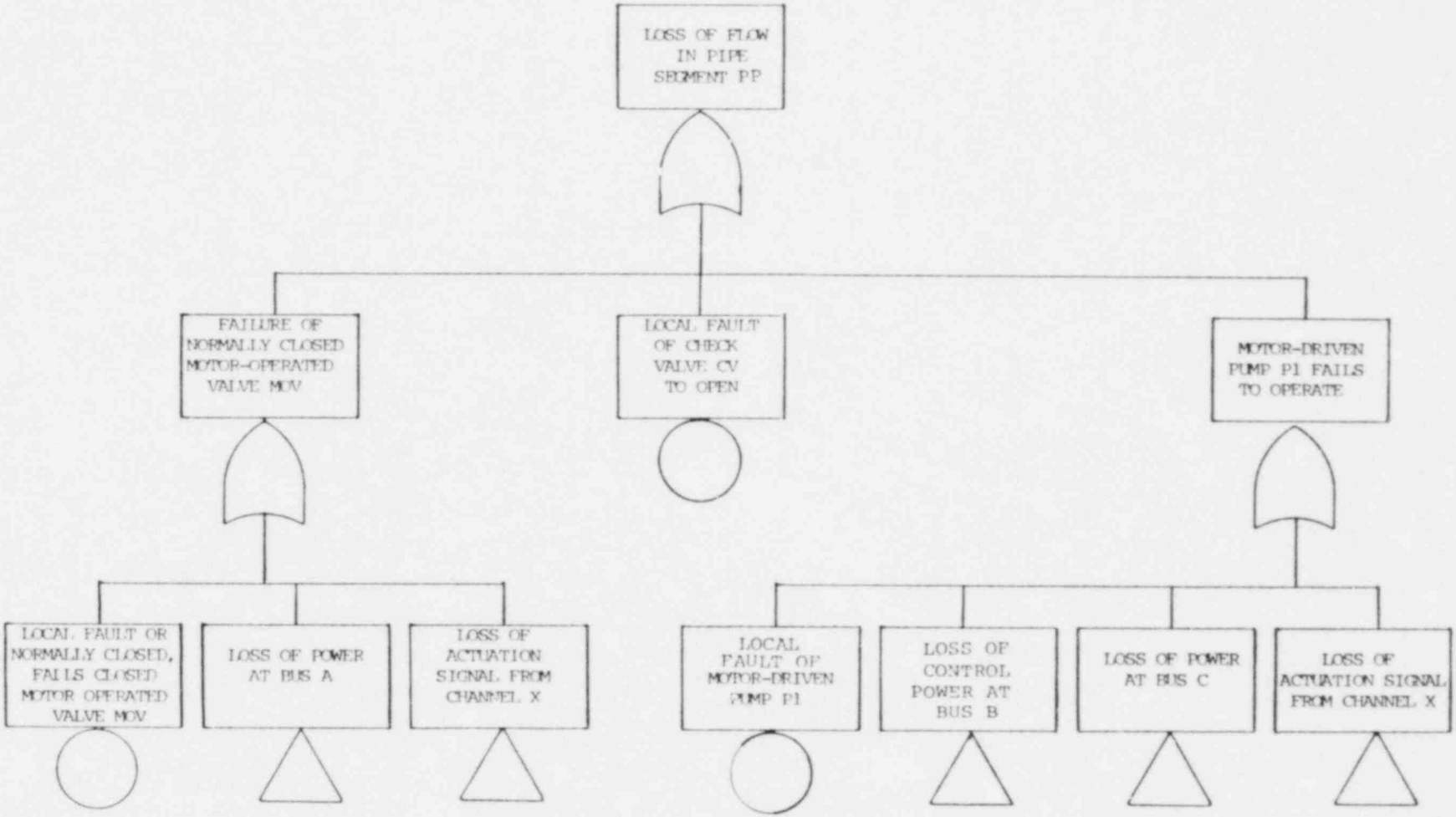


Figure 7-1. Example of Uncombined Fault Tree for Pipe Segment PP.

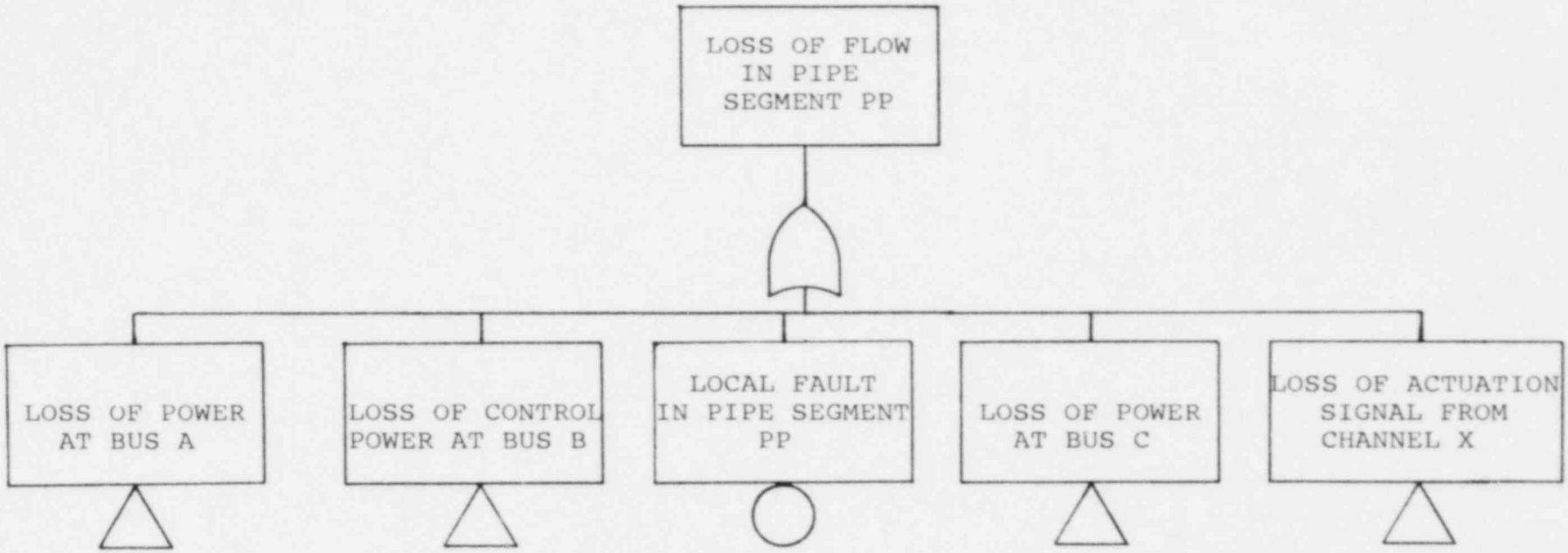


Figure 7-2. Example of Independent Subtree for Pipe Segment PP.

if it fails to operate or plugs (both local faults), if it has no power, or if it does not receive an actuation signal. (For simplicity, test, maintenance, circuit breakers, and cables are ignored in this example.) The motor-driven pump fails if it fails to start or to run, given start (both local faults), if it has neither motive nor control power, or if it does not receive an actuation signal (from the same channel as that of the MOV). Figure 7-2 presents this same fault tree combined into an independent subtree, with the single local fault of the pipe segment comprising all the faults which are unique to it.

By such coalescing of local faults into single events, the number of individual events was reduced, but the failure logic was maintained. In the sequence analysis, the number of events was further reduced by probability discrimination. Some events, or combinations of events, were very improbable in comparison to others within the same system and were assumed to be negligible. For example, the HPI system must inject water into two of four headers which are cross-tied. The sum of the probabilities of the various valve failure combinations within the headers was several orders of magnitude lower than other system failure mechanisms, and hence, the analysis did not consider these failures further.

7.1.2 Sequence Selection

As mentioned, not all of the possible sequences identified in the event trees of Chapter 5 were analyzed via computer. Three systems were found to have failure probabilities independent of each other and all other

systems. They were the failure of the reactor protection system (K), the failure of the safety relief valves to open (P), and the failure of the safety relief valve to reclose (Q). Thus, the probability of failure of these systems was solved independently. They were also removed from the computerized analysis because, e.g., the frequency of sequence $TKMD_1C$ could be calculated from the frequency of sequence TMD_1C by simply multiplying by the probability of event K. This considerably reduced the number of sequences requiring computer evaluation. Sequence selection is discussed in greater detail in Appendix C.

7.1.3 Data Base

The probabilities used for the basic events which appear in the fault trees were generally those generic probabilities provided by the NRC in Reference 14. This data base consisted of WASH-1400 data supplemented by data from licensee event reports. Other information was used, however. For many electrical components, the failure data came from NUREG-0666,[5] which has more recent data than WASH-1400.

Plant specific data were obtained by reviewing the ANO-1 maintenance reports and copies of information ANO-1 personnel have supplied to the Nuclear Plant Reliability Data System. These two sources were closely correlated since most maintenance reported was corrective rather than routine. The data review covered components of the front-line and support systems addressed in the IREP analysis. The plant specific data were used, rather than the generic, in those cases where they differed significantly.

In each case, plant specific and generic failure rates were compared using a statistical significance test based on the binomial distribution. In most cases the results of this test indicated that the two rates were consistent and the generic probability was, therefore, used in the analyses. There were, however, a few instances in which the plant specific data differed significantly and were therefore used in the analysis. These are presented in Appendix C.

Whether the data were generic or plant specific, the fault duration times were determined by the examination of ANO-1 test and operating procedures. Because the hourly failure rates were small, the duration time for a component was approximately one-half of its test or operating check interval, whichever was less provided that the check was sufficient to determine component availability.

In addition to the above, plant specific data were also used in determining the average frequency and duration of maintenance on system components. As a matter of policy, periodic preventive maintenance is not done on most safety components at ANO-1. The average maintenance frequency (in hours) was calculated by counting the number of maintenance actions recorded for each tvpe of component and dividing by the operating hours of the plant. The average duration of maintenance acts was also estimated based on plant experience. The product of these two figures (average maintenance frequency and average maintenance duration) was used to calculate the probability of unavailability due to maintenance.

Lastly, human errors, of both commission and omission, were determined from discussions with plant personnel and

from the information supplied in the "Handbook of Human Reliability Analysis," NUREG/CR-1278.[15] (The human factors portion of the analysis is discussed in detail in Appendix B15.)

7.1.4 Initial Sequence Analysis

The accident sequence Boolean reduction and cut set quantification was done using the SETS computer code.[16] All of the system fault trees were entered into the computer and reduced to minimal cut sets with the unavailabilities applied during each stage of the reduction. This was done for computational efficiency as the cuts sets were truncated at an unavailability product of 10^{-7} to 10^{-9}, depending on the specific sequences. Also, for a specific initiator, certain basic events in the fault tree were set to one or zero. (For example, for a loss-of-offsite power initiating event, the event of loss-of-offsite power in the fault trees was set to unity.) The complete system fault tree complements (successes) were formed from the original fault trees and reduced to minimal path sets with a corresponding list of events, for a given initiator, which were set to zero or one.

For each specific accident sequence, the appropriate failure models were "ANDed" together and Boolean reduced. The reduction involved application of several Boolean identities: $P + (P \cdot Q) = P$, $P \cdot P = P$, and $P + P = P$. Sequentially, the appropriate complement models were "ANDed" with the reduced failure cut sets. Contradictory terms, such as a given pump both failing and succeeding in the same term, were eliminated by the use of the

identity $P \cdot \overline{P} = \emptyset$, the null set. Using the systems successes in a given sequence is important because higher frequency results may ensue without it. If a system must succeed in a sequence, it may negate failure modes of systems which fail in that sequence. This is particularly true in the case of support system faults. It is not unusual to have a sequence frequency drop an order of magnitude or more when the sequence successes are considered.

The application of the $P \cdot \overline{P} = \emptyset$ identity eliminated the contradictory terms, but because of the addition of the complements, redundant terms remained. These redundant terms were eliminated by removing all complemented events from the remaining terms and reapplying the $P + (P \cdot Q) = P$ identity. For example, before eliminating the complemented terms, two terms in the reduced equation could be of the form $(A \cdot \overline{B}) + (A \cdot \overline{C})$, where $\overline{B}$ and $\overline{C}$ are the successes of events B and C, respectively. Since the minimum number of component failures, or minimal cut sets, which cause an accident sequences to occur is desired, the events $\overline{B}$ and $\overline{C}$, which are component successes, are irrelevant to the final accident sequence frequency. Thus, the two terms can be replaced by the single term A, which in this example, is the minimal cut set.

7.1.5 Recovery

Operator recovery of system failures was considered in the accident sequence analysis subsequent to the cut set determination. Recovery was only considered for those sequences with an initial frequency of 10^{-6}/yr or more. Heroic recovery actions were not considered, but routine recovery responses were. That is, for example, the overhaul of a pump or diesel generator was not considered,

but the manual realignment of a valve, whether by hand-switch or turning, was.

The first step in the recovery analysis was to consider whether or not a fault in a cut set was recoverable. As stated, heroic actions were not considered, and failures can occur that are non-recoverable. An example of this is the plugging of a check valve.

The second recovery consideration was that of the location of the recovery action, given that the fault was recoverable. The actions were separated into those which could be accomplished from the control room and those which could only be performed locally. If recovery could only be attempted locally and the local site was inaccessible (e.g., inside containment), the fault was considered to be non-recoverable.

A critical time for the action was established as the third step in the recovery analysis. The critical time was defined as the duration from the time of component failure, during which the restoration of the component would restore the system mitigative function. After the critical time, the system mitigative function was assumed to be lost, regardless of component recovery. For example, in a small LOCA sequence, it has been found[2] that onset of core melt occurs between 40 and 60 minutes if no water is injected by the HP system. Thus, in this case, the critical time for recovery of HP system faults was chosen as 40 minutes.

After the critical time and the locations of the recovery actions were determined for each recoverable unavailability of the fault was multiplied by a probability of non-recovery.

The analysis team constructed a histogram model of probabilities of non-recovery as a function of time for recovery actions which could be effected from the control room. The model assumed no recovery potential for the first five minutes, and all faults with critical times in excess of one hour were assumed to have a probability of non-recovery of 0.01. The histogram values are shown in Table 7-1, and this recovery model is an integral part of the sensitivity analysis discussed in Chapter 8.

Also presented in Table 7-1 are the histogram values for probabilities of non-recovery as a function of time for potential recovery action outside the control room and, hence, local at the fault. (This portion of the model is also a part of the sensitivity analysis of Chapter 8.) To consider local action, the total operator staffing per shift at ANO-1, and their interaction, were examined. At ANO-1, a minimum of five operators are available per shift: shift supervisor, senior operator, operator, auxiliary operator, and waste control operator. The latter two are located out in the plant, not the control room, but are in communication with the control room staff. After discussion with ANO-1 personnel, the analysis team determined that an additional ten minutes should be added to the control room critical times for recovery actions to yield the equipment local site information.

Table 7-1

Probability of Non-Recovery

P(NR)	Critical Time for Recovery Action in Control Room	Locally
1.00*	< 5 min	< 15 min
.25	5 - 10	15 - 20
.10	10 - 20	20 - 30
.05	20 - 30	30 - 40
.03	30 - 60	40 - 70
.01	> 60	> 70

*P(NR) = 1.00 if fault is also non-recoverable or if recovery location is inaccessible.

Thus, for example, if a discharge valve for a high pressure pump, which does not affect pump performance, did not open during a small LOCA because ESAS failed to provide a signal, recovery from the control room is possible within a critical time of ~40 minutes as discussed above. The probability of non-recovery, of the operator failing to actuate by the hand-switch, is 0.03 (see Table 7-1). If the valve, however, failed to open because the control circuit within its circuit breaker failed, local operation of the valve is required. The critical time is still ~40 minutes, but the probability of not recovering this fault locally is 0.05.

Although the critical times presented in Table 7-1 do not differentiate any time greater than seventy minutes, two additional critical times were used in the analysis. Both involved sequences that had high pressure injection failure and emergency feedwater success. In the first

case, cooling to the reactor coolant pump seals was provided, and the critical time was at least 60 hours, as explained in Section 3.2.1. For this time, the probability of non-recovery was assumed to be negligible, or conversely, that recovery was assumed to occur. In the second case, seal-cooling was not provided, and the critical time was at least five hours. (The second case is treated as a sensitivity issue. See Section 8.4 and Appendix D.) The failure which differentiated the two cases was loss of offsite power, and this event was the only failure considered for a recovery time of five hours. (In other sequences as appropriate, critical times for restoration of offsite power were thirty or sixty minutes, and the probability of non-recovery was taken from WASH-1400.[18] See Appendix C.)

The probabilities of non-recovery were determined for the individual failures in the fault trees, and the unavailabilities with recovery were calculated for these failures. The unavailabilities with recovery of the single local faults in the independent subtrees were the sums of the unavailabilities with recovery of the individual local faults comprising them, and the probability of non-recovery for a given independent subtree was the ratio of recovered unavailability to the unrecovered value.

As stated earlier, the recovery model was applied to only those sequences with frequencies greater than 10^{-6}/yr. after the initial analysis. In addition, within the cut sets of a dominant sequence, recovery was considered for only those failures needed to be restored so that the particular sequence could become a success sequence (i.e., non core melt). For example, if two

faults in a cut set were recoverable and the recovery of either would negate the core melt result, recovery actions were only considered for one of the faults and not both.

This same procedure was used for all of the examined sequences. If no fault in a specific cut set of the sequence was recoverable, the probability of non-recovery was 1. If only one cut set fault needed recovery, and could be recovered, to change the sequence from one of core melt to one of success, the cut set unavailability was multiplied by the appropriate P(NR) found in Table 7-1. If more than one fault required recovery to restore the sequence to a success state, then the cut set $P(NR)_{cs}$ was determined by

$$P(NR)_{cs} = 1 - \prod_{i=1}^{n} (1 - P(NR)_i)$$

where n is the number of faults in the cut set requiring recovery and $P(NR)_i$ are the individual P(NR) for these faults. This equation assumes parallel recovery actions, and when it was used (the cases were few), this assumption was examined as to its applicability to the specific cut set.

7.2 Example Calculation

The sequence chosen to illustrate the accident sequence methodology is the transient induced LOCA with the identifier T(LOP)LQ - D_3. It is a transient initiated by a loss of offsite power with concomitant failure of the power conversion system (T(LOP)). Additional system faults cause failure of the emergency feedwater system (L) and failure of one of the pressurizer safety/relief valves to reclose after opening (Q) resulting in a small LOCA. Also failing in this sequence is the high pressure

injection system when requiring both injection trains. This sequence is number 16 on the transient event tree in Fig. 5-10, which, with the induced LOCA, becomes sequence 31 on the B(1.66) LOCA event tree (Fig. 5-4). The dash in the sequence identifier represents a transfer from the transient to the LOCA event tree.

These system failures do not denote, however, the entire accident sequence because several system succeed as the accident progresses. These are the reactor protection system (K), the opening of the RCS relief valves (P), the reactor building cooling and spray systems (Y and C, respectively), and the containment spray recirculation system (F). Thus, although $T(LOP)LQ - D_3$ is a convenient shorthand identifier for the sequence, the actual Boolean representation of this sequence is $T(LOP)\bar{K}L\bar{P}Q\text{-}D_3\bar{Y}\bar{C}\bar{F}$. It was this Boolean representation which was analyzed to quantify this accident sequence. (Refer to Appendix A for the event tree description of this sequence.)

A number of the systems in the sequence have failure/success probabilities which are independent from all other system. These are K, P, and Q. Because their probabilities are independent, their individual unavailabilities/availabilities were determined separately and then all were multiplied together with the initiating event frequency. The unavailabilities/availabilities and initiating event frequency are

$$F(T(LOP)) = 0.32/yr$$

$$P(\bar{K}) = 1 - (4.2\times10^{-6}) \approx 1$$

$$P(P) = 1 - (9\times10^{-6}) \approx 1$$

$$P(Q) = 2\times10^{-2}$$

Multiplying these together yields 6.4×10^{-3}/yr.

The five remaining systems in the sequence ($LD_3\bar{Y}\bar{C}\bar{F}$) are dependent because of shared components, subsystems, or support systems, and hence, they must be solved together. The event tree discussion in Appendix A explains which system models in Appendix B are relevant for this loss-of-offsite power initiator. To solve this sequence, those appropriate models were used. The L and D_3 models were used as developed, because they already described the failure possibilities. The other models, for $\bar{Y}$, $\bar{C}$, and $\bar{F}$, were developed by computationally solving for the complement, i.e., the success, of the appropriate fault trees for Y, C, and F, respectively. The L and D_3 models were first "ANDed" together with the minimum cut set generation being truncated at 10^{-8}. Subsequently, the system success trees were consecutively "ANDed" with the LD_3 cut sets to eliminate failure/success contradictions. For example, a failure possibility for D_3 is the blockage of the BWST discharge pipe. This failure is contradictory to the total sequence, however, because the building spray system requires that the line permit flow, and this system, by the definition of the total accident sequence, succeeds (C). This process eliminates cut sets such as those involving blockage of the BWST discharge pipe.

Prior to the consideration of the sequence successes, the LD_3 unavailability was 1.2×10^{-3}. When the successes were considered, the $LD_3\bar{Y}\bar{C}\bar{F}$ unavailability became 8.3×10^{-4}. (In other sequences, accounting for successes reduced the unavailability by several orders of magnitude.)

The dominant cut sets of the sequence were examined individually to ascertain the recovery potential of the

safety function. That is, in this example, the accident propagation can be avoided if either the emergency feedwater function can be restored or if both high pressure pump trains are available (see Chapter 4 for functional success definitions). On the B(1.66) event tree, these success sequences are, respectively, sequence 1 and sequence 16. In addition, restoration of offsite power was considered for cut sets where it was appropriate. For example, a cut set for this sequence was local failure of diesel generator 1 and failure within the vector portion of the emergency feedwater initiation and control system to actuate the opening of the turbine driven pump discharge valves to the steam generators. The failure of diesel generator 1 fails one high pressure pump (the other is powered from diesel generator 2) and the motor-driven emergency feedwater pump. The recovery action considered for this cut set is for the operator to manually actuate the emergency feedwater valves from the control room, thus ensuring operation of one HP pump (powered by diesel generator 2) and one EFW pump (the turbine-driven). The action must be performed within twenty minutes. Another cut set was local failure of diesel generator 1 and local failure of the steam driven EFW pump. The only recovery considered possible for this is the restoration of offsite power, which must be done within one-half hour (twenty minutes for the EFW pump but forty for both HP pumps).

With each cut set examined for recovery possibilities, the unavailability of $LD_3\bar{Y}\bar{C}\bar{F}$ became 1.4×10^{-4}. Thus, the frequency of the entire sequence, $T(LOP)\bar{K}L\bar{P}Q\text{-}D_3\bar{Y}\bar{C}\bar{F}$, was determined to be 9×10^{-7} per reactor year. More detailed descriptions of this example and all candidate dominant accident sequences are given in Appendix C.

CHAPTER 8

RESULTS

One of the principal objectives of this study was to determine which accident sequences are most significant contributors to the risk associated with the operation of the ANO-1 plant. The most significant ANO-1 accident sequences, or "dominant accident sequences," are discussed in detail in Section 8.1. These sequences were derived by considering both the results of the system accident sequence quantification task described in Chapter 7 and Appendix C, and the core meltdown accident process analysis task described in Section 8.1.2.

Engineering insights gained via the analysis as a whole are presented in Section 8.2. Changes that have been made to the design and operation of ANO-1 as the result of this study are presented in Section 8.3. Analysis uncertainties which could significantly impact the results of this study are discussed in Section 8.4. The appropriate use of these results and the study limitations are discussed in Section 8.5.

8.1 ANO-1 Dominant Accident Sequences

Discussion of the ANO dominant accident sequences is split in two parts. Section 8.1.1 describes the most probable system and component failures for each dominant accident sequence. Section 8.1.2 summarizes the expected core meltdown phenomenology associated with these sequences.

8.1.1 System Accident Sequence Descriptions

The core meltdown accident sequences identified in Appendix C as having a frequency estimate $\geq 1 \times 10^{-6}$/Ryr, along with their appropriate containment failure mode/probability and release category (via Section 8.1.2),

are presented in Figure 8-1. These sequences are defined as the dominant accident sequences. A key to the figure nomenclature is given Table 8-1.

The histogram represents the release category frequencies. These were found by summing, for each release category, the point estimate frequencies of the 13 dominant accident sequences shown and less important sequences not shown (see Appendix C). These 13 sequences represent approximately 90 percent of the total release category frequencies.

The dominant accident sequences will now be discussed in the order they are displayed in Figure 8-1. Only the dominant cut sets for each accident sequence are listed and discussed. The probabilities of nonrecovery of these cut sets by the plant operators are discussed in general when recovery actions are possible. A detailed discussion of the nonrecovery probabilities utilized is given in Appendix C. The systems and cut set terms used to describe the accident sequences are depicted in the fault trees presented in Appendix B.

Sequence $B(1.2)D_1\ \alpha, \gamma, \beta, \epsilon$:

This sequence is initiated by a reactor coolant pump seal rupture or a rupture in the RCS piping in the range $.38" < D \leq 1.2"$ (B(1.2)), followed by failure of the high pressure injection system (D_1). 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 a small LOCA occurs followed by failure of the high pressure injection system.

Dominant Accident Sequences	Release Category						
	1	2	3	4	5	6	7
$B(1.2)D_1$	α 3×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ϵ 1×10^{-6}
$B(1.2)D_1C$	α 4×10^{-10}	γ 2×10^{-6}		β 3×10^{-8}		ϵ 2×10^{-6}	
$T(LOP)LD_1YC$	α 1×10^{-9}	δ 2×10^{-6}		β 7×10^{-8}		ϵ 8×10^{-6}	
$B(4)H_1$	α 1×10^{-8}	γ 7×10^{-7}			β 1×10^{-8}		ϵ 7×10^{-7}
$T(D01)LD_1YC$	α 3×10^{-10}	δ 6×10^{-7}		β 2×10^{-8}		ϵ 2×10^{-6}	
$T(D02)LD_1YC$	α 2×10^{-10}	δ 5×10^{-7}		β 2×10^{-8}		ϵ 2×10^{-6}	
$B(1.66)H_1$	α 1×10^{-10}	γ 6×10^{-7}			β 8×10^{-9}		ϵ 6×10^{-7}
$T(D01)LQ\text{-}D_3$	α 4×10^{-10}	γ 2×10^{-6}			β 3×10^{-8}		ϵ 2×10^{-6}
$T(A3)LQ\text{-}D_3$	α 3×10^{-10}	γ 2×10^{-6}			β 2×10^{-8}		ϵ 2×10^{-6}
$T(FIA)KD_1$	α 3×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ϵ 1×10^{-6}
$T(D01)LD_1$	α 2×10^{-10}	γ 1×10^{-6}			β 2×10^{-8}		ϵ 1×10^{-6}
$T(A3)LD_1$	α 1×10^{-10}	γ 5×10^{-7}			β 7×10^{-9}		ϵ 5×10^{-7}
$T(D01)LD_1C$	α 2×10^{-10}	γ 9×10^{-7}		β 1×10^{-8}		ϵ 9×10^{-7}	
$T(A3)LD_1C$	α 1×10^{-10}	γ 7×10^{-7}		β 1×10^{-8}		ϵ 7×10^{-7}	
Category Total	2×10^{-8}	2×10^{-5}	$<10^{-7}$	2×10^{-7}	2×10^{-7}	2×10^{-5}	1×10^{-5}

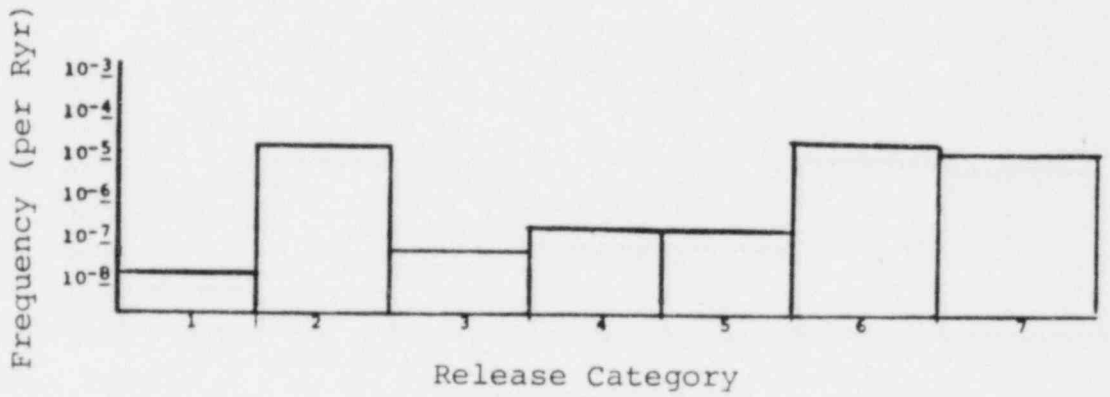


Figure 8-1. ANO-1 Dominant Accident Sequences

Table 8-1

Symbols Used in Figure 8-1

Initiating Events

B(1.2) - Reactor Coolant Pump Seal Rupture or Small-Small LOCA (.38" < D ≤ 1.2")

B(1.66) - Small LOCA (1.2" < D ≤ 1.66")

B(4) - Small LOCA (1.66" < D ≤ 4")

T(LOP) - Loss of Offsite Power Transient

T(PCS) - Loss of Power Conversion System Transient Caused by Other Than a Loss of Offsite Power

T(FIA) - Transients With All Front Line Systems Initially Available

T(A3) - Transient Initiated by Failure of the ES Bus A3 (4160VAC)

T(D01) - Transient Initiated by Failure of the ES Bus D01 (125VDC)

T(D02) - Transient Initiated by Failure of the ES Bus D02 (125VDC)

System Failures

C - Reactor Building Spray Injection System

D_1 - High Pressure Injection System (1 of 3 pumps)

D_3 - High Pressure Injection System (2 of 3 pumps)

H_1 - High Pressure Recirculation System

K - Reactor Protection System

L - Emergency Feedwater System

Q - Reclosure of Pressurizer Safety/Relief Valves

Y - Reactor Building Cooling System

Table 8-1 (Continued)

Containment Failure Modes

α - Vessel Steam Explosion

β - Penetration Leakage

γ - Overpressure Due to Hydrogen Burning

ϵ - Base Mat Melt-through

δ - Overpressure Due to Gas Generation

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 dominant failure mode of the HPIS is predicted to be failure of the operator to initiate the system. Information received from Babcock and Wilcox[3] indicates an engineered safeguards (ES) HPIS actuation signal due to low RCS pressure may not be generated following some LOCAs < 1.2" D. This sequence assumes an ES signal will not be generated prior to core uncovery and that the operator must initiate the system.

The frequency of this sequence is estimated as:

$$B(1.2)D_1 = 2.8\times10^{-6} \quad .$$

The dominant contributors, or cut sets, to this frequency are listed and discussed below.

Cut Set	Cut Set Frequency[1]
B(1.2)*HPI-PUMP-CM	2×10^{-6} (1)[2]
B(1.2)*LF-HPI-H14*LPI1407A-VCC-LF	5.3×10^{-7} (.23)
B(1.2)*LF-HPI-H14*LF-SWS-S2	7×10^{-8} (.05)
B(1.2)*LF-HPI-H14*LF-SWS-VCH4B	6.4×10^{-8} (.01)
B(1.2)*LF-HPI-H14*LF-SWS-S5	2.8×10^{-8} (.01)
B(1.2)*LF-HPI-H14*LF-SWS-S14	2.8×10^{-8} (.01)

[1]The number in parentheses represents the probability of nonrecovery which was factored into the cut set frequency To obtain the cut set frequency without recovery, divide the frequency listed by the number in parentheses.

[2]In general, operator errors are given a nonrecovery factor of 1. This is because the human factors models of these faults have explicitly considered recovery. (See Appendix B15.)

Term Descriptions

B(1.2) - reactor coolant pump seal failure; F (B(1.2)) = 2×10^{-2}/Ryr.

HPI-PUMP-CM - failure of operator to initiate HPIS; p(HPI-PUMP-CM) = 1×10^{-4} (See Appendix B15.

LF-HPI-H14 - local faults in HPIS pipe segment H14 (fails C pump); p(LF-HPI-H14) = .014.

LPI1407A-VCC-LF - local faults of valve CV1407 (fails A and B pump suction); p(LPI1407A-VCC-LF) = 8.2×10^{-3}.

LF-SWS-S2 - local faults in SWS pipe segment S2 (fails A and B pump cooling); p(LF-SWS-S2) = 5×10^{-3}.

LF-SWS-VCH4B - local faults of AC and DC switchgear room cooler VCH4B (fails A and B pump AC/DC power cooling); p(LF-SWS-VCH4B) = .023.

LF-SWS-S5 - local faults in SWS pipe segment S5 (fails A and B pump cooling); p(LF-SWS-S5) = .01.

LF-SWS-S14 - local faults in SWS pipe segment S14 (fails A and B pump cooling); p(LF-SWS-S14) = .01.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

An important insight realized from the analysis of this sequence is that a possibility exists for failing one of the three HPIS pumps given a LOCA < 1.2" D prior to generation of an ES signal. During normal operation, one of the pumps is operating and takes suction from the

makeup tank to perform the function of makeup and purification of the RCS. (This same pump is realigned to take suction from the BWST upon an ES signal to perform the function of emergency core cooling.)

Upon a small LOCA the pressurizer level and pressure would begin to decrease and automatic control actions will cause the makeup flow control valve to go full open and the pressurizer heaters to turn on respectively. The calculation presented in Appendix D.1 indicates that the pressurizer heaters will remain covered for an extended period and thus maintain RCS pressure well above the ES actuation set point. The calculation also indicates that the MU tank would empty prior to uncovering the pressurizer heaters. The MU tank is estimated to empty within approximately 14 minutes after LOCA initiation or about 10 minutes after the low MU tank level alarm. Upon dryout of the MU tank it is assessed that the operating HPI pump will fail in a short time.

It should be noted that failure of the operator to initiate the HPIS prior to MU tank dryout is part of the analyzed failure of the operator to initiate the system prior to core uncovery. (See Appendix B15 for details.)

Sequence B(1.2) D_1C α, β, γ, ϵ:

This sequence is initiated by a reactor coolant pump seal rupture or a rupture in the RCS piping in the range .38" $<$ D $\leq$ 1.2" (B(1.2)), followed by failure of the high pressure injection system (D_1) and reactor building spray injection system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure due to hydrogen burning (β), penetration leakage (γ), or base mat melt-through (ϵ).

This sequence is similar to the B(1.2) D_1 sequence described previously except that the reactor building spray injection system is also unavailable. Failure of the spray system results in a more severe release of radioactive material from the containment because the sprays are not available to scrub the containment atmosphere. The primary contributors to the frequency of this sequence are due to failures which are common to the suction paths of all three HPI pumps and both spray pumps. All five pumps take suction from the borated water storage tank (BWST) via a single manual valve in series with two MOVs in parallel. If the single manual valve or both MOVs are failed closed, the HPI pumps would fail within a few minutes, followed by failure of the spray pumps within approximately 15 minutes. Very little time is available to recover these faults before HPI pump failure and thus no recovery credit is given.

The remaining cut sets are combinations of suction MOV faults in one train and failure of pump support systems in the other train.

The frequency of this sequence is estimated as

$$B(1.2)\ D_1C = 4.4\text{x}10^{-6}.$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency
B(1.2)*LF-LPI-L25	$2\text{x}10^{-6}$ (1)
B(1.2)*LPI1407A-VCC-LF*LPI1408B-VCC-LF	$1.4\text{x}10^{-6}$ (1)
B(1.2)*LPI1407A-VCC-LF*LF-SWS-S1	$3.2\text{x}10^{-7}$ (.4)
B(1.2)*LPI1408B-VCC-LF*LF-SWS-S2	$4.2\text{x}10^{-8}$ (.05)
B(1.2)*LPI1407A-VCC-LF*LF-SWS-VCH4A	$3.8\text{x}10^{-8}$ (.01)
B(1.2)*LPI1408B-VCC-LF*LF-SWS-VCH4B	$3.8\text{x}10^{-8}$ (.01)

Term Descriptions

B(1.2) - reactor coolant pump seal failure; F(B(1.2)) = 2×10^{-2}/R yr.

LF-LPI-L25 - local fault of LPIS segment L25 (fails pump suction to all HPIS and RBSI pumps); P(LF-LPI-L25) = 1×10^{-4}.

LPI1407A-VCC-LF - local fault of LPIS valve CV1407 (fails suction to HPIS A and B pumps and RBSI A pump); P(LPI1407A-VCC-LF) = .0082.

LPI1408B-VCC-LF - local fault of LPIS valve CV1408 (fails suction to HPIS C pump and RBSI B pump); P(LPI1408B-VCC-LF) = .0082.

LF-SWS-S1 - local fault in SWS pipe segment S1 (fails cooling to HPIS C pump and RBSI B pump); P(LF-SWS-S1) = .005.

LF-SWS-S2 - local fault in SWS pipe segment S2 (fails cooling to HPIS A and B pump and RBSI A pump); p(LF-SWS-S2) = .005

LF-SWS-VCH4A - local faults in AC and DC switchgear room cooler VCH4A (fails HPIS pump C and RBSI pump B AC/DC power cooling; P(LF-SWS-VCH4A) = .023.

LF-SWS-VCH4B - local faults in AC and DC switchgear room cooler VCH4B (fails HPIS pump A and B, and RBSI pump A AC/DC power cooling); P(LF-SWS-VCH4B) = .023.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; category 4
$P(\epsilon) = 0.5$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 8-1.

Sequence T(LOP)LD$_1$YC α, β, δ, ε:

This sequence is initiated by a loss of offsite power with concomitant failure of the power conversion system (T(LOP)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D_1), the reactor building cooling system (Y), and the reactor building spray system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure (δ), penetration leakage (β), or base mat melt-through (ε).

This sequence is equivalent to the well known TMLB' sequence which was one of the dominant risk contributors for the Surry PWR reported in WASH-1400.

This sequence is initiated by a loss of offsite power transient followed by failure of all core cooling and containment systems capable of mitigating the accident. It is estimated that core melting will begin at approximately 1 hour.[1]

The frequency of this sequence is estimated as:

$$T(LOP)LD_1YC = 9.9 \times 10^{-6} \quad .$$

Approximately 80 percent of this frequency is due to common mode failure of both station batteries on demand following the loss of offsite power. (The probability of this common mode is calculated in Appendix D.3.) Since all mitigating systems require DC power for

[1]The one hour figure was estimated in the following manner: Reference 21 indicates that 37 minutes elapse between reactor trip to core uncovery. Reference 2 indicates that ~20 minutes elapse between core uncovery and the onset of core melt. Adding these two estimates yields ~1 hour.

successful operation, all mitigating systems will fail following failure of both batteries. This cut set, along with other important contributors are listed and described below.

It is estimated that the operator can restore approximately 75 percent of these faults prior to core uncovery. Most recovery actions involve recovery of offsite power.

Cut Set	Cut Set Frequency
T(LOP)*BATCM	8.3×10^{-6} (.36)
T(LOP)*LF-AC-DG1*LF-AC-DG2*LF-EFS-E11	5.1×10^{-7} (.36)
T(LOP)*LF-DC-D07*LF-DC-D06	1.4×10^{-7} (.36)
T(LOP)*LF-AC-DG1*LF-AC-DG2*LF-EFC-D1D2CM	8×10^{-8} (.05)

Term Descriptions

T(LOP) - loss of offsite power; F(T(LOP)) = .32/Ryr.

BATCM - common mode failure of both station batteires (fails all mitigating systems); P(BATCM) = 2.6×10^{-5}.

LF-DC-DO7 - local fault of battery DO7 (fails HPIS A and B pump, EFS electric pump and 1/2 turbine pump flow control valves, RBCS A and B fan, RBSI A pump); P(LF-DC-DO7) = .0011.

LF-AC-DG1 - local fault of diesel generator 1 (fails HPIS A and B pump, RBCS A and B fan, RBSI A pump, EFS electric pump); P(LF-AC-DG1) = .033.

LF-AC-DG2 - local fault of diesel generator 2 (fails HPIS C pump, RBCS C and D fan, RBSI B pump); P(LF-AC-DG2) = .033.

LF-DC-D06 - local fault of battery D06 (fails HPIS C pump, 1/2 EFS turbine pump control valves, RBCS C and D fan); P(LF-DC-D06) = .0011.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine driven pump); P(LF-EFS-E11) = 4×10^{-3}.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; Category 1
$P(\delta) = 0.2$; Category 2
$P(\beta) = 0.007$; Category 4
$P(\epsilon) = 0.8$; Category 6

Multiplying the sequence frequency with the containment failure mode probabiilities results in the values presented in Figure 8-1.

Sequence B(4) H_1 α, γ, β, ϵ:

This sequence is initiated by a rupture in the RCS piping in the range 1.66" < D $\leq$ 4" (B(4)) followed by failure of the high pressure recirculation system (H_1). 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 that the LOCA systems perform successfully during the injection phase but that the high pressure recirculation system (HPRS) fails during the recirculation phase. Failure of the HPRS would lead to boil off of the water covering the core resulting in core melt.

The prime contributor to HPRS failure is due to failure of the operators to initiate, or correctly follow emergency procedures while initiating, the HPRS. The HPRS is initiated when the BWST is 84 percent empty and requires several operator actions, some of which are conducted away from the control room: manual valves

connecting the suction of the high pressure pumps to the discharge of the low pressure pumps are opened in the auxiliary building and motor operated valves, connecting the suction of the low pressure pumps to the containment sump, are opened from the control room.

Another potentially important contributor to HPRS failure is the failure of the pump room cooling system. The temperatures of the three pumps are kept below their design operating temperature by a single operating cooler which consists of a fan/service water heat exchanger. (Two other non-operating coolers could potentially be used, but they must be started by the operator.)

Many single failures of the operating room cooler were identified. These include failure of the room cooler itself, failures in the fan electric power subsystem and failures in the heat exchanger service water subsystem. The number of single failures was large partly due to the fact that the service water pump supplying the heat exchanger is powered by the "odd" electrical load division and the fan is powered by the "even" load division. (ANO-1 has two load divisions, commonly referred to as "even" and "odd".) Because of this the room cooler is dependent on both load divisions. This arrangement roughly doubles the number of single failures.

The frequency of this sequence is estimated as:

$$B(4)H_1 = 1.4 \times 10^{-6} \quad .$$

The dominant cut sets are:

Cut Set	Cut Set Frequency
B(4)*HPRS-CM	6.1×10^{-7} (1)
B(4)*LF-SWS-S82*LF-SWS-S83	8.7×10^{-8} (.43)
B(4)*LF-SWS-VCH4B	8.7×10^{-8} (.01)
B(4)*LF-SWS-VCH4A	8.7×10^{-8} (.01)
B(4)*LF-SWS-S5	3.8×10^{-8} (.01)
B(4)*LF-SWS-S14	3.8×10^{-8} (.01)
B(4)*LF-LPI-L19*LF-LPI-L20	3.8×10^{-8} (.15)
B(4)*LF-LPI-L20*LF-SWS-S82	3.4×10^{-8} (.15)
B(4)*LF-LPI-L19*LF-SWS-S83	3.4×10^{-8} (.15)
B(4)*LF-SWS-S1	1.9×10^{-8} (.01)
B(4)*LF-SWS-S2	1.9×10^{-8} (.01)
B(4)*LF-ECS-ROOM100	1.9×10^{-8} (.01)
B(4)*LF-ECS-ROOM99	1.9×10^{-8} (.01)
B(4)*LF-LPI-ROOM55	2.9×10^{-9} (.01)

Term Descriptions

B(4) - RCS pipe break $1.66" < D \leq 4"$; F(B(4)) = 3.8×10^{-4}/Ryr.

HPRS-CM - failure of operator to initiate the HPRS; P(HPRS-CM) = .0016 (See Appendix B15.)

LF-SWS-S2 - local faults in SWS pipe segment S2 (fails cooling to HPRS pump room heat exchanger); P(LF-SWS-S2) = .005.

LF-SWS-S82 - local faults in SWS pipe segment S82 (S82 and S83 fail suction cooling to all HPRS pumps); P(LF-SWS-S82) = .023.

LF-SWS-S83 - local faults in SWS pipe segment S83 (S83 and S82 fail suction cooling to all HPRS); P(LF-SWS-S83) = .023.

LF-SWS-VCH4B - local faults in AC and DC switchgear room cooler VCH4B ("odd" AC/DC power fails causing SWS pump which feeds the HPRS room heat exchanger to fail); P(LF-SWS-VCH4B) = .023.

LF-SWS-VCH4A - local faults in AC and DC switchgear room cooler VCH4A (fails HPRS pump room fan AC/DC power); P(LF-SWS-VCH4A) = .023.

LF-SWS-S5 - local faults in SWS pipe segment S5 (fails cooling to HPRS pump room heat exchanger); P(LF-SWS-S5) = .01.

LF-SWS-S14 - local faults in SWS pipe segment S14 (fails cooling to HPRS pump room heat exchanger); P(LF-SWS-S14) = .01.

LF-LPI-L19 - local faults in LP pipe segment L19 (L19 and L20 fail suction to all HPRS pumps); P(LF-LPI-L19) = .026.

LF-LPI-L20 - local faults in LP pipe segment L20 (L20 and L19 fail suction to all HPRS pumps); P(LF-LPI-L20) = .026.

LF-SWS-S1 - local faults in SWS pipe segment S1 (fails AC and DC room cooler which fails HPRS pump room fan AC/DC power); P(LF-SWS-S1) = .005.

LF-ECS-ROOM100 - local faults in AC room cooler 100 ("odd" AC power fails causing SWS pump which feeds the HPRS room heat exchanger to fail); P(LF-ECS-ROOM100) = .005

LF-ECS-ROOM99 - local faults in AC room cooler 99 ("even" AC power fails causing failure of HPRS room fan); P(LF-ECS-ROOM99) = .005.

LF-HPI-ROOM55 - local faults in HPRS room cooler; P(LF-HPI-ROOM55) = 7.5×10^{-4}.

As can be noted, the single HPRS room cooler cut sets all have a non-recovery probability of .01. The recovery action for these cut sets involve manual initiation of one of the two non-operating room coolers. Initiation of these coolers is performed outside the control room and would most likely be done following a high pump stator winding temperature alarm. Initiation of the alternate room coolers is not described in the LOCA procedures, but we feel that recovery following failure of HPRS room cooling is likely (i.e., non-

recovery probability of .01) because the room heat up would be slow since the water pumped by the HPRS is cooled by the low pressure heat exchangers.

It should be noted that failure of the HPRS via room cooling failure should be considered to be "potentially" important since no plant tests have been performed which absolutely establish the need for HPRS room cooling.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.01$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence T(DO1)LD$_1$YC α, β, δ, ϵ :

This sequence is initiated by a failure of the engineered safeguards power bus DO1 (125DVC) with concomitant failure of the power conversion system (T(DO1)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D_1), the reactor building cooling system (Y), and the reactor building spray system (C). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure (δ), penetration leakage (β), or base mat melt-through (ϵ).

This sequence assumes a transient induced by the failure of the "odd" DC bus followed by failure of all core cooling and containment systems capable of mitigating the accident.

Roughly 60 percent of the sequence frequency is due to failure of the "even" DC bus. Failure of this bus would render the plant totally without DC power. DC control power is required by all transient front line systems, and thus no mitigating systems would be available. Recovery from this event would depend upon the severity of the DC bus failure. We have assumed that the fault is non-recoverable since insufficient data was available to estimate recovery and the recovery actions must be performed within approximately 1 hour to prevent the onset of core melt.

The remaining 40 percent of the sequence frequency is comprised of several combinations of failures due to the initiating event, faults in the front-line systems, and support system faults.

The frequency of this sequence is estimated to be:

$$T(D01)LD_1YC = 3.1x10^{-6}.$$

The dominant cut sets are:

Cut Set	Cut Set Frequency
T(D01)*LF-DC-D02	$1.8x10^{-6}$ (1)
T(D01)*LF-SWS-S1*LF-EFS-E4	$5.4x10^{-8}$ (.05)
T(D01)*LF-SWS-S1*LF-EFC-ACBD4	$5x10^{-8}$ (.05)
T(D01)*LF-SWS-S1*LF-EFS-E29	$3.6x10^{-8}$ (.05)
T(D01)*LF-SWS-S1*-LF-EFC-BB7B1CM	$2.5x10^{-8}$ (.05)
T(D01)*LF-SWS-S1*-LF-EFC-D1D2CM	$2.2x10^{-8}$ (.05)
T(D01)*LF-SWS-S1*-LF-EFC-VCD2	$4.3x10^{-8}$ (.05)
T(D01)*LF-SWS-VCH4A*LF-EFS-E4	$5x10^{-8}$ (.01)
T(D01)*LF-SWS-VCH4A*LF-EFC-ACBD4	$4.5x10^{-8}$ (.01)
T(D01)*LF-SWS-VCH4A*LF-EFC-VCD2	$4x10^{-8}$ (.01)
T(D01)*LF-SWS-VCH4A*LF-EFS-E29	$3.4x10^{-8}$ (.01)
T(D01)*LF-SWS-VCH4A*LF-EFC-BB7B1CM	$2.2x10^{-8}$ (.01)
T(D01)*LF-SWS-VCH4A*LF-EFC-D1D2CM	$2.2x10^{-8}$ (.01)

Term Descriptions

T(DO1) - failure of ES bus DO1 (125VDC) (fails EFS electric pump and 1/2 turbine pump flow control valves and 1/2 turbine pump steam admission valves, HPIS A and B pump, RBCS fans A and B, RBSI pump A); F(T(DO1)) = 1.8×10^{-2}/Ryr.

LF-DC-DO2 - local fault of ES bus DO2 (125VDC) (fails 1/2 EFS turbine pump flow control valves, HPIS C pump, RBCS fans C and D, RBSI pump B); P(LF-DC-DO2) = 1×10^{-4}.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E4) = .012.

LF-EFC-ACBD4 - local fault in "EFIC Initiate signal" path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-ACBD4) = .011.

LF-EFC-VCD2 - local fault in "EFIC Vector" signal path (fails 1/2 EFS turbine pump flow control valves); P(LF-EFC-VCD2) = .0094.

LF-EFS-E29 - local fault in EFS pipe segment E29 (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFS-E29) = .0081.

LF-EFC-BB7B1CM - local fualt in "EFIC Initiate" signal path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-BB7B1CM) = .0054.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

LF-SWS-S1 - local fault in SWS pipe segment S1 (fails pump and heat exchanger cooling to HPIS C pump, RBCS C and D fan, RBSI pump B); P(LF-SWS-S1) = .005.

LF-SWS-VCH4A - local faults of AC and DC switchgear room cooler VCH4A (fails AC/DC power to HPIS C pump, RBCS C and D fan, RBSI pump B); P(LF-SWS-VCH4A) = .023.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.2$; category 2
$P(\beta) = 0.007$; category 4
$P(\epsilon) = 0.8$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 8-1.

Sequence T(D02)LD$_1$YC α, β, δ, ϵ:

This sequence is initiated by a failure of engineered safeguards bus D02 (125VDC) with concomitant failure of the power conversion system (T(D02)), followed by failure of the emergency feedwater system (L), the high pressure injection system (D$_1$), the reactor building cooling system (Y), and the reactor building spray system (C). Contaminent failure is predicted by one of the following: vessel steam explosion (α), contaminent overpressure (δ), penetration leakage (β), or base mat melt-through (ϵ).

This sequence is similar to the T(D01)LD$_1$YC sequence just described, except that in this case, failure of the "even" DC bus is the initiating event.

Roughly 70 percent of the sequence frequency is due to failure of the "odd" DC bus. Failure of this bus would render the plant totally without DC power. DC control power is required by all transient front line systems, and thus, no mitigating systems would be available. As was the case for the previous sequence, no recovery credit for this fault was given because of

the relatively short time to the onset of core melt (~1 hour) and since insufficient data was available to estimate recovery.

The frequency of this sequence is estimated as

$$T(D02)LD_1YC = 2.5x10^{-6}.$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency
T(D02)*LF-DC-D01	$1.8x10^{-6}$ (1)
T(D02)*LF-AC-B5*LF-EFW-E5	$2.3x10^{-8}$ (.25)
T(D02)*LF-AC-B5*LF-EFW-E28	$1.5x10^{-8}$ (.22)
T(D02)*LF-AC-A3*LF-EFW-E5	$1.3x10^{-8}$ (.25)

Term Descriptions

T(D02) - failure of ES bus D02 (125VDC) (fails HPIS pump C, RBCS fans C and D, RBSI pump B 1/2 EFS turbine pump flow control valves and 1/2 turbine steam admission valves, 1/2 EFS electric pump flow control valves); $F(T(D02)) = 1.8x10^{-2}/Ryr$.

LF-EFS-E5 - local fault in EFS pipe segment E5 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E5) = .012.

LF-AC-A3 - local fault of ES bus A3 (4160VAC) (fails HPIS pump A and B, RBCS fans A and B, RBSI pump A, EFS electric pump); $P(LF-AC-A3) = 2.4x10^{-4}$.

LF-DC-D01 - local fault of ES bus D01 (125VDC) (fails HPIS pump A and B, RBCS fans A and B, RBSI pump A, 1/2 EFS turbine pump flow control valves, and EFS electric pump); $P(LF-DC-D01) = 1x10^{-4}$.

LF-AC-B5 - local fault of ES bus B5 (480VAC) (fails HPIS pump A and B suction, RBCS fans A and B, RBSI pump A suction, 1/2 EFS electric pump flow control valves); $P(LF-AC-B5) = 4.4x10^{-4}$.

LF-EFW-E28 - local fault of EFS pipe segment E28 (fails 1/2 turbine pump steam admission valves); $P(\text{LF-EFW-E28}) = 8.1 \times 10^{-3}$.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\delta) = 0.2$; category 2
$P(\beta) = 0.007$; category 4
$P(\epsilon) = 0.8$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 8-1.

Sequence $B(1.66)H_1$, α, γ, β, ϵ:

This sequence is initiated by a rupture in the RCS piping in the range 1.2" < D $\leq$ 1.66" (B(1.66)) followed by failure of the high pressure recirculation system (H_1). 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 $B(4)H_1$ sequence discussed previously. The systems responding during both sequences are similar; the only difference is that for $B(1.66)H_1$, the emergency feedwater system is successful. However, this difference does not affect the dominant cut sets.

The frequency of this sequence is estimated as:

$$B(1.66)H_1 = 1.2 \times 10^{-6} \quad .$$

The dominant cut sets are the same as for $B(4)H_1$. The quantitative values of each cut set can be determined by substituting $F(B(1.66)) = 3.1 \times 10^{-4}$/Ryr.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence T(DO1)LQ - D_3 α, β, γ, ϵ:

This sequence is initiated by a failure of the engineered safeguards power bus DO1 (125 VDC) with concomitant failure of the power conversion system (T(DO1)), followed by failure of the emergency feedwater system (L), failure of one pressurizer safety/relief valve to reclose (Q), and failure to inject flow from two of three high pressure injection pumps (D_3). 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 a transient induced LOCA (TQ) in which core cooling fails during the injection phase (LD_3). TQ sequences require the same core cooling requirements during the injection phase (ECI) as B(1.66) LOCAs since a stuck open pressurizer safety valve falls in $1.2 < D \leq 1.66$ break size range. ECI success, as presented in Table 4-1, requires either two of three nigh pressure pumps OR one of three high pressure pumps and one of two emergency feedwater system (EFS) pumps. Failure of events L and D_3 precludes either ECI success mode.

Loss of DC power bus D01, the initiating event, precludes the success of two high pressure pumps and fails approximately one half of the EFS. The dominant cut sets therefore all involve single failures of the remaining half of the EFS.

The frequency of this sequence is estimated as:

$$T(D01)LQ - D_3 = 4x10^{-6} \quad .$$

The dominant cut sets are:

Cut Set	Cut Set Frequency
T(D01)*LF-EFS-E11*Q	$1.5x10^{-6}$ (1)
T(D01)*LF-EFS-E4*Q	$1.1x10^{-6}$ (.25)
T(D01)*LF-EFS-E29*Q	$6.4x10^{-7}$ (.22)
T(D01)*LF-EFC-ACBD4*Q	$2x10^{-7}$ (.05)
T(D01)*LF-EFC-VCD2*Q	$1.7x10^{-7}$ (.05)
T(D01)*LF-EFS-E22*Q	$1.1x10^{-7}$ (1)
T(D01)*LF-EFC-BB7B1*Q	$1x10^{-7}$ (.05)
T(D01)*LF-EFC-D1D2CM*Q	$8x10^{-8}$ (.05)
T(D01)*LF-EFC-CSY2*Q	$7.2x10^{-8}$ (.05)
T(D01)*LF-EFS-E2*Q	$3.6x10^{-8}$ (1)

Term Descriptions

T(D01) - failure of ES bus D01 (125VDC) (fails EFS electric pump and 1/2 turbine pump flow control valves and 1/2 turbine pump steam admission valves, HPIS A and B pump); F(T(D01)) = .018.

Q - failure of one of two pressurizer safety/relief valves to close after being demanded open; P(Q) = .02.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine pump); P(LF-EFS-E11) = .0041.

LF-EFS-E22 - local fault in EFS pipe segment E22 (fails suction path to both EFS pumps); P(LF-EFS-E22) = $3x10^{-4}$.

LF-EFC-CSY2 - local fault in "EFIC Initiate" signal path (fails 1/2 turbine pump steam admission values); P(LF-EFC-CSY2) = .0039.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control values); P(LF-EFS-E4) = .012.

LF-EFC-ACBD4 - local fault in "EFIC Initiate" signal path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-ACBD4) = .011.

LF-EFC-VCD2 - local fault in "EFIC Vector" signal path (fails 1/2 EFS turbine pump flow control valves); P(LF-EFC-VCD2) = .0094.

LF-EFS-E29 - local fault in EFS pipe segment E29 (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFS-E29) = .0081.

LF-EFC-BB7B1CM - local fault in "EFIC Initiate" signal path (fails 1/2 EFS turbine pump steam admission values); P(LF-EFC-BB7B1CM) = .0054.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control values); P(LF-EFC-D1D2CM) = .0046.

LF-EFS-E2 - local fault in EFS pipe segment E2 (fails 1/2 turbine pump flow path); P(LF-EFS-E2) = 1×10^{-4}.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence T(A3)LQ - D_3 α, β, γ, ϵ:

This sequence is initiated by a failure of the engineered safeguards power bus A3 (4160VAC) with concomitant failure of the power conversion system (T(A3)),

followed by failure of the emergency feedwater system (L), failure of one pressurizer safety/relief valve to reclose (Q), and failure to inject flow from two of three high pressure injection pumps (D_3). 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 one just discussed except it is initiated by an AC rather than DC bus failure. It is a transient induced LOCA (TQ) in which core cooling fails during the injection phase (LD_3). TQ sequences require the same core cooling requirements during the injection phase (ECI) as B(1.66) LOCAs since a stuck open pressurizer safety valve falls in $1.2 < D \leq 1.66$ break size range. ECI success, as presented in Table 4-1, requires either two of three high pressure pumps OR one of three high pressure pumps and one of two emergency feedwater system (EFS) pumps. Failure of events L and D_3 precludes either ECI success mode.

Loss of AC power bus A3, the initiating event, precludes the success of two high pressure pumps and fails approximately one half of the EFS. The dominant cut sets therefore all involve single failures of the remaining half of the EFS.

The frequency of this sequence is estimated as:

$$T(A3)LQ - D_3 = 3.3 \times 10^{-6}$$

The dominant cut sets are:

Cut Set	Cut Set Frequency
T(A3)*LF-EFS-E11*Q	2.9×10^{-6} (1)
T(A3)*LF-EFS-E22*Q	2.2×10^{-7} (1)
T(A3)*LF-EFC-D1D2CM*Q	1.6×10^{-7} (.05)
T(A3)*LF-EFW-E4*LF-EFW-E5*Q	2.5×10^{-8} (.25)

Term Descriptions

T(A3) - failure of ES bus A3 (4160VAC) (fails EFS electric pump, and HPIS A and B pump); F(T(A3)) = .035.

Q - failure of one of two pressurizer safety/relief valves to close after being demanded open; P(Q) = .02.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine pump); P(LF-EFS-E11) = .0041.

LF-EFS-E22 - local fault in EFS pipe segment E22 (fails suction path to both EFS pumps); P(LF-EFS-E22) = 3×10^{-4}.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E4) = .012.

LF-EFS-E5 - local fault in EFS pipe segment E5 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E5) = .012.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence $T(FIA)KD_1$ α, γ, β, ϵ :

This sequence is initiated by a requirement for a reactor trip with all front-line systems initially

available (T(FIA)) followed by failure of the reactor protection system (K), and failure of the high pressure injection system (D_1). Containment failure is predicted by one of the following: vessel steam exposion (α), 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.(1) The report states that if the reactor protection system fails to scram the reactor following a transient, an RCS peak pressure of 4,900 psi may result.[1] (4,900 is quoted for cases in which the pressurizer ERV fails to open. This applies to ANO-1 since the ERV has been effectively disabled due to closure of the block valve.) Analysis conducted by B&W indicates that RCS components should remain functional after this peak pressure.(12) The analysis of this sequence assumes that the RCS components would survive the peak pressure. (It should be noted that ATWS for B&W plants is currently an unresolved safety issue which, for PWRs rest primarily upon the peak pressure question.)

The 4900 psi pressure quoted in Reference 1 assumed an ATWS following a loss of main feedwater (LOMF). The LOMF ATWS is the worst case in terms of peak pressure because the only available RCS heat removal system capable of reducing the peak pressure is the emergency feedwater

---

[1] It should be noted that in order to attain a peak pressure of 4900 psi, Reference 1 assumed pessimistic values for certain parameters, e.g., moderator temperature coefficient.

system (EFS). Since the EFS has a heat removal capacity much smaller than the main feedwater system, it is relatively ineffective (in comparison with the main feedwater) in reducing the peak pressure. It should be noted, however, that in the sequence analyzed here, the main feedwater is initially available. Whether or not main feedwater is initially available at ANO-1 is not expected to significantly affect the peak pressure. The reason for this is that many requirements for a reactor trip also automatically cause the main feedwater system to trip off one main feed pump and runback the remaining feed pump to a level approximately that of the EFS (e.g., these actions would be taken following a turbine trip).

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 these situations, the high pressure injection system must be actuated by the operator to inject borated (i.e., negative reactivity) water to successfully shut down the reactor and to replace RCS inventory lost via the pressurizer valves during the pressure transient. This sequence assumes that the high pressure injection fails followed by an eventual core melt.

The frequency of this sequence is estimated as:

$$T(FIA)KD_1 = 2.8x10^{-6}$$

The dominant contributors to RPS failure are due to double circuit breaker failures. (These circuit breaker failures cannot be recovered by pushing the trip buttons

within the control room and were, therefore, assessed to be non-recoverable.) HPIS failure is dominated by failure of the operator to actuate the system.

These cut sets are listed below:

Cut Set	Cut Set Frequency
T(FIA)*RPSOOOBB-BCC-LF*RPSOOD2D-BCC-LF*HPIPUMP-CM	7.1×10^{-7} (1)
T(FIA)*RPSOOOBB-BCC-LF*RPSOOD1D-BCC-LF*HPIPUMP-CM	7.1×10^{-7} (1)
T(FIA)*RPSOOOAA-BCC-LF*RPSOOC2CBCC-LF*HPIPUMP-CM	7.1×10^{-7} (1)
T(FIA)*RPSOOOAA-BCC-LF*RPSOOC1C-BCC-LF*HPIPUMP-CM	7.1×10^{-7} (1)

Term Descriptions

T(FIA) - reactor trip with all front line systems initially available (e.g., turbine trip); F(T(FIA)) = 7.1/Ryr.

RPSOOOBB-BCC-LF - reactor trip breaker B fails to open (B and D1 or D2 will cause RPS failure); P(RPSOOOBB-BCC-LF) = 1×10^{-3}.

RPSOOOAA-BCC-LF - reactor trip breaker A fails to open (A and C, or C2 will cause RPS failure); P(RPSOOOBB-BCC-LF) = 1×10^{-3}.

RPSOOD2D-BCC-LF - reactor trip breaker D2 fails to open (D2 and B will cause RPS failure); P(RPSOOD2D-BCC-LF) = 1×10^{-3}.

RPSOOD1D-BCC-LF - reactor trip breaker D1 fails to open (D1 and B will cause RPS failure); P(RPSOOD1D-BCC-LF) = 1×10^{-3}.

RPSOOC2C-BCC-LF - reactor trip breaker C2 fails to open (C2 and A will cause RPS failure); P(RPSOOC2C-BCC-LF) = 1×10^{-3}.

RPSOOC1C-BCC-LF - reactor trip breaker C1 fails to open (C1 and A will cause RPS failure); P(RPSOOC1C-BCC-LF) = 1×10^{-3}.

HPIPUMP-CM - operator fails to initiate HPIS; P(HPIPUMP-CM) = 0.1. (This probability was assigned to be 0.1 to reflect an extremely high stress situation.)

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence $T(D01)LD_1\alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus D01 (125VDC) with concomitant failure of the power conversion system T(D01), followed by failure of the emergency feedwater system (L), and the high pressure injection system (D_1). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure due to hydrogen burning (β), penetration leakage (γ), or base mat melt-through (ϵ).

This sequence depicts a loss of the systems which provide the normal and emergency 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 actuate the high pressure injection system (HPIS) and establish a "feed and bleed"

core cooling operation. If the operator fails to actuate the HPIS or the HPIS subsequently fails, the RCS inventory would boil off through the pressurizer safety relief valves leading to uncovering the core and eventual core melt. It is estimated that core melting will begin at approximately one hour.

This sequence is initiated by failure of the "odd" DC bus. Failure of this bus causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the HPIS and emergency feedwater system. Hardware and human failures in the remaining one-half of these two systems comprise the dominant contributors to the sequence frequency. It is estimated that roughly 85 percent of these failures can be recovered before the onset of core melt. Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

The frequency of this sequence is estimated as:

$$T(D01)LD_1 = 2.2 \times 10^{-6}.$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency
T(D01)*LF-HPI-H14*LF-EFW-E4	7×10^{-7} (.23)
T(D01)*LF-HPI-H14*LF-EFW-E29	4.5×10^{-7} (.22)
T(D01)*LF-HPI-H14*LF-EFW-E11	2.3×10^{-7} (.23)
T(D01)*LF-HPI-H14*LF-EFC-ACBD4	1.4×10^{-7} (.05)
T(D01)*LF-HPI-H14*LF-EFC-VCD2	1.2×10^{-7} (.05)
T(D01)*LF-HPI-H14*LF-EFC-BB7B1CM	6.8×10^{-8} (.05)
T(D01)*LF-HPI-H14*LF-EFC-D1D2CM	5.8×10^{-8} (.05)
T(D01)*LF-HPI-H14*LF-EFC-CSY2	4.9×10^{-8} (.05)
T(D01)*HPI-PUMP-CM*LF-EFW-E11	4×10^{-8} (1)

Term Descriptions

T(D01) - failure of ES bus D01 (125VDC) (fails EFS electric pump and 1/2 turbine pump flow control valves and 1/2 turbine pump steam admission valves, HPIS A and B pump); F(T(D01)) = 1.8×10^{-2}/Ryr.

LF-HPI-H14 - local fault in HPIS pipe segment H14 (fails HPIS C pump); P(LF-HPI-H14) = .012.

HPI-PUMP-CM - failure of operator to initiate HPIS; P(HPI-PUMP-CM) = 5×10^{-4} (See Appendix B15.)

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine driven pump); P(LF-EFS-E11) = 4×10^{-3}.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E4) = .012.

LF-EFC-ACBD4 - local fault in "EFIC Initiate signal" path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-ACBD4) = .011.

LF-EFC-VCD2 - local vault in "EFIC Vector" signal path (fails 1/2 EFS turbine pump flow control valves); P(LF-EFC-VCD2) = .0094.

LF-EFS-E29 - Local fault in EFS pipe segment E29 (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFS-E29) = .0081.

LF-EFC-BB7B1CM - local fault in "EFIC Initiate" signal path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-BB7B1CM) = .0054.

LF-EFC-CSY2 - local fault in "EFIC Initiate" signal path (fails 1/2 turbine pump steam admission valves); P(LF-EFS-CSY2) = .0039.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence $T(A3)LD_1\alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus A3(4160VAC) with concomitant failure of the power conversion system (TA3), followed by failure of the emergency feedwater system (L), and the high pressure injection system (D_1). 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 $T(D01)LD_1$ sequence just described, except that in this case the initiating event is caused by failure of an "odd" AC bus. Like in the previous sequence, failure of this bus causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the high pressure injection system and emergency feedwater system. Hardware and human failures in the remaining one-half of these two systems comprise the dominant contributors to the sequence frequency. It is estimated that roughly 85 percent of these failures can be recovered before the onset of core melt (~1 hour). Most recovery actions

entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

The frequency of this sequence is estimated as:

$$T(A3)LD_1 = 1x10^{-6} .$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency
T(A3)*LF-HPI-H14*LF-EFS-E11	$4.6x10^{-7}$ (.23)
T(A3)*LF-HPI-H14*LF-EFC-D1D2CM	$1.1x10^{-7}$ (.05)
T(A3)*HPI-PUMP-CM*LF-EFS-E11	$8x10^{-8}$ (1)
T(A3)*LF-HPI-H14-LF-EFW-E22	$3.4x10^{-8}$ (.23)
T(A3)*LF-HPI-H14*LF-EFW-E5*LF-EFW-E4	$1.6x10^{-8}$ (.23)

Term Descriptions

T(A3) - failure of ES bus A3 (4160VAC) (fails HPIS pumps A and B, and EFS electric pump F(T(A3)) = $3.5x10^{-2}$/Ryr.

LF-HPI-H14 - local fault in HPIS pipe segment H14 (fails HPIS C pump); P(LF-HPI-H14) = .012.

HPI-PUMP-CM - failure of operator to initiate HPIS; P(HPI-PUMP-CM) = $5x10^{-4}$ (See Appendix B15.)

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine driven pump); P(LF-EFS-E11) = $4x10^{-3}$.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E4) = .012.

LF-EFS-E5 - local fault in EFS pipe segment E5 (fails 1/2 turbine pump flow control valves); P(LF-EFS-E5) = .012

LF-EFS-E22 - local fault in EFS pipe segment E22 (fails turbine pump); P(LF-EFS-E22) = $3x10^{-4}$.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; 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 8-1.

Sequence $T(D01)LD_1C$ α, β, γ, ϵ :

This sequence is initiated by a failure of engineered safeguards power bus D01(125VDC) with concomitant failure of the power conversion system T(D01), followed by failure of the emergency feedwater system (L), the high pressure injection system (D_1), and the reactor building spray system (C). 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 $T(D01)LD_1$ discussed earlier except that for this sequence the reactor building spray system (RBSS) also fails. Failure of DC bus D01 causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the emergency feedwater system, high pressure injection system (HPIS), and RBSS. Hardware failures in the remaining half of the latter three systems comprise the dominant contributors to the sequence frequency. Failure of the HPIS and RBSS is dominated by a MOV which is common to the suction of the pumps in the remaining half

of these systems. It is estimated that roughly 85 percent of the hardware failures can be recovered before the onset of core melt (~1 hour). Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room.

The frequency of this sequence is estimated as:

$$T(D01)LD_1C = 1.8 \times 10^{-6} .$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency
T(D01)*LPI1408B-VCC-LF*LF-EFW-E11	6.1×10^{-7} (1)
T(D01)*LPI1408B-VCC-LF*LF-EFW-E4	4.5×10^{-7} (.25)
T(D01)*LPI1408B-VCC-LF*LF-EFW-E29	2.7×10^{-7} (.22)
T(D01)*LPI1408B-VCC-LF*LF-EFC-ACBD4	8.1×10^{-8} (.05)
T(D01)*LPI1408B-VCC-LF*LF-EFC-VCD2	7×10^{-8} (.05)
T(D01)*LPI1408B-VCC-LF*LF-EFC-BB7B1CM	4×10^{-8} (.05)
T(D01)*LPI1408B-VCC-LF*LF-EFC-D1D2CM	3.4×10^{-8} (.05)
T(D01)*LPI1408B-VCC-LF*LF-EFC-CSY2	2.9×10^{-8} (.05)

Term Descriptions

T(D01) - failure of ES bus D01 (125VDC) (fails EFS electric pump and 1/2 turbine pump flow control valves and 1/2 turbine steam admission valves, HPIS A and B pump and RBSI A pump); F(T(D01)) = .018.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine pump); P(LF-EFS-E11) = .0041.

LF-EFC-CSY2 - local fault in "EFIC Initiate" signal path (fails 1/2 turbine pump steam admission valves); P(LF-EFC-CSY2) = .0039.

LF-EFS-E4 - local fault in EFS pipe segment E4 (fails 1/2 turbine pump flow control values); P(LF-EFS-E4) = .012.

LPI1408B-VCC-LF - local fault of LPIS valve CV1408 (fails suction to HPIS C pump and RBSI B pump); P(LPI1408B-VCC-LF) = .0082.

LF-EFC-ACBD4 - local fault in "EFIC Initiate signal" path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-ACBD4) = .011.

LF-EFC-VCD2 - local vault in "EFIC Vector" signal path (fails 1/2 EFS turbine pump flow control valves); P(LF-EFC-VCD2) = .0094.

LF-EFS-E29 - local fault in EFS pipe segment E29 (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFS-E29) = .0081.

LF-EFC-BB7B1CM - local fault in "EFIC Initiate" signal path (fails 1/2 EFS turbine pump steam admission valves); P(LF-EFC-BB7B1CM) = .0054.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; category 4
$P(\epsilon) = 0.5$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 8-1.

Sequence $T(A3)LD_1C$ $\alpha, \beta, \gamma, \epsilon$:

This sequence is initiated by a failure of engineered safeguards power bus A3 (4160VAC) with concomitant failure of the power conversion system T(A3), followed by failure of the emergency feedwater system (L), the

high pressure injection system (D_1), and the reactor building spray system (C). 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 very similar to T(D01)LD_1C just discussed except that this sequence is initiated by an AC rather than a DC bus failure. Failure of AC bus causes a reactor trip, interruption of the power conversion system, and failure of approximately one-half of the emergency feedwater system, high pressure injection system (HPIS), and RBSS. Hardware failures in the remaining half of the latter three systems comprise the dominant contributors to the sequence frequency. Failure of the HPIS and RBSS is dominated as in the previous sequence, by a MOV which is common to the suction of the pumps in the remaining half of these systems. It is estimated that roughly 60 percent of the hardware failures can be recovered before the onset of core melt (~1 hour). Most recovery actions entail starting systems manually from the control room following failure of auto actuation circuitry or opening valves and closing circuit breakers outside the control room. The frequency of the sequence is dominated, however, by two cut sets which are estimated to have little or no recovery potential. If the HPIS/RBSS common suction valve fails closed, the HPI pumps would fail within a few minutes followed by failure of the spray pumps within approximately 15 minutes. The emergency feedwater system non-recoverable faults are due to failure of the turbine pump or one of its condensate storage tanks (CST) suction valves. No plant data was available

to estimate recovery of the turbine pump given a start failure and thus no recovery credit was given. Also, if one of the turbine pump CST suction valves fails closed, the pump is predicted to fail before the operator can reallign the pump to the alternate service water system water source.

The frequency of this sequence is estimated as:

$$T(A3)LD_1C = 1.4x10^{-6}$$

The dominant contributors to this frequency are:

Cut Set	Cut Set Frequency	
T(A3)*LPI1408B-VCC-LF*LF-EFW-E11	$1.2x10^{-6}$	(1)
T(A3)*LPI1408B-VCC-LF*LF-EFW-E22	$8.8x10^{-8}$	(1)
T(A3)*LPI1408B-VCC-LF*LF-EFC-D1D2CM	$6.7x10^{-8}$	(.05)

Term Descriptions

T(A3) - failure of ES bus A3 (4160VAC) (fails EFS electric pump, HPIS A and B pump and RBSI A pump); F(T(A3)) = .035.

LF-EFS-E11 - local fault in EFS pipe segment E11 (fails turbine pump); P(LF-EFS-E11) = .0041.

LPI1408B-VCC-LF - local fault of LPIS valve CV1408 (fails suction to HPIS C pump and RBSI B pump); P(LPI1408B-VCC-LF) = .0082.

LF-EFC-D1D2CM - local fault in "EFIC Vector" signal path (fails EFS turbine pump flow control valves); P(LF-EFC-D1D2CM) = .0046.

LF-EFS-E22 - local fault in EFS pipe segment E22 (fails turbine pump); P(LF-EFS-E22) = $3x10^{-4}$.

The containment failure mode probabilities and release category placements taken from Section 8.1.2 are:

$P(\alpha) = 0.0001$; category 1
$P(\gamma) = 0.5$; category 2
$P(\beta) = 0.007$; category 4
$P(\epsilon) = 0.5$; category 6

Multiplying the sequence frequency with the containment failure mode probabilities results in the values presented in Figure 8-1.

8.1.2 Core Meltdown Phenomenology Associated With Dominant System Accident Sequences

The results of the expected core meltdown phenomenology associated with the dominant and near dominant Arkansas Nuclear One (ANO) sequences is summarized in Table 8-2. The accident processes, timing of core melt, containment failure modes, and fission product releases to the atmosphere for these sequences have been estimated based primarily on previous analyses for the Oconee PWR.[2] Comparison of the ANO plant specifications, as described in the Final Safety Analysis Report, with those of Oconee indicates the two plants are quite similar. With one exception, the accident sequences examined for Oconee are similar in character to those listed in Table 8-2 for ANO. Several of the ANO sequences involve reactor coolant pump seal ruptures which did not appear in the Oconee study. The resulting LOCA is significantly smaller than any LOCA analyzed for Oconee. It is believed, however, that the Oconee analysis provides a sufficient data base to evaluate the ANO accident phenomenology and fission product releases, and no plant-specific MARCH or CORRAL code calculations were performed for the present ANO evaluation.

The fission product release categories listed in Table 8-2 for the various sequences are the same as those employed for the PWR in the Reactor Safety Study.[18]

Table 8-2

Summary of Expected Core Meltdown Phenomenology
Associated With ANO Sequences

Sequence**	Release Category*						
	1	2	3	4	5	6	7
$B(1.2)D_1$	$\alpha = .0001$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
$B(1.2)D_1C$	$\alpha = .0001$	$\gamma = .5$		$\beta = .007$		$\epsilon = .5$	
TLDYC	$\alpha = .0001$	$\delta = .2$		$\beta = .007$		$\epsilon = .8$	
$B(1.66)H_1$	$\alpha = .0001$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
$TLQ-D_3$	$\alpha = .0001$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
$B(4)H_1$	$\alpha = .01$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
TKD_1	$\alpha = .0001$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
TLD	$\alpha = .0001$	$\gamma = .5$			$\beta = .007$		$\epsilon = .5$
TLDC	$\alpha = .0001$	$\gamma = .5$		$\beta = .007$		$\epsilon = .5$	

*Reactor Safety Study (Reference 18) PWR release categories and containment failure modes, where:

α = vessel steam explosion
β = penetration leakage
γ = overpressure due to hydrogen burning
δ = overpressure due to steam evolution
ϵ = base mat melt-through

**The phenomenology of the ANO-1 transient accident sequences is independent of the specific transient initiating event. Thus, only nine dominant sequences are listed here because, e.g., $T(A2)LD_1$ and $T(D01)LD_1$, have similar phenomenological characteristics.

The notation for the containment failure modes (α, γ, δ, etc.) is also the same. The probability (α) that a steam explosion in the reactor vessel causes containment failure is taken to be 0.01 for those sequence in which the primary system has depressurized by the time of the assumed explosion. This is identical to the value used in the Reactor Safety Study. For explosions taking place at elevated system pressure the probability is taken to be 0.0001. The lower value is based on recent research performed at Argonne and Sandia National Laboratories which indicates steam explosions may be suppressed at high system pressures. Thus, for cases in which core meltdown occurs with the primary system at high pressure, steam explosions are assessed to be less likely. Containment isolation failure (β) is assumed to be the same as in the Oconee study.

Early containment overpressure failure may occur at ANO due to two mechanisms. For cases in which the containment building fan coolers or sprays are operating, early containment overpressure by rapid hydrogen burning (γ) is possible. For cases in which the containment safety features are not operating, combustible hydrogen mixtures are not predicted due to the high partial pressures of steam. However, for sequences of this type early containment overpressure (δ) is possible due to rapid steam generation from a debris-water interaction in the reactor cavity. This steam pressure spike results when accumulator injection is delayed by the high primary system pressures until after bottom head failure. Interaction of the accumulator water and core debris may produce a steam pressure rise approaching

the nominal containment failure pressure.[1] A containment failure probability of $\delta = 0.2$ is estimated for this failure mechanism. Hydrogen burning taking place at the time of vessel head failure produces a pressure approximately equal to the nominal containment failure pressure;[2] thus, a failure probability of $\gamma = 0.5$ is estimated.

There is considerable uncertainty as to whether containment melt-through would take place. Whether or not melt-through occurs depends on the geometry/coolability of the melted core in the reactor cavity. For the present evaluation melt-through is assumed if the other modes of containment failure are avoided.

Table 8-2 assigns the several containment failure modes to fission product release categories. Steam explosions produce PWR Category 1 releases. Isolation failure (β) produces Category 4 and 5 releases, and basemat melt-through (ϵ) produces Category 6 and 7 releases. The lower releases are obtained when containment sprays operate to remove fission products from the containment atmosphere. Early containment failure (γ and δ) produces a PWR Category 2 release. Note that the fission product releases associated with early containment failures are not affected by the potential availability of containment sprays to scrub fission products. This occurs because containment sprays are not initiated for these sequences. The building coolers maintain containment pressures below 30 psig set point for the sprays until after head failure.

---

[1] Based on the Oconee TMLB'- δ results.
[2] Based on the Oconee TML- γ results.

However, simultaneous hydrogen burning would fail containment and preclude effective spray function. If hydrogen burning does not occur, the sprays would be activated by the rapid vaporization of the accumulator water in the reactor cavity. Consequently, the and releases are affected by potential spray scrubbing but not the β and ϵ releases.

8.2 Engineering Insights

During the course of this analysis, several engineering insights were realized concerning the operational safety of ANO-1. These insights can be categorized as being related to either plant design and hardware or plant operations.

8.2.1 Plant Design Engineering Insights

- The list of the dominant sequences (Figure 8-1) and those identified to be near dominant (Appendix C) indicates that the following general classes of accident sequences contribute most to the ANO-1 core melt frequency.
  - LOCAs initiated by reactor coolant pump seal ruptures contribute 20 percent.
  - Station blackout sequences contribute ~ 20 percent.
  - Sequences initiated by ANO AC and DC power bus failures contribute ~35 percent.
  - Other transients and small LOCAs contribute ~ 20 percent.
  - Large LOCA sequences contribute <5 percent.

- The total frequency of core melt for ANO-1 is estimated at 5×10^{-5}/yr. This estimate is similar to estimates made for several other light water reactors in other probabilistic risk assessments, e.g., Surry, Peach Bottom,[18] Oconee,[2] and Grand Gulf.[26]

- Several single failures were identified in front line/support systems. Operator recovery of some of these single failures is possible, however. The singles identified were:

  - The high pressure recirculation system pump room cooling has several single failures due to loss of electric power and service water events. The operator may recover from this event by starting an alternate room cooler, but plant procedures and/or control room indication may not be adequate to perform recovery actions before high pressure pump failure occurs.

  - A single valve failure can obstruct the common service water discharge line. This would cause a reactor trip and several transient mitigating systems to be unavailable. The operator may recover from this event by performing actions away from the control room and utilizing an alternate discharge line.

  - Both emergency feedwater pumps take suction from the condensate storage tank through a common header containing three valves. Failure of any of these valves could cause failure of both pumps before

the operator recognizes the problem and aligns the suction of the pumps to an alternate water supply.

- All pumps located within the high pressure, low pressure, and spray system take suction from the borated water storage tank via a common header containing a manual valve. Failure of this valve in the closed position would cause failure of all three systems. No recovery action was identified since the dominant valve failure mode would require disassembly of the valve to correct.

o The list of dominant accident sequences indicate that support system faults are important to the risk of the plant. The most important support systems were AC/DC power and service water. Of lesser importance were room cooling systems and automatic actuation systems. The former were most important because faults within these systems can cause a reactor initiating event with concomitant failure of several safety system components. AC/DC and service water faults also had lower recovery potential than other support systems. Room cooling and auto actuation system faults were of less importance because significant initiating events were not identified and recovery potential was generally high.

o Review of ANO-1 logs revealed the following safety-related data trends as compared with generic nuclear industry data. (The generic data was provided by NRC and was very similar to the WASH-1400 data base.)

- Motor operated valve failure on demand probabilities are higher than industry data (~ factor of 4).
- Air operated valve failure on demand probabilities are higher than industry data (~ factor of 10).
- Diesel generator failure on demand probabilities are about the same as industry data.
- Pump and valve control circuit failure on demand probabilities are lower than what can be derived from industry data (~ factor of 4).
- Reactor building fan coolers have a higher failure on demand probability than industry fan data because of the policy at ANO-1 not to repair a reactor building fan until the next reactor shutdown. (~ factor of 80)
- The probability of main feedwater system failure following reactor trips which were not initiated by loss of main feedwater (e.g., turbine trip, loss of load, etc.) is higher than that reported in WASH-1400 (~ factor of 6).
- Review of ANO-1 trip logs and comparison with reactor trip data presented in Reference 4 indicated that ANO-1 transient frequencies and type are typical of the nuclear industry.

o An upgrade of the emergency feedwater system and installation of a new emergency feedwater control system/steam generator isolation

control system is scheduled to be completed by 1982. The new control systems were designed such that single integrated control system (ICS) faults or nonnuclear instrumentation (NNI) faults will not fail or significantly degrade the emergency feedwater system. (These types of failures have plagued B&W reactors in the past.) Review of preliminary design information verified this to be the case.

- An upgrade of NNI power supplies has been implemented at ANO-1. This upgrade has enhanced the reliability of NNI power supplies and has eliminated NNI single failures which can cause an inadvertant LOCA due to opening of the PORV. (This type of failure was possible in the previous NNI/ERV design.)

- The switchover from the borated water storage tank to the containment sump, in response to small LOCA, requires some operator actions outside the control room in radiation areas. Switchover at other plants we have studied can perform all required actions within the control room.

- Via use of probabilistic importance measures,[1] the ANO-1 components/events which contribute most to the core melt frequency, assuming the operator does not attempt to recover failed system components, are all related to the plant design. The top 40 components/events are ranked according to Fussell-Vesely importance measure in Table 8-3. (The Birnbaum measure is also given.) The top 10 consist of six initiating events (T(D01), B(1.2), B(4), T(LOP),

[1]There are a number of probabilistic importance measures that can be applied to a core melt probability expression. These include the Birnbaum, Criticality, and Fussell-Veseley measures and the upgrading function. All of these measures are defined and discussed in Reference 23 and compared in Reference 24. The criticality and Fussell-Vesely measures and the upgrading function all give the same ranking of events for reliable systems. The Birnbaum and Fussell-Vesely measures are applied to the core melt expression. The Birnbaum measure for a primary event is the partial derivative of the probability expression with respect to the probability of each primary event. It is an indication of the sensitivity of the overall system reliability to the primary event reliability since it measures the rate of change of system reliability to change in primary event reliability. This measure is not a function of the primary event probability, however, so it is usually used with one of the measures which does include the probability of the primary event such as the Fussell-Vesely measure. The Fussell-Vesely measure is the product of the Birnbaum measure and the probability of the primary event divided by system unavailability (or core melt frequency). Thus, the Fussell-Vesely measure is the probability of the union of all of the minimal cut sets which contain the primary event divided by the core melt frequency. The ranking of the primary events is an indication of which events contribute most to the core melt frequency.

Table 8-3

Importance Measure Ranking of
Fault Tree Events

	Event	Fussell-Vesely Measure	Birnbaum Measure
1	T(D01)	.362	4.327E-03
2	B(1.2)	.157	1.688E-03
3	B(4)	.153	8.635E-02
4	T(LOP)	.144	9.662E-05
5	Q	.126	1.355E-03
6	B(166)	.124	8.609E-02
7	BATCM	.109	3.200E-01
8	EFW0P7AX-PTD-LF	.061	3.536E-03
9	ECS6254B-B-AASF	.051	2.018E-03
10	T(A3)	.060	3.741E-04
11	SWS3810B-VCC-LF	.049	2.560E-03
12	LPI1408B-VCC-LF	.049	2.561E-03
13	ECS6034B-DPC-LF	.038	2.018E-03
14	ECS6034B-BPC-LF	.038	2.018E-03
15	EFICVD25-CBL	.036	3.411E-03
16	EFICAC04-1AC-LF	.035	1.379E-03
17	EFICBD04-1BD-LF	.035	1.379E-03
18	ECSCH4AB-CWU-LF	.035	2.018E-03
19	ECS5254A-B-AASF	.029	1.162E-03
20	IEAODG1A-GEN-LF	.027	1.793E-04
21	EFICVD12-CBL	.026	3.251E-03
22	EFW2620B-VCC-LF	.026	1.362E-03
23	EFWD0X1A-VDC-LF	.026	1.362E-03
24	EFW00Y2B-VCC-LF	.026	1.362E-03
25	EFICVD41-CBL	.026	1.362E-03
26	EFICCSY2-CBL	.025	1.362E-03
27	ECS6036A-BPC-LF	.022	1.162E-03
28	ECS6036A-DPC-LF	.022	1.162E-03
29	SWS6214B-B00-CC	.022	2.325E-03
30	HPIA406B-B00-CC	.022	2.325E-03
31	SWS3820A-V00-LF	.022	1.162E-03
32	SWS3643A-V00-LF	.022	1.162E-03
33	LPI1407A-VCC-LF	.021	1.087E-03
34	ECSCH4BA-CWU-LF	.020	1.162E-03
35	IEA0DG2B-GEN-LF	.019	1.252E-04
36	LPI6164B-B00-CC	.019	2.049E-03
37	5653A-CBL-LF	.018	1.162E-03
38	5181A-CBL-LF	.018	1.162E-03
39	ECS6254B-B00-CC	.018	1.886E-03
40	SWS0402B-B00-CC	.018	1.886E-03

B(1.66), T(A3)), failure of the pressurizer safety values to reclose after being demanded open (Q), common mode battery failure (BATCM), failure of the turbine driven emergency feedwater pump (EFWOP7AX-PTD-LF), and failure of the thermostat which actuates AC/DC room cooler VCH4A (ECS6254-B-AASF).

- The core meltdown analysis presented in Section 8.1.2 suggests that there is a strong correlation between the ANO core melt frequency and expected ANO risk. Table 8-2 indicates that every core melt sequence has a .2 to .5 probability of being placed in a high risk release category (Category 2).

8.2.2 Plant Operations Engineering Insights

- A review of the dominant and near dominant accident sequence cut sets reveals that only 10 percent of the total core melt frequency is attributed to operator errors committed during the course of an accident. One of the main reasons for this low contribution is due to the post Three Mile Island directive by the NRC requiring an increased number of licensed operators to be present in the control room. The added human redundancy afforded by this directive significantly increases the probability of recovering from operator errors. Another reason for the low contribution is due to the recent installation of the Safety Parameter Display System (SPDS) at ANO-1. The SPDS continuously plots the reactor coolant system pressure and temperature and

compares them to operating envelopes and saturation curves. We feel the SPDS is an excellent diagnostic tool and thus affords recovery potential from operator errors. The SPDS also provides the type of information necessary to determine that a core damage accident is likely.

- A review of the dominant and near dominant sequences reveals that operator recovery actions play an important role in reducing the frequency of various accidents. Overall, operator recovery reduced the ANO-1 core melt frequency by approximately a factor of 6.

- The unavailability of ANO-1 systems due to outages resulting from test and maintenance is generally small compared with other faults. Test unavailabilities are small because most systems are not taken out of service during the test and are thus able to perform their safety function. For those systems that are taken from service, test personnel are, in general, kept in contact with control room operators so that the system could be quickly restored to service upon request by the operator. Review of plant maintenance logs revealed that the frequency at which a given active component is taken out for maintenance is small while the plant is at power. A comparison of the ANO maintenance frequency with the plants studied in the RSS, for example, indicates that components are taken out for maintenance about an order of magnitude less frequently at ANO. The primary reason for the small maintenance frequency is due to the policy at ANO-1 not to

perform periodic preventive maintenance on safety systems when the plant is at power. Preventive maintenance on these systems is conducted during reactor shutdowns.

- Safety system/component unavailabilities caused by the failure of personnel to realign valves and circuit breakers to their safeguards positions after test and maintenance activities are generally small compared with other faults. There are several reasons for this including: (1) the component tagging procedure requires the operators to perform redundant checks of valve and circuit breaker alignment following test and maintenance, (2) most safety system valves and circuit breakers have alignment indication in the control room and are verified via a check list to be in the correct position every 8-hour shift, (3) required post maintenance tests of components would, in general, inform the operator that valves and circuit breakers have not been aligned properly.

8.3 Design and Procedural Changes Made at ANO-1

There were three changes made in ANO-1 procedures as a result of this study. The systems analysis presented in this study is based on the implementation of these changes. These changes are listed and discussed below.

1. Quarterly tests of the two station batteries are now required to be performed on a staggered basis, i.e., one battery every six weeks. The previous procedure allowed both batteries to be tested on the same day by the same personnel.

2. AC and DC switchgear room cooler actuation circuitry are now required to undergo a complete test. The previous test procedure omitted the sensing portion of the circuitry.

3. An error identified in the low pressure pump test procedure was corrected.

Results presented in "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants" (Reference 5) indicate that failure of multiple station batteries at nuclear power plants have occurred in the past. One of the potential causes for such failures identified in that report was due to common mode test and maintenance errors. The changes introduced to the battery test procedure, requiring staggered battery tests, reduced the probability of such a common mode failure.

As discussed in Chapter 6, cooling of the AC and DC switchgear rooms is required for successful long term operation of LOCA and transient safety systems. The fault tree analysis of the room chillers revealed that the thermostat circuitry which actuates the room chillers was not required to be tested. The change introduced to the room chiller test procedure now requires the chillers to be actuated by applying a heat source to the thermostats.

A potentially significant error was identified in the low pressure injection system pump test procedure. Upon completion of a pump test, certain valves must be realigned to return the pump train to service. The procedure requested the wrong valves to be realigned.

Discussions with plant personnel revealed that this error had been identified and corrected a few years previous. However, they could not account for the reintroduction of the error. Upon closer examination, it became evident the error was reintroduced because the names of the valves to be realigned violated the standard component naming scheme implemented at the plant. In most systems at the plant, components in train A have an "A" in the component identifier and components in train B have a "B" in the component identifier. However, an exception to this rule exists in the low pressure injection system. Some valves with a "B" identifier must be realigned to return an "A" pump to service and vice versa. An unknowing reviewer of the test procedure must have seen an "A" and "B" together and thought it was a typographical error. It has been suggested to the plant that for all procedures involving a violation of the component naming scheme that a special note be attached warning reviewers and test personnel that the procedure is correct.

8.4 Analysis Uncertainties

The data and analytical models used to quantify the ANO-1 accident sequences are not absolute. Uncertainties that are sometimes large exist in both areas. This section will investigate many of these uncertainties and assess the affect they can have on the quantative results of this study. Section 8.4.1 and 8.4.2 address the data and modelling uncertainties respectively.

8.4.1 Data Uncertainties

In order to take into account variations and uncertainties in the data, a Monte Carlo simulation was

performed on the Boolean expressions for the dominant accident sequences. A simulation was also performed on a Boolean expression for core melt.

The core melt expression was formed in the following manner. Each dominant accident sequence, S_i, has a Boolean minimal cut set expression

$$S_i = \sum_{j=1}^{K} M_j .$$

where M_j = minimal cut sets excluding recovery. A core melt expression was formed by taking the Boolean sum of the dominant accident sequences,

$$CM = \sum_{i=1}^{n} S_i .$$

By substituting the minimal cut set expressions for each S_i and applying the minimal cut set algorithm to the resulting Boolean expressions, a core melt Boolean expression was formed. This expression represents all of the smallest combinations of primary events which, if they all occur, will cause core melt. These combinations of primary events are the core melt minimal cut sets. The Boolean minimal cut set expression for core melt has a related probability expression.

A median probability and an error factor were associated with each primary event. The error factor was used to define a possible range of values for a particular random variable. If the median probability of occurrence of some primary event X is $X_{0.5}$, then the

possible values of the random variable representing the occurrence of X are between $X_{0.5}/f$ and $X_{0.5} \cdot f$, where f is the associated error factor. The primary event error factors utilized was dependent upon the data type, i.e., (a) generic data was generally assigned the error factors listed in Reference 14 see also Appendix C, (b) plant specific data was assigned an error factor of 3, (c) human error data was assigned an error factor of 10. The median probability and the error factor were used to calculate upper and lower bounds which were assumed to be 95th and 5th percentile points of a log-normal distribution. From this, the parameters of the probability distribution for the primary events were calculated. The applicability of the log-normal distribution for describing the various data ranges is discussed in Reference 18.

By taking a random sample from the probability distribution for each primary event, a total frequency was computed for each accident sequence and core melt Boolean expression. By repeating this for a total of 1200 trials, a distribution of the accident sequence and core melt frequencies was determined. For the resulting distributions, a mean and standard deviation, as well as the 5th, 50th and 95th percentile points, were formed.

The frequency of the initiating events and the probability of nonrecovery were included as point estimates in the sequence uncertainty calculations. Insufficient information regarding the distributions associated with each of these parameters was available to feel confortable assigning error factors to them. Thus, the resulting uncertainty estimates include only the uncertainty

associated with the data, not the initiating events and the recovery factors. Uncertainty in the recovery model is investigated in the following section.

The results of the simulations performed on the dominant accident sequences and the core melt expression are summarized in Table 8-4. As can be noted, all sequences have approximately an order of magnitude spread between the 5 percent and 95 percent bounds (i.e. roughly an error factor of 3) except T(LOP)LD_1YC, T(D01)LQ-D_3, T(A3)LQ-D_3, and T(FIA)KD_1. These sequences have a much larger error spread. The large error spread on T(LOP)LD_1YC is due to the error factor of 10 assigned to the dominant cut set, namely, the common mode battery failure term. The error spread on the T(D01)LQ-D_3 and T(A3)LQ-D_3 sequences results from error factor of 10 assigned to Q event. The Q event appears in every sequence cut set and represents failure of either pressurizer safety valve to reclose after opening. During these sequences, solid and/or two phase water is expected to be relieved through these valves. Since these valves were designed to relieve steam only, the error factor of 10 represents the uncertainty associated with this off normal operation. The error spread on T(FIA)KD_1 is due to the human error of failing to actuate high pressure injection (error factor of 10) which appears in every dominant cut set, and the fact that the top four cut sets are all derived from the same data base. Cut sets which are quantified from the same data base are "statistically dependent," summing statistically dependent cut sets tends to broaden uncertainty bounds.

Table 8-4

Data Uncertainty Analysis Results

Sequence	Point Estimate	Median	Mean	Error Factor
$B(1.2)D_1$	2.8E-6	5.2E-6	6.5E-6	3
$B(1.2)D_1C$	4.4E-6	5.5E-6	7.0E-6	3
$T(LOP)LD_1YC$	9.9E-6	1.7E-5	6.4E-5	11.4
$B(4)H_1$	1.4E-6	1.7E-6	2.0E-6	2.4
$T(D01)LD_1YC$	3.1E-6	3.6E-6	4.2E-6	3.8
$T(D02)LD_1YC$	2.5E-6[1]	2.2E-6	3.4E-6	4.4
$B(1.66)H_1$	1.2E-6	1.5E-6	1.8E-6	2.2
$T(D01)LQ-D_3$	4.0E-6	4.8E-6	1.6E-5	11.6
$T(A3)LQ-D_3$	3.3E-6	4.7E-6	1.6E-5	13
$T(FIA)KD_1$	2.8E-6	2.8E-6	2.0E-5	37
$T(D01)LD_1$	2.2E-6	3.2E-6	4.3E-6	3.2
$T(A3)LD_1$	9.5E-7	1.4E-6	1.8E-6	3.4
$T(D01)LD_1C$	1.8E-6	2.2E-6	3.0E-6	3.3
$T(A3)LD_1C$	1.4E-6	1.9E-6	2.5E-6	3.0
Total Core Melt	4.2E-5[2]	6.0E-5	9.2E-5	4.3

NOTES: 1. Point estimate is larger than median due to cut set truncation which was required to perform the Monte Carlo simulation.
2. This is the total core melt frequency of these 14 sequences only.

8.4.2 Modeling Uncertainties

Several assumptions were incorporated into the structure of the analytic models utilized in this study. These assumptions were generally founded upon engineering judgment. While we feel the assumptions are good, we recognize that alternate assumptions could have been made which could significantly impact the model structure. In this section we investigate the affect that an alternate set of assumptions would have on quantitative results of this study. Nine of the more controversial assumptions, defined as sensitivity issues, are investigated in the following paragraphs. Table 8-5 summarizes the affect that these sensitivity issues have on the total core melt frequency estimated for ANO-1.

Reactor Coolant Pump (RCP) Seal Leakage Induced by Loss of Seal Cooling

The fault trees and event trees developed for ANO-1 do not explicitly model loss of seal cooling to a stationary RCP. This is potentially nonconservative since analyses (References 20 and 22) of RCPs similar to ANO-1s (Byron Jackson) have indicated that seal leakage in the range of 10-70 gpm per pump may result following an extended loss of RCP seal cooling. This study did not model loss of seal cooling events primarily because the experiment reported in Reference 19 showed that significant leakage did not occur for 56 hours following interruption of seal cooling to a static Byron Jackson RCP seal. It should be noted, however, that this experiment was performed in a laboratory using a new seal, and may not be directly applicable to a worn seal. RCP seals may experience

Table 8-5
Summary of Sensitivity Issues

Sensitivity Issue	ANO Total Core Melt Frequency
Base Case	5×10^{-5}
Reactor Coolant Pump Seal Leakage Induced by Loss of Seal Cooling (70 gpm maximum leak case)	1.6×10^{-4}
Emergency Core Cooling Success Criteria for LOCAS $1.2" < D \leq 1.66"$	4.1×10^{-5}
Electromatic Relief Valve/ Block Valve Status	5×10^{-5}
Battery Depletion	5.3×10^{-5}
Recovery Model (No recovery credit within 5 minutes case)	4.8×10^{-5}
Anticipated Transients Without Scram	7.7×10^{-5}
Grit in Containment Sump	7×10^{-4}
Core Melt/System Interactions	5×10^{-5}
Reactor Coolant Pump Seal Rupture Initiating Event Frequency	9.7×10^{-5}

significant wear before being replaced at ANO. If one assumes that the experiment is not applicable and that the seal leaks quoted in References 20 and 22 occur, the ANO-1 core melt frequency is affected as described below.

Reference 20 states that each RCP would leak 5 gpm at 30 minutes and 10 gpm at 60 minutes. After 60 minutes the leakage is expected to stabilize at approximately 10 gpm. Let us suppose that ANO experiences a reactor trip in which the emergency feedwater system is successful in removing decay heat. However, let us also suppose that failures in support systems occur (diesel generators, batteries, service water), which are common to the high pressure injection, reactor building cooling, and reactor building spray systems, and cause these three front line systems to be unavailable. Failure of these support systems will also cause failure of the reactor coolant pump seal cooling. Upon loss of seal cooling the seals will begin to leak, causing the RCS to lose inventory. Since the HPIS is unavailable, the RCS will continue to lose inventory leading to core uncovery and eventual core melt. Reference 17 quotes that ~38000 gallons are present above the core. Assuming a 40 gpm RCS leak rate (ANO has four RCPs) yields a core uncovery time of approximately 16 hours. This should be ample time to perform the recovery actions necessary to restore the HPIS and prevent a core melt. The ANO core melt frequency is, therefore, not significantly affected if one assumes the leak rate stated in Reference 20.

Reference 22 estimates a conservative upper bound leak rate of 70 gpm per pump. Given a scenario similar as to that outlined in the previous paragraph, except for the assumption of a linearly increasing leak rate to

a maximum of 70 gpm, yields a core uncovery time of 5-6 hours (see Appendix D.2 for calculation). Since the core uncovery time is significantly reduced for this scenario, much less time is available to perform HPIS recovery actions. Because of this, the frequency of several accident sequences increase substantially (i.e., become > 10^{-6}/Ryr) and impact the ANO core melt frequency; raising the total frequency from $5x10^{-5}$ to $1.6x10^{-4}$/Ryr. These sequences and their assessed frequencies are listed below:

T(LOP)D_1YC (Figure 5-10, sequence 5) $5.8x10^{-5}$
T(LOSW) (Figure 5-11, sequence 1) $2.6x10^{-5}$
T(A3)D_1YC (Figure 5-10, sequence 5) $1.3x10^{-5}$
T(D02)D_1YC (Figure 5-10, sequence 5) $5.4x10^{-6}$
T(D01)D_1YC (Figure 5-10, sequence 5) $5.1x10^{-6}$

The dominant cut sets for these sequences are:

Cut Set	Cut Set Frequency
T(LOP)*LF-AC-DG1*LF-AC-DG2	$4.2x10^{-5}$ (.12)
T(LOP)*LF-AC-DG1*LF-SWS-S1	$2.7x10^{-6}$ (.05)
T(LOP)*LF-AC-DG2*LF-SWS-S2	$2.7x10^{-6}$ (.05)
T(LOP)*LF-AC-DG1*LF-SWS-S63	$1.8x10^{-6}$ (.02)
T(LOP)*LF-AC-DG2*LF-SWS-S62	$1.8x10^{-6}$ (.02)
T(LOP)*LF-AC-DG2*LF-DC-D07	$1.4x10^{-6}$ (.12)
T(LOP)*LF-AC-DG1*LF-DC-D06	$1.4x10^{-6}$ (.12)
T(LOSW)	$2.6x10^{-5}$ (.01)
T(A3)*LF-AC-A4	$8.4x10^{-6}$ (1)
T(A3)*LF-DC-D02	$3.5x10^{-6}$ (1)
T(A3)*LF-SWS-S1	$1.4x10^{-6}$ (.05)
T(A3)*LOSP*LF-AC-DG2	$1.4x10^{-7}$ (.12)
T(D02)*LF-AC-A3	$4.3x10^{-6}$ (1)
T(D02)*LF-SWS-S2	$7.2x10^{-7}$ (.05)
T(D02)*LOSP*LF-AC-DG1	$7.2x10^{-8}$ (.12)
T(D01)*LF-AC-A4	$4.3x10^{-6}$ (1)
T(D01)*LF-SWS-S1	$7.2x10^{-7}$ (.05)
T(D01)*LOSP*LF-AC-DG2	$7.2x10^{-7}$ (.12)

Term Descriptions

T(LOP) - loss of offsite power; F(T(LOP)) = .32/Ryr.

LF-AC-DG1 - local fault of diesel generator 1 (fails HPIS A and B pump, RBCS A and B fan, RBSI A pump and 1/2 RCP seal cooling); P(LF-AC-DG1) = .033.

LF-AC-DG2 - local fault of diesel generator 2 (fails HPIS C pump, RBCS C and D fan, RBSI B pump, and 1/2 RCP seal cooling); P(LF-AC-DG2) = .033.

LF-SWS-S1 - local faults in SWS pipe segment S1 (fails cooling to HPIS C pump, RBCS C and D heat exchanger, RBSI B pump and 1/2 RCP seal cooling); P(LF-SWS-S1) = .005.

LF-SWS-S2 - local faults in SWS pipe segment S2 (fails cooling to HPIS A and B pump, RBCS A and B heat exchanger, RBSI A pump and 1/2 RCP seal cooling); P(LF-SWS-S63) = .005.

LF-SWS-S63 - local faults of SWS pipe segment S63 (fails cooling to diesel generator 2 causing failure of HPIS C pump, RBCS C and D fan, RBSI B pump, and 1/2 RCP seal cooling); P(LF-SWS-S63) = .0085.

LF-SWS-S62 - local faults of SWS pipe segment S62 (fails cooling to diesel generator 1 causing failure of HPIS A and B pump, RBCS A and B fan, RBSI A pump and 1/2 RCP seal cooling); P(LF-SWS-S62) = .0085.

LF-DC-D07 - local fault of battery D07 (fails HPIS A and B pump, RBCS A and B fan, RBSI A pump and 1/2 RCP seal cooling); P(LF-DC-D07) = .0011.

LF-DC-D06 - local fault of battery D06 (fails HPIS C, RBCS C and D fan, RBSI B pump and 1/2 RCP seal cooling) P(LF-DC-D06) = .0011.

T(LOSW) - loss of service water system (fails all HPIS pumps, RBSI pumps, RBCS fans, RCP seal cooling) $F(T(LOSW)) = 2.6 \times 10^{-3}/Ryr$.

T(A3) - failure of ES bus A3 (4160VAC) (fails HPIS pumps A and B, RBCS fans A and B, RBSI pump A and 1/2 RCP seal cooling); $F(T(A3)) = 3.5 \times 10^{-2}/Ryr$.

LF-AC-A4 - local fault of ES bus A4 (4160VAC) (fails HPIS pump C, RBCS fans C and D, RBSI pump B and 1/2 RCP seal cooling); P(LF-AC-A4) = 2.4×10^{-4}.

LF-DC-D02 - local fault of ES bus D02 (125VDC) (fails HPIS pump C, RBCS fans C and D, RBSI pump B and 1/2 RCP seal cooling); P(LF-DC-D02) = 1×10^{-4}.

LOSP - loss of offsite power following reactor trip; P(LOSP) = .001.

T(D02) - failure of ES bus D02 (125VDC) (fails HPIS pump C, RBCS fans C and D, RBSI pump B and 1/2 RCP seal cooling); F(T(D02)) = 1.8×10^{-2}/Ryr.

LF-AC-A3 - local fault of ES bus A3 (4160VAC) (fails HPIS pump A and B, RBCS fans A and B, RBSI pump A and 1/2 RCP seal cooling); P(LF-AC-A3) = 2.4×10^{-4}.

T(D01) - failure of ES bus D01 A3 (125VDC) (fails HPIS pumps A and B, RBCS fans A and B, RBSI pump A, and 1/2 RCP seal cooling); F(T(D01)) = 1.8×10^{-2}/Ryr.

As can be seen, many cut sets have a high likelihood of recovery. Cut sets with the .12 factor involve the non-recovery of off-site power. Cut sets with factors less than 10^{-1} generally involve failure of the operator to perform recovery actions such as opening valves or closing circuit breakers.

Emergency Core Cooling Success Criteria for LOCAs 1.2" < D < .66"

Table 4-1 indicates that in response to a LOCA within the range 1.2"<D≤1.66," the following combinations of safety systems are required to successfully cool the core during the injection phase:

1/2 emergency feedwater system (EFS) pumps

and

1/3 high pressure injection system (HPIS) pumps

OR

2/3 HPIS and

1/2 pressurizer safety relief valves.

This success criteria was obtained from discussions with B&W (Reference 6). The requirement for 2/3 HPIS pumps, when the EFS is unavailable, had an important influence on the frequency calculated for the T(D01)LQ-D_3 and T(A3)LQ-D_3 dominant accident sequences (see discussion of these sequences in Section 8.1.1). This section investigates the affect that a less stringent HPIS success criteria, given the EFS is unavailable, would have on the frequency calculated for these two sequences.

One of three HPIS pumps rather than 2/3 pumps, without the aid of the EFS, may adequately cool the core for LOCAs "$1.2<D\leq1.66$" for the following reasons:

1. B&W stated that for breaks in this range, 2/3 HPIS pumps were required to prevent core damage. They would not specify how much core damage occurred with only one HPIS pump. While we do not disagree that some core damage could occur, we question whether a core melt would ensue. Referring to Table 4-1, it can be seen that the core cooling success criteria for breaks size ranges just larger and smaller than the range discussed, do not require the EFS and only need one HPI pump. This implies to us that one HPI pump may be adequate to prevent core melt for the "$1.2<D\leq1.66$" range also.

2. The B&W analysis was most likely based upon the flow characteristics of a typical B&W HPI pump, i.e, pump flow of 200 gpm at 2600 psid. ANO HPI pump test data suggest that at least two of the pumps would have a higher flow rate at 2600 psi.

Sequence T(D01)LQ-D_3 was requantified assuming that 1/3 HPIS would cool the core. The frequency of this sequence was reduced by over an order of magnitude (i.e., $3x10^{-7}$) before application of the recovery model described in Chapter 7. Application of the recovery model would most likely lower the sequence frequency below $1x10^{-7}$. The frequency of T(A3)LQ-D_3 would also be expected to drop below $1x10^{-7}$ since it is very similar in nature to T(D01)LQ-D_3. Lowering the frequencies of these sequences reduces the ANO core melt frequency from $5x10^{-5}$ to $4.1x10^{-5}$/Ryr.

Electromatic Relief Valve/Block Valve Status

As stated in Chapter 3, the analysis presented in this report was based on the assumption that the block value for the pressurizer electromatic relief valve (ERV) was closed. The block valve was closed during the time the analysis was performed due to ERV leakage. Discussions with ANO personnel indicate that they intend to reopen the block valve following repair of the ERV. This section will analyze the affect that reopening the block valve will have on the accident sequences identified in this report.

The operability of the ERV and its block valve could potentially impact the accident sequences in three general areas: (1) overpressure transients, (2) feed

and bleed core cooling, and (3) LOCA initiating events. Each of these areas are discussed in turn below.

1. If the RCS experiences an overpressure transient, the peak RCS pressure can be reduced if the ERV automatically opens as designed at 2450 psig. With the block valve closed, the ERV cannot mitigate overpressure transients unless the operator opens the block prior to ERV demand. Since overpressure transients are, in general, fairly rapid, it is unlikely that the operator could open the block valve in time. The most significant overpressure transient analyzed in this study occurs following an ATWS. Reference 1 states that a peak pressure of 4000/4900 psi may occur if the ERV does/does not open to relieve RCS pressure. Since both pressures are excessive, the mitigative capability of the ERV following an ATWS event is questionable. (ATWS is a sensitivity issue which will be discussed later.)

2. If all methods of achieving decay heat removal via the steam generators are unavailable following a transient, the ANO-1 emergency procedures instruct the operator to establish feed and bleed core cooling by opening the ERV and its block valve (if closed) and actuating high pressure injection. Information received from B&W indicates that feed and bleed does not require the operator to open the ERV as long as the flow from at least one HPI is allowed to boil off through a pressurizer code safety relief valve.[3] The status of the ERV and its block valve, therefore,

does not affect the probability of failing to establish feed and bleed core cooling.

3. With the block valve in the open position, a failed open ERV would create a small LOCA. An ERV could fail open spuriously or fail to reclose after opening in response to an overpressure transient. Neither of these ERV failure modes significantly impact the results of this study.

   Spurious ERV openings occur with a frequency .02/Ryr (refer to Table 4-4, entry 8). Assuming the operator has a .1 probability of failing to recover, by closing the block valve, yields a small LOCA initiating event frequency of 2×10^{-3}/Ryr. A stuck open ERV would be classified a B(1.2) LOCA. Since the B(1.2) LOCA frequency utilized in this report is 2×10^{-2}, an additional contribution of 2×10^{-3} is not significant.

Following the TMI accident the ERV open setpoint was raised to 2450 psig. Because of this change it can be reasonably assured that if the ERV is demanded open during an overpressure transient, so will the two code safety relief valves (2500 psig setpoint). This analysis has explicitly considered accident sequences in which one of the safety valves fails to close following a demand. Accident sequences involving failure of an ERV to lose would be bounded by the safety valve sequences already considered.

In summary, the status of the ERV block valve does not significantly affect the overall frequency of core melt predicted for ANO-1.

Battery Depletion

The fault trees developed for ANO-1 do not model DC power failure caused by station battery depletion following interruption or failure of battery charging subsystems. This is potentially nonconservative since for certain accident sequences, battery charging subsystems are interrupted with a moderate probability (i.e., station blackout). Battery depletion was not modeled because ANO-1 battery discharge test data suggest that the batteries will provide an adequate output to safely shutdown the plant for up to 24 hours. The results have proven adequacy for at least eight hours with no load shedding. However, if the proper load shedding outlined in the emergency procedures is performed, the batteries are predicted to last for nearly 24 hours. The probability of not recovering a battery charging subsystem within 24 hours is expected to be small and, thus, the effort required to properly model battery depletion was not felt to justified. Nevertheless, this section will investigate the affects of battery depletion if it assumed that local shedding is not performed and the batteries fail at 8 hours.

ANO-1 has three battery charging subsystems. Each subsystem is capable of being powered by either engineered safeguards 480V AC load division, if required, via control room switches. Each battery has a dedicated battery charger with the third charger capable of servicing either battery. We will, therefore, assume that if AC power is available, the operator will perform the proper switching within the 8-hour time frame, to insure that the battery(s) involved in the shutdown do not deplete. The only case we will investigate then, will be station blackout, i.e., no offsite or onsite AC power available.

If a station blackout occurs, critical DC loads are not shed, and offsite or onsite AC power is not restored within approximately eight hours, the two station batteries would deplete causing a total loss of DC power. DC power failure will cause core cooling to be interrupted. The RCS inventory will begin to boil off resulting in core uncovery and an eventual core melt. (We assume a core melt would ensue within a few hours following DC power failure.) The following are the dominant cut sets which result in this scenario:

Cut Set	Cut Set Frequency
T(LOP)*LF-AC-DG1*LF-AC-DG2	2.5×10^{-6} (.007)
T(LOP)*LF-AC-DG1*LF-DC-D06	1.4×10^{-7} (.012)
T(LOP)*LF-AC-DG2*LF-DC-D07	1.4×10^{-7} (.012)

Term Descriptions

T(LOP) - loss of offsite power; F(T(LOP)) = .32/Ryr.

LF-AC-DG1 - local fault of diesel generator 1; P(LF-AC-DG1) = .033.

LF-AC-DG2 - local fault of diesel generator 2; P(LF-AC-DG2) = .033.

LF-AC-D06 - local fault of battery D06 (required for successful operation of DG2); P(LF-DC-D06) = .0011.

LF-AC-D07 - local fault of battery D07 (required for successful operation of DG1); P(LF-DC-D07) = .0011.

The recovery factors were derived via:

$.007 = .02\ (.6)^2$,
$.012 = .02\ (.6)$,

where

.02 = the probability of not recovering offsite power within 10 hours (Reference 18).

.6 = the probability of not recovering a diesel generator within 10 hours (Reference 18).

Summing these cut sets yields 2.8×10^{-6}. They would be applicable to the already dominant sequence $T(LOP)LD_1YC$. The sequence frequency would be increased to 1.3×10^{-5} and the overall ANO core melt frequency increased from 5×10^{-5} to 5.3×10^{-5}/Ryr.

Recovery Model

Operatory recovery of the system and component failures depicted on the event trees and fault trees was described in Section 7.1.5. The primary recovery model utilized was presented in Table 7.1. The nonrecovery probabilities listed in the table should be considered to be very rough since, as described in 7.1.5, they were based upon engineering judgment and not real data. Several individuals from Arkansas Power and Light (AP&L) feel the model is not realistic in the following areas:

1. The model assumes that no recovery is possible within the first five minutes following an accident for actions which can be performed in the control room. AP&L operating experience supports the fact that many plant failures are recovered within a few minutes.

2. The model assumes that all control room recovery actions beyond 60 minutes and all remote recovery actions beyond 70 minutes have a constant .01 nonrecovery probability. AP&L feels that this

probability is too high for certain situations in which times greater than 70 minutes may be available to perform the recovery actions.

3. The model is very simplistic and does not allow for situation specific performance shaping factors which could increase or decrease the nonrecovery probabilities listed in Table 7.1. AP&L and others feel a more detailed model should be developed which takes into account situation specific performance shaping factors.

These three areas will be addressed in turn.

1. Not giving credit for recovery in the control room for the first five minutes affects the probability of pump failure in two systems which appear in the dominant accident sequences. Both emergency feedwater system pumps draw from the condensate storage tank via a common set of suction valves. If these valves fail closed, the pumps are predicted to fail in less than five minutes unless the operator stops the pumps, realigns their suction to the service water system and restarts the pumps. (Once the operator stops the pumps, ~ 20 minutes are available to perform the other recovery actions.)

   Similarly, the high pressure pumps draw from the borated water storage tank via a parallel set of MOVs. If these MOVs do not open, the pumps are predicted to fail in less than five minutes unless the operator stops the pumps, opens the MOVs locally, and restarts the pumps.

(Once the operator stops the pumps, 40 minutes are available to perform the other recovery actions.)

If it is assumed the operator has a 75 percent chance of stopping the pumps in these systems before failure, some of the cut sets in the dominant accident sequences would have a non-recovery probability of .25 rather than 1.0. The cuts sets affected are those involving events LPI1407A-VCC-LF, LPI1408B-VCC-LF, and LF-EFWE22. The frequencies of the following dominant sequences would be affected:

$B(1.2)D_1C$ - decrease 24%,
$T(D01)LD_1C$ - decrease 25%,
$T(A3)LQ\text{-}D_3$ - decrease 5%,
$T(A3)LD_1C$ - decrease 70%.

Lowering the frequency of these sequences, in turn lowers the ANO core melt frequency from $5x10^{-5}$ to $4.8x10^{-5}$.

2. Some of the faults modeled on the fault trees would have times greater than 70 minutes to perform recovery actions (e.g., some room cooling failures, low pressure and spray pump lube oil cooling failures, etc.). While knowledgeable AP&L personnel are confident that for certain situations at least 70 minutes would be available, they are not able to predict with accuracy how much additional time beyond 70 minutes would be available. In order to predict the additional time beyond 70 minutes, detailed engineering calculations and/or tests would have to be performed. This type of work would be costly and

is not justified when one considers the limited scope and approximate nature of this IREP study.

3. The ANO analysis team, with the aid of AP&L personnel, created an alternate recovery model which took into account some performance shaping factors (PSFs). These PSFs were used to develop and estimate a "best guess" assessment time, i.e., the average time required for the operator to determine the appropriate recovery action to be performed. This exercise yielded four different assessment times; the shortest time (2 minutes) was characterized by a few control room alarms which gave a direct indication of the failure, and the longest time (8 minutes), was characterized by several control room alarms which gave an indirect indication of the failure. The assessment time was then added to an estimated fix time (the estimated time required to actually perform the recovery action, given a correct assessment has been made) to yield an estimated recovery time. Two fix times were chosen; simple control room recovery actions (e.g., flip a switch, push a button) were assigned a time of one minute and simple recovery actions outside the control room (e.g., turn a hand wheel, push a button) were assigned a time of 10 minutes. The time estimates were assumed to be medians, and a log normal probability distribution was assumed with an error factor of 4 for each time estimate to take into account what we felt was the uncertainty in our estimates. These distributions were then integrated to yield plots of the probability of

nonrecovery as a function of time (see Figure 8-2). Four of these plots apply to control room operations and four apply to operations outside the control room. Also plotted in Figure 8-2 is the recovery model utilized in this study, i.e., the "staircase" functions.

Via comparison of the recovery model used in this study and the alternate recovery model, the following observations can be made:

a. The "control room" recovery model utilized in this study is roughly similar to the worst case "alternate control room" recovery model for the first 60 minutes.

b. The "outside control room" recovery model utilized in this study is roughly similar to the best case "alternate outside control room" recovery model for the first 70 minutes.

Since the alternate model shows similarities to the model utilized in this study, and since both models rely solely upon engineering judgment, we did not reanalyze the dominant sequences using the alternate model.

Anticipated Transients Without Scram (ATWS)

The discussion of the T(FIA)KD_1 sequence in Section 8.1.1 indicated that following an ATWS event, a peak RCS pressure of 4900 psi may occur. It was assessed in that discussion that this pressure spike would not directly cause core melt based on analysis presented in Reference 12. Since ATWS sequences are currently a NRC unresolved safety issue for B&W plants, primarily due to the peak pressure question, we will assume in this section that the pressure spike will directly cause core melt.

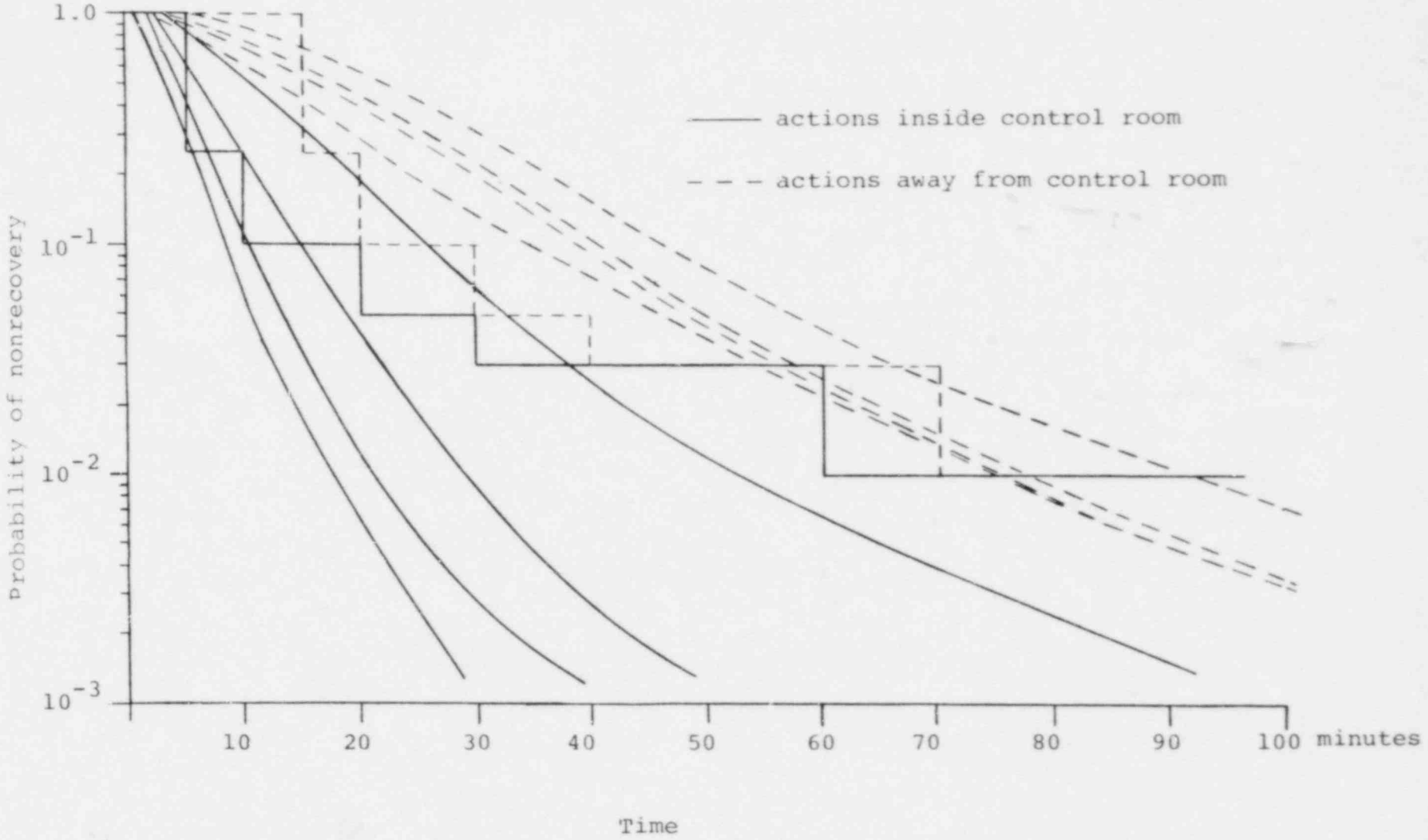


Figure 8-2. Probabilities of Operator Nonrecovery as a Function of Time

The frequency of $T(FIA)KD_1$ given in Section 8.1.1 is $3x10^{-6}$. Referring to that section it can be seen that this frequency is dominated by four cut sets. Each cut set involves failure of the operator following the peak pressure to prevent a core melt via manual actuation of the high pressure injection system (HPIS). If one assumes that the peak pressure causes core melt, actuation of the HPIS is moot. The dominant ANO-1 ATWS sequence would, therefore, be labeled T(FIA)K and would have a frequency estimate of $3x10^{-5}$/Ryr. Increasing the frequency of ATWS core melts in turn increases the ANO core melt frequency from $5x10^{-5}$ to $7.7x10^{-5}$/Ryr.

Grit in Containment Sump

The fault trees and event trees developed for ANO-1 do not model failure or degradation of safety system pumps caused by a contaminated water supply. In response to an LOCA, safety system pumps draw from two water sources. During the injection phase they draw from a water storage tank. When this tank empties the pumps are realigned to draw from the containment sump. The water in the tank is expected to be very clean; pump operation would, therefore, not be affected. The water in the sump water, however, would be expected to be contaminated with "grit" present in the containment which may affect pump operation.

Three types of pumps draw from the sump at ANO: building spray, low pressure, and high pressure. Discussions with B&W pump experts indicate that all of these pumps contain wear rings which would degrade when exposed to gritty water(6). They also stated that a pump may sieze if the wear rings contact each other. Though

B&W does not expect the pumps to sieze when pumping nonmetallic gritty water, they are still investigating the affect that metallic chips have on pump operation. Since the wear ring gap on the high pressure pumps (2.5 mil) are much smaller than on the low pressure and spray pumps (30 mil), B&W feels that the high pressure pumps would be the most adversely affected by metallic chips.

It is not unreasonable to assume that metallic chips would be present in the sump water following a LOCA. The containment would be flooded and any metallic grit deposited from construction or maintenance could be diverted to the sump. In response to LOCAs with a diameter $1.2" < D \leq 4"$, the high pressure pumps are aligned during the recirculation phase to draw from the sump. If one assumes the high pressure pumps fail due to metallic grit, core cooling will also fail followed by a core melt. This study has estimated the frequency of $1.2" < D \leq 4"$ LOCAs to be $\sim 7 \times 10^{-4}$/Ryr. If the high pressure pumps fail with a 100 percent probability, the core melt frequency for ANO-1 would be increased from 5×10^{-5} to $\sim 7 \times 10^{-4}$/Ryr.

Core Melt/System Interactions

The ANO-1 event trees imply that the reactor building spray system and reactor building fan cooler system may be utilized to scrub radioactivity and protect the containment from overpressure during a core melt accident. The fault tree analysis of these systems also assumes that the system reliability will not be degraded due to the adverse environment within containment following a core melt. This assumption is potentially nonconservative.

Rough hand calculations based on data obtained from recent core meltdown computer code and experimental research performed at Sandia suggest that PWR fan cooler systems may be significantly degraded or fail when operating in a post-core melt environment. The research indicates that within the first 24 hours following the initiation of a core melt accident, large quantities (~one ton) of 2-4 micron aerosols are generated (personal communication from R. K. Cole, Sandia). These aerosols have a very low thermal conductivity and plate out very well on cooled surfaces. If the aerosols plate out on the ANO fan cooling system coils, their heat removal capability may be degraded to the point of uselessness. It is also estimated that in a post-core melt environment, the cooler design temperature and radiation limits would be exceeded.

Results from the Sandia experiments and discussions with pump experts at Babcock and Wilcox suggest that spray recirculation system pumps may fail during a core melt accident. The experiments 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 containment sump would be contaminated with these metal chips. Pump experts at Babcock and Wilcox feel that containment spray pumps may sieze if the sump water contains small metal chips.

If one assumes the fan coolers and spray recirculation pumps fail due to core melt/system interactions, the ANO-1 risk should not be greatly impacted, however.

The core meltdown analysis presented in Section 8.1.2 implies there is nearly a direct correlation between core melt frequency and expected ANO-1 risk, i.e., every core melt sequence has a .2 to .5 probability of being placed in a high risk release category (category 2).

Reactor Coolant Pump (RCP) Seal Rupture Initiating Event Frequency

The frequency of B(1.2) LOCAs (.02/Ryr) was dominated by RCP seal ruptures (refer to discussion in Section 4.2). This frequency estimate was based upon generic industry data.[9] On May 10, 1980, ANO-1 experienced one of the most severe RCP seal rupture events that have occurred in the nuclear industry. The peak flow rate was estimated at 350 gpm and the high pressure injection was actuated by the operators in accordance with the ANO LOCA emergency procedure. Before termination of the event, 60,000 gallons of RCS water accumulated in the containment. This section will recalculate the frequency of core melt accidents initiated by B(1.2) LOCAs using ANO specific, rather than generic, RCP rupture date.

Before presenting the results of the recalculation, it should be noted that generic RCP seal rupture data was used because a statistical significance test indicated that generic and ANO specific data were not inconsistent (refer to Section 7.1.3). The recalculation presented below is, therefore, only meaningful if for some reason ANO should in the future become atypical via an occurrence of another RCP rupture event.

ANO-1 has operated for approximately seven years with the occurrence of one major (i.e., >50 gpm) LOCA

due to a RCP seal rupture. The B(1.2) LOCA frequency based on this data is .14/Ryr. The frequency estimates for the $B(1.2)D_1$ and $B(1.2)D_1C$ dominant accident sequences are increased to $2x10^{-5}$ and $3.5x10^{-5}$, respectively, via use of this datum. In addition, some sequences which were previously nondominant would now become important. These are listed below and the dominant cut sets given in Appendix C:

$$B(1.2)D_1YC = 5.1x10^{-6}$$
$$B(1.2)LH_1 = 6x10^{-6}.$$

Increasing the frequency of these four sequences in turn raises the ANO core melt frequency from $5x10^{-5}$ to $9.7x10^{-5}$/Ryr.

8.5. Limitations of the IREP Methodology and Analysis and Future Uses of the Models

The quantitative results of this IREP study must be viewed and used with a thorough understanding of the limitations of the methodology used. As previously identified, this is principally a reliability study. While insights regarding risk-dominant accident sequences can be obtained from the analysis, a detailed risk analysis was not performed, nor was it intended. The analysis leading to the grouping of accident sequences into release categories relied heavily on previous studies performed on similar plants without extensive plant-specific analyses. Recognizing the inherent uncertainties in this type of categorization, the information generated was not used as an input to a calculation of consequence distribution. External events such as earthquakes, fires, floods, and other influences from without were not considered. Thus, the quantitative results must be regarded as being incomplete from a risk perspective.

In utilizing the results of this study, the following limitations should be recognized:

1. The generic data based used in the quantification analyses was very similar to the WASH1400 data base, with some modifications resulting from limited analyses of LER submittals. Plant-specific data was utilized when the analyst found it different from the generic base. However, the detailed comprehensive examination of plant logs necessary to fully evaluate in-plant data was not performed.

2. Human performance was modeled using the techniques described in NUREG/CR-1278.[15] However, the systematic bias in human response (either positive or negative) that may result because of morale or management practices were not included. In addition, human acts of commission were, in general, not included in the analysis.

3. An attempt was made to couple the root cause of the initiating event with system faults in analyzing accident sequences. The technique used is believed to be reasonably efficient to identify single failures which may initiate a transient and degrade the performance of one or more safety systems. However, multiple fault scenarios of this type may have been omitted.

4. Coupling of faults associated with design, fabrication, or environmental conditions, was not treated explicitly.

There were also several assumptions made throughout the analysis regarding the depth of analysis which

could influence the results. In many cases these assumptions were made based on a judgement that further modeling was not important probabilistically. The depth of the analysis in many ways defines the level of interactions or dependencies considered and while we believe the assumptions made are valid, the possibility exists that additional dependencies might be identified with further analysis. Examples of the type of assumptions made include: (1) including only those single passive failures which can fail an entire system, and (2) ignoring misposition faults for valves which automatically are commanded to the proper position upon ESF actuation and for valves which have position indicated in the control room and are monitored each shift using a checkoff procedure.

The incompleteness and subjectivity associated with the aforementioned topics does not invalidate the analysis performed. The important product of this project is the framework of engineering logic generated in constructing the models, not the precise numbers resulting from the mathematical manipulations of these models.

The patterns, ranges and relative behaviors which are obtained can be used to develop insights into the design and operation of a plant which can only be _ined from an integrated consistent approach such as this IREP analysis. These insights are applicable to utility and regulatory decision making, although they should not be the sole basis for such decisions. By comparative evaluations, those features of the plant which are predicted to have a more significant influence on risk can be identified and owner and regulatory efforts can be

focussed on them to determine if they are acceptable. Similarly, regulatory efforts addressed to items having an insignificant influence on predicted risk should also be evaluated. The ranking of risk dominant accident sequences provides a framework for future value-impact analyses on potential plant modifications.

Application of Results

The generic views regarding the usefulness of the IREP analyses expressed above suggest several concrete applications that can be made. They are presented below in the form of suggestions to plant owners for applications of the results. In many cases, the models may have to be perturbed somewhat to achieve the various goals. However, we have attempted to construct them in such a manner as to minimize the difficulty associated with such use. It is desirable for these models to be maintained in a current status and used as tools in operations management. Specific suggestions are listed below:

1. Operator training and simulator design

   The IREP study generated a catalog of severe accident sequences, with rough assessments of the likelihood, severity and principal root causes of each. Some of these could be included in operator training and simulator design. This information can also be used as a starting point for further studies intended to assess the similarity of the symptom profile among accidents requiring different operator response and to survey the hazards associated with misdiagnosis or less-than-optimum recovery actions. A natural followup is an assessment of the adequacy of instrumentation and status monitoring equipment.

2. Emergency planning

The catalog of accident sequences and the likelihood estimates emerging from IREP can be used to train emergency response personnel in what to expect. IREP results can also serve as a basis to improve the set of symptoms to be used as trigger points for the declaration of site or general emergencies, and they can be used in developing guides on the diagnosis and prognosis of accidents as they develop.

3. Adequacy of procedures

It is common in studies such as IRLP to discover a few instances in which emergency procedures or maintenance procedures should be improved and which are of prime importance to the accident susceptibility of the plant. The results herein should be studied to determine if this is the case here. Beyond these lessons, IREP models can be used to measure the importance of individual procedures to safety and to explore the risk associated with errors in following procedures.

4. Adequacy of limiting conditions of operation

An IREP study provides the tools with which to optimize allowable outage times and surveillance intervals. The IREP models can also be used in evaluating requests from utilities to continue power generation when equipment is out of service beyond their specified allowable outage times.

5. Systems integration reviews

IREP is designed to model explicit functional and hardware dependencies among systems. It

is not uncommon to discover that an auxiliary system is a weak link with respect to reliability in such a manner that it governs plant risk. Hard-wired systems interactions, human behavior that can couple the unavailabilty of several safety systems, and the importance of auxiliary systems to safety have emerged in IREP results. Such findings are not complete or precise; nonetheless, they represent a vast improvement on safety analyses done to date.

6. Significance of component reliability

   The IREP models can be used to develop quantitative measures of importance to safety for the reliability of components, trains, whole systems, and classes of accident sequences. These models enable the use of cost-benefit analyses on reliability improvements for components, and the more discriminating use of the more expensive qualification of in-service inspection techniques.

7. System reliability

   Estimates of system reliability are produced in an IREP study. Quantitative measures of the importance of system components can be calculated from the IREP models and the more likely failure modes which are believed to dominate the unavailability of these systems are identified. With this information, one can assess the possibility that a failed system could be repaired before its failure reaches a point of no return under accident conditions. Operators can be trained in fault diagnosis and in "quick fixes." The adequacy of diagnostic

instrumentation and status monitoring can be assessed. Surveillance practices can be altered to improve the availability of particularly critical systems.

8. Accident sequences

In addition to identifying accident sequences and estimating their frequency, IREP models can also serve as a test-bed with which to explore the effects of changes in design or operations practices. Possible improvements may be obvious in light of the results. In other cases, the effectiveness of hypothetical improvements can be assessed (within the limits of the completeness of the models). A particularly valuable use of these models lies in the evaluation of attendant risks associated with changes; i.e., will a fix for one safety problem make different accident sequences more likely? IREP provides a tool that can be used to address such questions.

9. Evaluation of operating occurrences

The IREP models and results can be used in the evaluation of whether a fault occurring in plant operation or testing was a precursor of a more serious event, and to evaluate its importance. One can explore each of the classes of severe accident sequences for the role that might have been played by the actual event. In addition, patterns of licensee events or trends can be assessed for risk significance with the IREP models.

10. Validation of IREP analyses

The occurrence of faults or errors in the operation or testing of the plant can be used to update, validate, or improve the completeness or accuracy of the IREP models and the projected failure frequencies. Doing so has the dual advantage of improving the IREP model for its many other uses as well as illuminating the safety significance of the operating experience.

11. Design errors and generic safety issues

There are several classes of safety problems in reactor plants that IREP studies do not analyze. Among these are susceptibility to fires, floods, sabotage, earthquakes, design or installation errors that are not revealed by the explicitly known, hard-wired functional dependencies among systems, and effects assumed to be negligible in the IREP study, such as the role of snubber failures. However, the models generated in IREP can be used to put such concerns into perspective once the concern has been explicitly postulated. For example, one can use IREP to assess which accident sequences might be affected by the postulated safety issue and estimate at what level of severity the deficiency -- if any -- might emerge from the background of minor contributors to risk into one of the dominant concerns. Thus, IREP can be immensely useful even in contexts in which its predictive power is poor.

It should be noted that none of the uses suggested above depends upon the bottom line predictions of risk.

They all depend upon the more trustworthy comparative measures of importance and upon the catalog of accident sequences to which the subject plant is susceptible.

Some of the applications are sensitive to the limitations of the study, particularly in completeness and quantitative accuracy. Nonetheless, the applications can be tailored to the known limitations and the models generated can provide a coherent framework to address the "what if" questions concerning its accuracy in these applications.

The suggested applications of the models in this report do not require a precise analysis of the phenomenology of reactor accidents. Thermal hydraulics, containment challenge analyses, and the like need only be good enough to develop the broad outlines -- the "cliffs and valleys" -- in the accident processes, although there are rare occasions when uncertainties in the modeling of accident processes can make large differences in the course of consequences of reactor accidents.

In general, formal, plant-specific consequence analysis is unnecessary for these applications. It is useful to be able to identify accident sequences with categories of outcome severity, and the applications to emergency planning require some information on offsite consequences. However, the accuracy warranted can be met by interpolating the accident sequences among those in the published risk assessments that have included formal consequences analysis.

It is hoped that studies similar to this IREP analysis will become a common language, shared by the NRC and the licensees, to put safety issues in context. The use of IREP as a tool for safety analysis and in

operations management should enable many loopholes in the assurance of reactor safety to be identified and closed, and at the same time improve the cost-effectiveness and risk-relevance of NRC regulatory initiatives.

REFERENCES

1. U. S. Nuclear Regulatory Commission, Anticipated Transients without Scram for Light Water Reactors, Unresolved Safety Issue Program, Office of Nuclear Reactor Regulation, NUREG/CR-0460, March 1980.

2. G. J. Kolb, S. W. Hatch, P. Cybulskis, and R. O. Wooton, Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant, NUREG/CR-1659, SAND80-1897, Sandia National Laboratories, May 1981.

3. Letter from W. Jones, B&W, to Dennis Taylor, AP&L, Subject, IREP Support for ANO-1, June 15, 1981.

4. ATWS: A Reappraisal - Part III, Frequency of Anticipated Transients, prepared by Science Applications, Inc., EPRI NP-801-Project 767, Interim Report, July 1978.

5. P. W. Baranowsky, A. M. Kolaczkowski, M. A. Fedele, A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants, NUREG-0666, April 1981.

6. Letter from C. Craddock, AP&L, to G. Kolb, SNL, Subject, ANO-1 Responses to IREP Questions, February 24, 1981.

7. Arkansas Nuclear One - Unit 1, Final Safety Analysis Report, Arkansas Power and Light Company, nd, na.

8. A. A. Garcia, et al., Crystal River-3 Safety Study, NUREG/CR-2515 SAND81-7229/1, December 1981.

9. Memorandum for D. G. Eisenhut, NRC, from T. E. Murley, NRC, Subject, Reactor Coolant Pump Seal Failure, nd.

10. Letter from H. D. Hukill, Metropolitan Edison Company -- GPU, to R. W. Reid, NRC, Subject Response to NUREG-0737 Items II. K. 3.1, II. K. 3.2, and II. K. 3.7, April 6, 1981.

11. Integrated Control System Reliability Analysis, Babcock and Wilcox, BAW-1564, August 1979.

12. Analysis of B&W NSSS Response to ATWS Events, Babcock and Wilcox, BAW-1610, January 1980.

13. G. B. Varnado, W. Horton, and P. Lobner, Fault Tree Analysis Procedures for the IREP, Draft Report, SAND81-0062, Sandia National Laboratories, December 1980.

14. Letter from J. A. Murphy, NRC, to D. D. Carlson, SNL, Subject, Component Failure Rates to be Used for IREP Quantification, September 26, 1980.

15. A. D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Draft Report, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, September 1980.

16. R. B. Worrell and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, Sandia National Laboratories, November 1978.

17. Letter from F. B. Saffell Jr., EG&G Idaho, to R. E. Tiller, DOE Idaho, Subject, Preliminary Analysis of Additional PWR Station Blackout Sequences-Saff-128-81, May 21, 1981.

18. 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.

19. Memorandum from J. J. Zudans, NRC, to Z. R. Rosztoczy, NRC, Subject, St. Lucie 2; Reactor Coolant Pump Seal Hot Stand by Test, September 19, 1980.

20. Memorandum from H. A. Baily, B&W, to E. J. Domaleski, B&W, Subject, Response to 10CFR50.34(e) RCP Seal Damage (II. K. 2.16), October 7, 1981.

21. C. D. Fletcher, A Summary of PWR Loss of Offsite Power Calculations, EGG-CAAP-5283, November 1980.

22. Letter from D. B. Waters, BWR Owners Group, to D. E. Eisenhut, NRC, Subject, BWR Owners' Group Evaluation of NUREG-0737, Requirement II. K. 3.25, Received May 29, 1981.

23. Lambert, H. E. and F. M. Gilman, 1977. The IMPORTANCE Computer Code, ERDA Report UCRL-79269, Lawrence Livermore Laboratory, Livermore, California.

24. Engelbrecht-Wiggans, R., and D. R. Strip, 1981. On the Relation of Various Reliability of Measures to Each Other and to Game Theoretic Values, SAND80-2624, Sandia National Laboratories, Albuquerque, New Mexico.

25. Letter from Donald A. Rueter, Manager of Licensing, AP&L, to E. Morris Howard, Director, Office of Inspection and Enforcement, Region IV, USNRC, September 20, 1977.

26. S. W. Hatch, P. Cybulskis and R. O. Wooton, Reactor Safety Study Methodology Applications Program: Grand Gulf #1 BWR Power Plant, NUREG/CR-1659, SAND80-1897, Sandia National Laboratories, October 1981.

DISTRIBUTION:

US NRC Distribution Contractor (CDSI) (400 copies)
7300 Pearl Street
Bethesda, MD 20014
400 copies for AN, RG, XA, 1S
25 copies for NTIS

P. A. Amico
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

P. B. Bleiweis
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87182

W. T. Craddock
Arkansas Power & Light Co.
P. O. Box 551
Little Rock, AR 72203

P. Cybulskis
Battelle Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201

W. L. Ferrell
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

W. J. Galyean
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87102

A. A. Garcia
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

J. Kelly
Science Applications, Inc.
5 Palo Alto Square, Suite 200
El Camino Real at Page Mill Rd.
Palo Alto, CA 94304

D. M. Kunsman (5)
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87102

DISTRIBUTION (Cont.)

David Moses
Oak Ridge National Laboratory
P. O. Box X
Building 6025
Oak Ridge, TN 37830

J. A. Murphy (25)
Division of Risk Analysis
Office of Nuclear Regulatory Researc
US Nuclear Regulatory Commission
Washington, DC 20555

K. Neamtz (5)
Arkansas Power & Light Co.
P. O. Box 551
Little Rock, AR 72203

J. Robertson
Arkansas Power & Light Co.
P. O. Box 551
Little Rock, AR 72203

M. Stewart
EG&G Idaho, Inc.
P. O. Box 1625
Idaho Falls, ID 83415

J. Trainer
Wood-Leaver & Assoc, Inc.
545 Shoup Ave., Suite 209
Idaho Falls, ID 83402

R. O. Wooton
Battelle Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201

J. Young
Energy, Inc.
515 W. Harrison, Suite 220
Kent, Washington 98031

7223 R. R. Prairie
7223 B. J. Bell
7223 A. D. Swain III
7223 D. P. Miller
3141 L. J. Erickson (5)
3151 W. L. Garner (3)
9400 A. W. Snyder
9410 D. J. McCloskey
9412 J. W. Hickman (25)
9412 N. L. Brisbin

DISTRIBUTION (Cont.)

9412 D. D. Carlson (10)
9412 W. R. Cramond
9412 D. D. Drayer
9412 F. T. Harper
9412 S. W. Hatch
9412 A. M. Kolaczkowski
9412 G. J. Kolb (5)
9412 S. H. McAhren
9412 A. C. Payne
9412 R. G. Spulak
9412 T. A. Wheeler
9413 N. R. Ortiz
9414 G. B. Varnado
9414 A. S. Benjamin
9414 D. L. Berry
9414 D. R. Gallup
9414 G. A. Sanders
9414 D. W. Stack
9414 R. B. Worrell
9415 D. C. Aldrich
9416 L. D. Chapman
9416 B. J. Roscoe
9420 J. V. Walker
9440 D. A. Dahlgren
9450 J. A. Reuscher
8214 M. A. Pound

☆U.S. GOVERNMENT PRINTING OFFICE: 1982-0-576-021/588

Org.	Bldg.	Name	Rec'd by	Org.	Bldg.	Name	Rec'd by

Sandia National Laboratories