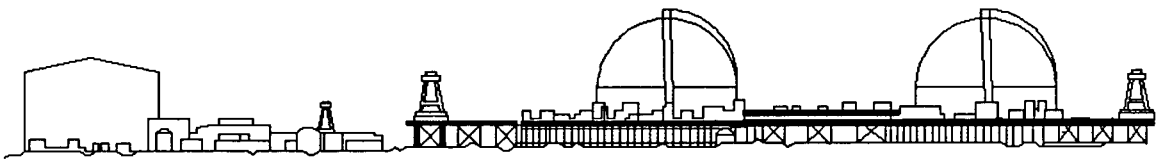
SONGS 1
ECCS SINGLE FAILURE ANALYSIS FOLLOW-UP REPORT

February 27, 1991



Southern California Edison Company

SAN ONOFRE NUCLEAR GENERATING STATION

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

The purpose of this report is to discuss the safety significance of issues resulting from the new single failure analysis (SFA) of the SONGS 1 Emergency Core Cooling System (ECCS).

Background

SONGS 1 was designed in the mid-1960s, prior to the existence of single failure analysis standards. The plant design incorporated many features which increased operational flexibility and the ability to mitigate potential accidents through the use of shared systems (e.g., swing electrical buses). While these types of systems provided the operational flexibility intended in the original design, they cause difficulty in evaluating and implementing the single failure criterion.

The single failure criterion for SONGS 1 was first discussed in 1971, as part of meeting the Interim Acceptance Criteria (IAC) for the ECCS. The AEC requested that we perform a Failure Modes and Effects Analysis (FMEA) on the ECCS using the Single Failure Criterion. In 1974 the final ECCS acceptance criteria were issued as 10CFR50, Appendix K. In response to Appendix K, we completed the first detailed single failure evaluation on the ECCS and submitted a report to the NRC on December 21, 1976. Nine plant modifications were implemented to eliminate potential single failure susceptibilities identified in the 1976 SFA.

Failure of the main steam transmitter (PT-459) in 1986 revealed that there were additional single failures in Reactor Protection System (RPS) and Engineered Safety Features (ESF) systems which had not been previously identified. As a result, a new single failure analysis was performed for the RPS and ESF in 1987. Plant modifications were implemented to correct these single failures.

Subsequent to the 1987 RPS/ESF SFA, we discovered additional single failure susceptibilities in the ECCS. By letter dated March 17, 1989, we committed to perform a new ECCS SFA. This new analysis was completed using an extensive boundary valve evaluation and FMEA methodology. It also included event specific and time dependent functions necessary to mitigate Main Steamline Breaks, Feedwater Line Breaks, Steam Generator Tube Ruptures, and Loss of Coolant Accidents (LOCAs). These events bound all accident scenarios for which ECCS operation is required. The results of this new analysis are documented in SCE Engineering Document M-41383 (SFA Report) which was submitted to the NRC on February 22, 1991. This new analysis was performed to current SFA standards. It supersedes all previous ECCS SFAs and establishes a new, current single failure design basis for SONGS 1.

II. SUMMARY OF RESULTS

The new ECCS SFA identified additional single failure susceptibilities which required evaluation and resolution. As discussed below, the majority of these susceptibilities were resolved through changes to plant procedures or design calculations, or have been shown to be acceptable by other means (e.g., meeting current regulatory criteria). There were relatively few single failure susceptibilities which required plant modifications.

Previously Reported Issues

On July 31, 1990, we submitted an interim report on the single failure issue. The interim report described eight single failure issues which required modifications. Three of the single failure issues that were described in the interim report were resolved by the "Validation of Assumptions" effort described below and they will not be discussed further in this report. These issues are: Diversion of Alternate Hot Leg Recirculation (Issue number 3 in the July 31, 1990 Report), Partial Loss of CCW due to Loss of SWC to One Heat Exchanger (Issue number 6), and Potential Loss of Saltwater Cooling (Issue number 7).

Since the interim report was issued, the number of issues resulting from the single failure analysis and their effect on plant operation has changed significantly. This follow-up report discusses the resolution and safety significance of all issues resulting from the new ECCS SFA and supersedes the discussions in the interim report.

Validation of Assumptions

The new ECCS SFA was completed assuming a certain plant configuration (e.g., equipment alignments and administrative controls). The results of an SFA are strongly dependent on the assumed plant configuration. Therefore, we completed a validation of the SFA assumptions during the current outage.

As a result of this validation effort, all assumptions of the analysis were confirmed either by review of existing plant documentation (analysis, EQ documentation, procedures, etc.) or by developing new documentation. For example, part of the validation effort was to confirm that inter-system isolation valves are maintained in the position required to assure system separation. Plant procedures were revised to assure that these valves are maintained in the required position.

Resulting Issues

The results of this new ECCS SFA identified nine single failure issues that required resolution by implementation of plant modifications. Eight of these issues will be corrected prior to restart from the current outage. The resolution for one issue (Issue number A7 in the Appendix) has been deferred to the Cycle 12 refueling outage. This deferral is due to the long material lead times and the low safety significance of the issue. A description of the nine single failure issues and their safety significance is provided in Appendix A.

An additional issue (Issue number A10 in the Appendix) was identified during the SFA, but ultimately was shown not to be a single failure concern. This issue involved loss of instrument air and its potential impact on the containment spray line's containment isolation function. Previously, this same line was evaluated and was found to be acceptable during the Systematic Evaluation Program (SEP). A re-evaluation confirmed that the line continues to meet the SEP acceptance criteria. However, as part of the planned Cycle 12 ECCS modifications, an upgrade of the containment isolation function of this line will be implemented to further increase plant safety.

Potential Future Issues

The SFA recommended further review of several items which are related to other ongoing programs. These programs will evaluate single failure susceptibilities not assessed in the ECCS SFA. These programs are: Basis Documentation Program; SEP Topic VI- 7.C.2 (separation); SI/Recirculation System Modifications (IST upgrades); NUREG- 0737 Item III.D.3.4, "Control Room Habitability Requirements"; and revision to Chapter 15 of the UFSAR. The Chapter 15 revision is a new SCE effort to upgrade the design basis accident analyses to meet modern day criteria to the extent practical. At this time no corrective actions are known to be required to be mitigated in these areas. The current schedule for resolution of these items is the end of the Cycle 12 refueling outage.

III. SAFETY SIGNIFICANCE

This section addresses the safety significance of the nine postulated single failures that resulted from the new ECCS SFA. For completeness this report also discusses the tenth issue, which was ultimately determined not to be a single failure concern.

Prior Plant Operation

All single failure issues discussed in this report, individually and collectively, had low safety significance during prior operation of SONGS 1. This conclusion is

based on evaluations described in Appendix A, which show that each issue had a low safety significance due to one or more of the following reasons:

1. A demonstration that the system or component could have completed its safety function because of inherent design features (e.g., high quality components, reliability testing, strength of materials).

2. Likely operator action that would have been taken to mitigate postulated accidents.

3. The results of PRAs indicate an insignificant contribution to the total plant risk.

The total contribution to core damage of all nine single failure issues was estimated to be approximately 4E-6/year. This represents approximately 2% of the total estimated risk for the plant and is therefore of low safety significance.

Future Operation

With the implementation of the identified plant modifications described in this follow-up report, all known single failure susceptibilities have been resolved.* The low safety significance of the issues identified in the new ECCS SFA is consistent with the conclusion made in our Restart Report dated March 17, 1989. In that 1989 report, we stated that "future issues will also have a low safety significance and will not impact safe plant operations." That expectation has been confirmed by the results presented in this report.

IV. CONCLUSIONS

Based on the resolution of issues resulting from completion of this new ECCS SFA, it is concluded that:

1. The identified single failure susceptibilities have been resolved*, and

2. The single failure issues were determined to be of low safety significance.

---

* One item (Vital Bus Transfer) is the subject of SCE's Amendment Application No. 189, currently under NRC review, and will be resolved during the Cycle 12 refueling outage.

APPENDIX A: DESCRIPTION AND SAFETY SIGNIFICANCE OF RESULTING ISSUES

A1. REACTOR COOLANT PUMP OVERCURRENT PROTECTION FAILURE

INTRODUCTION

A failure of the control power which feeds both the Reactor Coolant Pump (RCP) breakers and the bus feeder breakers could have led to failure of the containment electrical penetration(s) due to cable overheating from a potential overcurrent fault(s). However, an overcurrent fault was not expected because of the inherent high reliability of the RCPs and associated electrical cables. To eliminate the potential for this failure mode, a separate source of DC control power for the bus feeder breaker was installed during the current outage.

BACKGROUND

During power operation, the three RCPs receive 4160 volt power from Busses 1A and 1B through separate containment penetrations. The 125 volt DC Bus 1 provided control power to the RCP breakers as well as the bus feeder breakers (see Figure A1). The RCP breakers and bus feeder breakers provide automatic electrical isolation of the electrical containment penetrations from the main generator via Auxiliary Transformers A and B.

In responding to a Loss of Coolant Accident (LOCA), operators are directed to immediately trip the RCPs if they have not automatically tripped, and take action to verify that the RCPs have, in fact, tripped.

During a LOCA, environmental conditions are expected to deteriorate and non-environmentally qualified equipment could fail. The RCP motors and their associated electrical cabling are non-safety related and, therefore, are not environmentally qualified.

If the RCPs did not immediately trip due to loss of 125 volt DC Bus 1 control power, a potential fault path would exist until the main generator coasted down and Auxiliary Transformers A and B were isolated from the grid, thereby removing the power source to the RCPs.

SINGLE FAILURE

If a large overcurrent fault of an energized RCP occurred during failure of the DC Bus 1 control power, the resulting overcurrent could have caused the associated containment electrical penetration to overheat and fail, resulting in the loss of containment integrity.

SAFETY SIGNIFICANCE

This single failure scenario has been eliminated with the plant modifications discussed in the Resolution Section below. The safety significance of the condition which existed prior to these modifications is evaluated below. The evaluation considers operation of the pumps during power operation. The evaluation concluded that even though the RCPs and associated cabling are not environmentally qualified, they are not expected to experience a fault during a LOCA because of their location in the plant, inherent design, and existing integrity.

Cable Failure(s)

The cable is not susceptible to flooding during a LOCA because it is routed above the flood level. Each cable conductor has butyl insulation and neoprene jackets and is surrounded by an armored aluminum sheath. The cables are designed for applications in a steam environment of up to 350 degrees Fahrenheit. The containment is not expected to exceed this temperature during a LOCA. Additionally, these cables are periodically meggered to detect any pre-existing defect capable of degrading sufficiently to cause a fault during an accident.

An evaluation of the potential effects of jet impingement from an RCS pipe slot break concluded that jet impingement will not damage the cables' armored sheath.

Because of their design, the cables are not expected to suffer an electrical fault due to a LOCA environment.

Motor Failure(s)

The RCP motors are housed in a drip-proof case designed for outdoor use. If spray from a postulated pipe break should enter openings in the drip-proof case from below, the motor windings are protected by their insulation. The motor windings are also meggered every refueling outage to verify their integrity. The winding insulation is "Thermalastic." Testing of this insulation material has demonstrated that it will function for a minimum of 400 hours at 400 degrees Fahrenheit.

The junction box on the motor is also enclosed to preclude spray entry. In addition, the cable connections and bus bars inside the junction box are insulated.

Because of the water-proof cases and the insulation, the RCP motors are not expected to suffer an electrical fault due to a LOCA environment.

Operator Action Following a LOCA

Following a LOCA, Emergency Operating Instructions (EOIs) direct the operators to verify that the RCPs have tripped. Upon detection of the failure of the RCPs to trip, the operators would disconnect power to the main transformer by tripping the switchyard breakers from the control room. This would leave the RCPs powered only from the stored energy in the main generator. Once the generator has completed its coast-down, power is no longer available to the RCPs. The possibility for an overcurrent condition is terminated once the power to the RCPs is removed.

A PRA (attached) was also conducted to evaluate the risk of containment failure due to an electrical fault. This PRA estimates that the containment failure frequency due to this scenario was approximately 3.0E-10 per year. This risk is insignificant, since it is a small fraction of the overall risk of containment failure.

RESOLUTION

A plant modification was implemented during this outage to provide a separate source of DC power to the RCP bus feeder breakers. This modification provides a redundant means of tripping the RCPs: either by the RCP bus feeder breaker or by the RCP breakers.

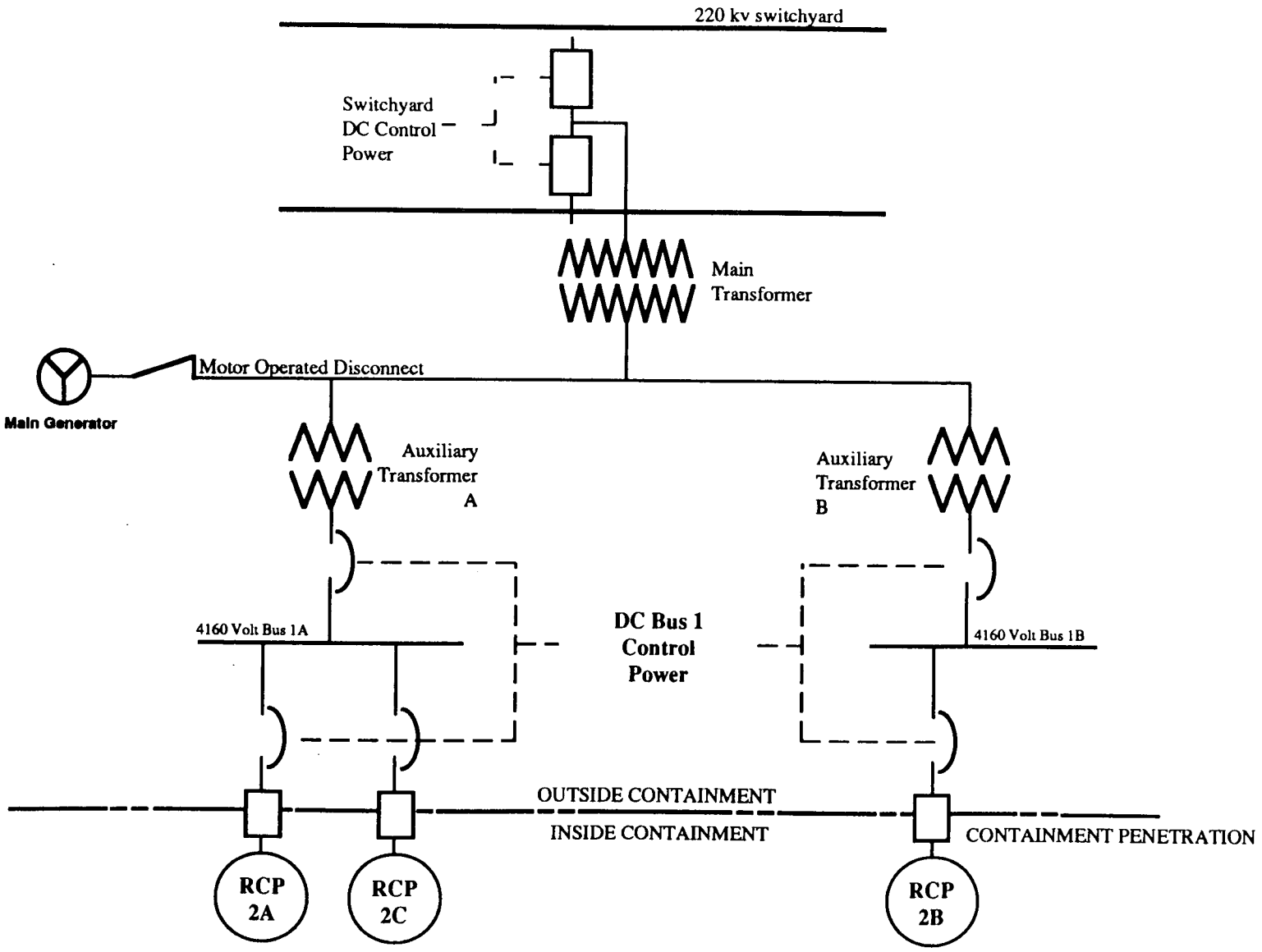


Figure A1. RCP Breaker Configuration

PRA FOR REACTOR COOLANT PUMP OVERCURRENT PROTECTION FAILURE

PURPOSE

The purpose of this probabilistic risk assessment (PRA) is to determine the annual likelihood of containment failure due to reactor coolant pump (RCP) penetration failure from shorted RCP motor circuits.

ASSUMPTIONS

1. The RCP motors windings are encapsulated and enclosed in drip proof enclosures. The pump windings insulation provides protection from spray from below. The motor cables are waterproof and armored. It is assumed that a steam or water environment would have little likelihood of causing a major electrical short.

2. Were a short to occur and not be isolated, the circuit would fail at its weakest point. It is not believed that the penetration would be the point where the circuit would fail. However, prior to fault interruption by circuit failure, excessive current would be carried through the penetration. It is conservatively assumed that 90% of shorts will result in penetration failure and that failure will occur quickly.

3. LOCAs can only short one RCP due to the separation and compartmentalization of the three primary loops within containment.

4. Operator actions to manually trip the RCPs, the RCP feeder breakers, or the switchyard breakers are not assumed to be successful in the analysis since the RCP penetration may have failed prior to the time normal operator response can be credited.

5. Although the DC control bus that provided tripping power to the RCP breakers has a number of unqualified loads inside containment, it is not expected that the bus will fail if these loads are also shorted. Each of the non-qualified loads is protected by breakers and fuses. The likelihood of sufficient shorted loads remaining on the bus to significantly affect bus performance is assumed to be negligible.

6. Based upon a physical inspection of the RCP motor and cable layout inside containment, it is unlikely that LOCAs would result in jet impingement loads sufficient to cause cable or motor failure (the RCP components are adequately protected from the effects of LOCA pipe whip). Pump winding insulation provides protection from spray from below. Although an evaluation has concluded that cable/motor damage is not possible, it is conservatively assumed that an RCP short will occur with a 0.01 likelihood following a large LOCA and a 0.001 likelihood following a small or small-small LOCA.

7. From the Oconee PRA (NSAC-60), the following initiating event frequencies are assumed:

   Large LOCA - 9.3E-4/year

   Small LOCA - 3.0E-3/year

8. The frequency of a small-small LOCA is assumed to be 2E-2 per year as used in the SONGS-1 PRA. This value is based upon an NRC estimate of the frequency of an RCP seal LOCA.

9. From the IREP Procedures Guide (NUREG/CR-2728), the failure probability of a circuit breaker to trip is 3.0E-3 per demand and the probability of bus shorts is 1.0E-8 per hour.

10. In addition to the possibility of mechanical failure of individual 4160 volt RCP pump breakers, failure of DC Bus 1 or the 4160 volt bus control power breaker would result in a common cause failure of all breakers. The probability of spurious opening of the 4160 volt bus control power breaker is negligible and is not considered. It is conservatively assumed that DC power is required for a period of one hour after an accident to clear RCP-related faults.

11. Under normal operating conditions, both the DC battery and the battery charger are capable of supplying the DC loads. The battery is seldom removed from service for maintenance (There are redundant battery chargers). Based upon SONGS 1 operating experience, it is assumed that the battery is removed from service for two hours every year, resulting in a 2.28E-4 probability that the battery is out of service at the start of the accident. If the battery is not available, the DC bus is dependent upon the battery charger. The IREP Procedures Guide recommends a failure rate of 1E-6/hour for these devices. However, for conservatism, a failure rate of 1E-5/hour will be used based upon past problems with the chargers. No credit is taken for connecting the redundant battery charger to the bus if the operating battery charger fails.

12. If the DC bus is powered from only the charger, an interruption of power to the charger will also de-energize the DC bus. The most likely reason for charger power interruption is a loss of offsite power (which the SONGS-1 PRA assumes occurs at a rate of 1E-3 per plant trip). The emergency diesel generator would not be actuated to restore power with an interruption of the DC bus. Therefore it is assumed that a loss of offsite power during periods that the DC bus is powered only from the battery charger would prevent tripping of the RCP protective circuit breakers.

ANALYSIS

The following scenarios are postulated:

Large LOCA: A large LOCA occurs and an RCP shorts. The RCP supply breaker and the bus feeder breaker fail to trip.

Small LOCA: A small LOCA occurs and an RCP shorts. The RCP supply breaker and the bus feeder breaker fail to trip.

Small-Small LOCA: A small-small LOCA occurs and an RCP shorts. The RCP supply breaker and the bus feeder breaker fail to trip.

The probability of DC Bus #1 loss during the first hour after an accident is calculated as follows:

P(DC Bus loss) = P(bus short in first hour) +
P(battery unavailable) * [P(charger failure) +
P(loss of offsite power following accident)]

= (1.0E-8/hour)(1 hour) +(2.28E-4) * [(1E-5/hour) * (1 hour) + 1E-3]
= 2.4E-7

Therefore, the failure of a single RCP breaker and its bus feeder breaker is calculated as follows:

P(RCP and feeder breaker failure) = [P(RCP breaker failure) *
P(feeder breaker failure)] + P(DC bus loss)
= [(3E-3) * (3E-3)] + 2.3E-7
= 9.2E-6

The calculation of frequency of containment failure due to RCP penetration overcurrent is provided below:

	Large LOCA	Small LOCA	Small-Small LOCA
Initiator Frequency	9.3E-4	3.0E-3	2.0E-2
Probability of RCP Short	0.01	0.001	0.001
RCP Breaker & Bus Feeder Breaker Fail to Trip	9.2E-6	9.2E-6	9.2E-6
Fault Causes Penetration Failure	0.9	0.9	0.9
Containment Failure Frequency	7.6E-11	2.4E-11	1.6E-10

The total calculated containment failure frequency for LOCAs is 3.0E-10 per year.

CONCLUSION

The results of the above calculation show that the risk of containment failure and significant release of radioactivity to the environment due to uncleared RCP motor shorts is very low at 3.0E-10 per year. As noted throughout the calculation, there is significant conservatism included in the calculated value. Hence, the actual risk of containment failure is probably much lower.

A2. INADEQUATE RECIRCULATION FLOW DUE TO LOSS OF INDICATION

INTRODUCTION

An undetected loss of recirculation flow indication could have resulted in reduced long term cooling during an accident. However, other indications were available to alert the operators to the reduced core cooling condition. Since the operators would have been able to correct the condition using other indicators, the safety significance is low. A modification has been performed so that a single failure will not result in loss of recirculation flow indication to more than one loop.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the refueling water Storage Tank (RWST) to the Reactor Coolant System (RCS) and the Containment Spray System (CSS). After the RWST inventory has been depleted, recirculation is initiated to utilize the water accumulated in the containment sump for containment spray and long term cooling.

The operators have control room indication of recirculation flow to RCS loops A, B, and C (Figure A2). Operators rely on these indicators to manually set and maintain the proper recirculation flow rates. If a LOCA were to occur with the break in loop A, only the flow to loops B and C would be available to provide core cooling. The flow instruments for loops B and C had a common power supply. The output of the common power supply is not indicated or alarmed.

SINGLE FAILURE

The common power supply could have failed such that the loops B and C flow instruments provided a non-erratic indication that was higher than actual flow but not off-scale. If this failure were undetected, the operators may not have set a recirculation flow adequate for core cooling.

SAFETY SIGNIFICANCE

This single failure scenario has been eliminated by the modification described in the resolution section below. The safety significance of the condition which existed prior to these modifications is evaluated below. The evaluation concluded the safety significance was low because of the likelihood that the failure would have been apparent to operators who could then take appropriate action. Additionally, the probability of the common power supply failing in this specific mode is low.

If a power supply failure resulting in non-erratic, on-scale indication were to have occurred, the instruments could have appeared to have been responding normally when the operators adjusted recirculation flow rates. If the loops B and C instruments had been indicating higher than actual flow rates, the operators could have unknowingly set flow lower than required. The lower flows could have resulted in decreased core heat removal, which would have been indicated by increasing RCS temperatures. Operators could have detected the temperature rise on the core exit thermocouples. Operators could have then increased the total recirculation flow to within the limit of the charging pump motor current and restored adequate core cooling.

A PRA was performed (attached) which assumed the low flow condition remained undetected. The probability of core damage was determined to be 2.1E-9 per year using this assumption. This risk is an insignificant contribution to the overall plant core damage frequency.

Based on the expected operator action and the low contribution to total core damage frequency of the specific failure mode, this issue has low safety significance.

RESOLUTION

A modification was performed during this outage to provide separate power supplies for the loops B and C recirculation flow instruments. The failure of a power supply as described above would therefore affect only one flow instrument, leaving two loops with correct indications. One of these loops will be available to feed the break, leaving the other loop available to cool the core as required by the design basis.

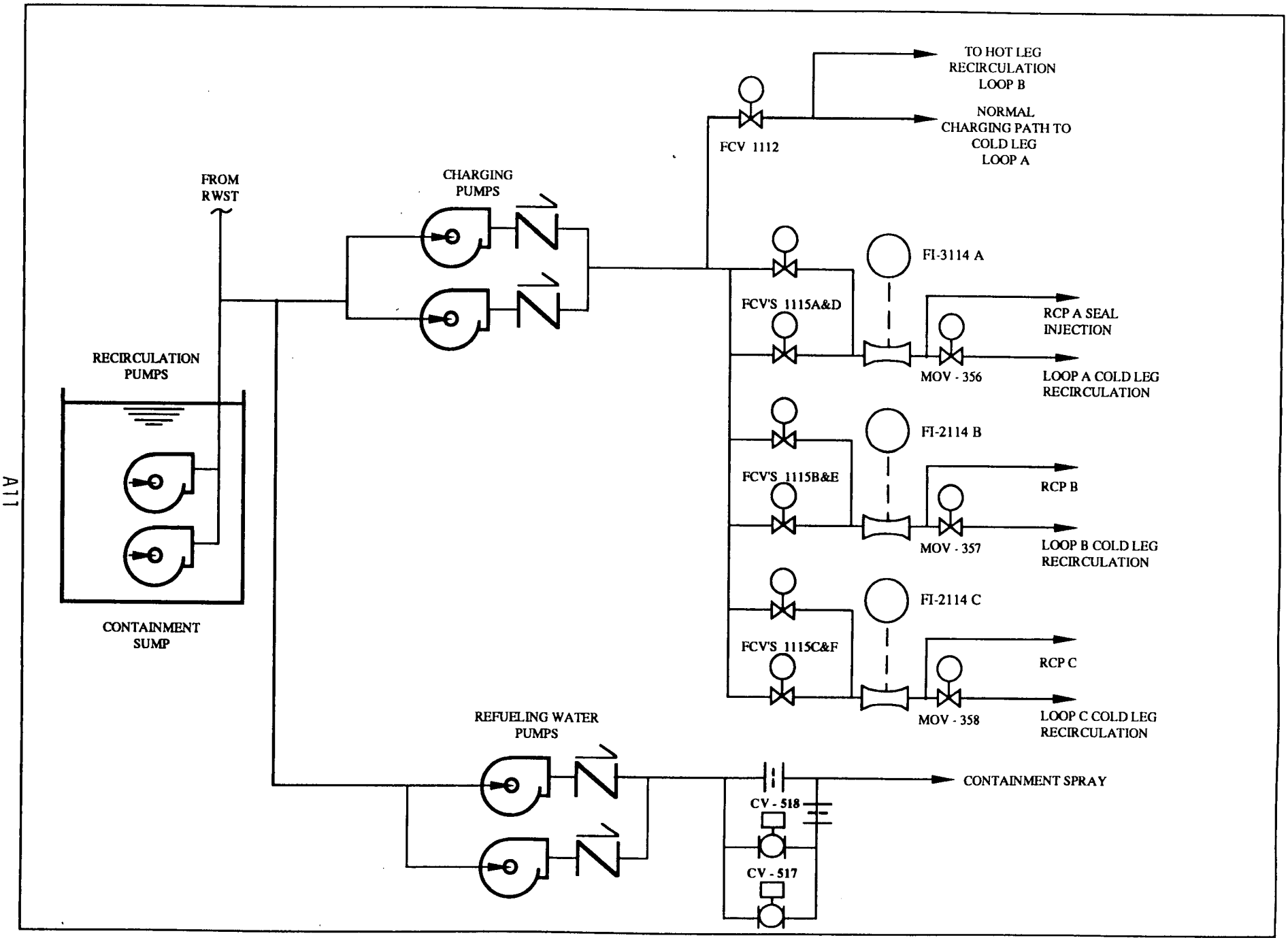


Figure A2. Recirculation System Configuration

PRA FOR INADEQUATE RECIRCULATION FLOW DUE TO LOSS OF INDICATION

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of a postulated failure of the common power supply to the loop B and C recirculation flow instruments.

ANALYSIS

The analysis considers the potential for core damage resulting from failure of the common power supply to the loop B and C recirculation flow instruments. The following assumptions were used in the analysis:

- The mission time of the loop B and C recirculation flow instruments is assumed to be six hours. Failure of the common power supply within six hours is assumed to lead to core damage. Failure of the common power supply after six hours is assumed not to lead to core damage since the associated loop recirculation flows would have been set by that time and significant time is available for recovery actions to assure adequate core cooling.

- The probability of a small and large LOCA is assumed to be 3.9E-3 per year from the Oconee PRA (NSAC-60).

- The probability of the common power supply failing is not indicated in any of the generic data sources. For conservatism, the failure rate of the common power supply was assumed to be the same as the failure rate of a battery charger. A battery charger is a more complex device than a regulated power supply, but contains many of the same electronic components. There is no data for the probability of a battery charger failing with the output high, non-erratic, but less than a specified value. Therefore the failure rate for a charger simply failing high was used. From IEEE Std 500-1984, page 66, this value is 9E-8 per hour.

The frequency of common cause failure of the loop B and C recirculation instruments potentially leading to core damage, F(CD), is calculated as follows:

F(CD) =F(LOCA) *
P(COMMON POWER SUPPLY FAILS HIGH FAILURE RATE) *
MISSION TIME

where:

F(LOCA) = Frequency of a LOCA
= 3.9E-3 per year (Oconee PRA (NSAC-60))

P(COMMON POWER SUPPLY FAILS HIGH FAILURE RATE) = 9.0E-8 per hour (taken from IEEE Std. 500-1984)

MISSION TIME = 6 hours (as indicated above)

Thus, F(CD) = 3.9E-3 per year * 9.0E-8 per hour * 6 hours
= 2.1E-9 per year

CONCLUSIONS

The postulated failure of the loops B and C flow instruments common power supply has an insignificant impact upon total plant risk with an estimated frequency of 2.1E-9 per year. This contribution to the overall plant core damage frequency, estimated to be 2E-4 per year, is approximately 0.001%.

A3. LOSS OF REACTOR COOLANT INVENTORY DUE TO FAILURE OF LETDOWN ISOLATION VALVES

INTRODUCTION

A failure of a letdown isolation valve could have led to loss of recirculation flow and potential inadequate core cooling due to the resulting loss of reactor coolant inventory. However, in response to alarms, operators would have taken action to isolate the letdown flow. Accordingly, the safety significance of this scenario is low. A modification has been implemented to provide redundant automatic letdown isolation capability.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the refueling water storage tank (RWST) to the Reactor Coolant System (RCS) and the Containment Spray System (CSS). After the RWST inventory has been depleted, recirculation is initiated to utilize the water which accumulates in the containment sump for containment spray and long term cooling.

The Letdown and Excess Letdown Systems are also connected to the RCS. These systems, in conjunction with the Charging System, regulate the letdown and charging flows to control the volume of water (inventory) in the RCS and maintain a programmed pressurizer level. Letdown is directed to the Volume Control Tank (VCT) outside of containment. In the event of a high level in the VCT, the letdown flow is directed to the Radwaste System (RWS). The flow will pass through the RWS Flash Tank, and then into the RWS Hold-up Tank.

The Letdown System is normally in operation while the Excess Letdown System is isolated from the RCS by multiple valves. However, the Excess Letdown System is periodically placed in service during stroke testing of the letdown isolation valves. Figure A3 shows the valve configuration of the Letdown and Excess Letdown Systems. Letdown isolation valves CV-202, CV-203, and CV-204 automatically isolate the Letdown System from the RCS on a SIS. The Excess Letdown System is isolated from the RCS using remote-manual valves. Containment isolation valves CV-525 and CV-526 are also remotely operated from the control room.

During a LOCA, the total reactor coolant inventory available to mitigate the consequences of the accident is the volume of water in the RCS plus the volume of water injected from the RWST. During recirculation, the inventory which collects in the containment sump must be sufficient to provide the Net Positive Suction Head (NPSH) required to support subsequent recirculation pump operation.

SINGLE FAILURE

If a Letdown System isolation valve failed to close on a safety injection signal or leaked excessively, post-LOCA reactor coolant inventory could have been lost. Reactor coolant inventory also could have been lost through the Excess Letdown System if it was in operation at the time of the event.

Reactor coolant inventory loss during a LOCA could have reduced the containment sump level and the NPSH available to the recirculation pumps. However, the amount of reactor coolant inventory that could have been lost due to the single failure of a letdown isolation valve is a small portion of the amount that would have had to have been lost to have a significant effect on the recirculation pump NPSH (approximately 85,000 gallons). Therefore, the operators would have had sufficient time to stop the diversion flow.

In the unlikely event this condition would not have been recognized, insufficient NPSH to the recirculation pumps could have resulted causing pump cavitation, eventual pump failure, loss of recirculation flow, and potential inadequate core cooling. Additionally, the diverted letdown could have filled the RWS Hold-up Tank which could have eventually overflowed, thereby increasing off-site radiological releases.

SAFETY SIGNIFICANCE

This single failure scenario has been eliminated with the plant modifications discussed in the Resolution Section below. The safety significance of the condition which existed prior to these modifications is evaluated below. The evaluation concluded that safety significance of the potential diversion is low due to the likelihood of operator action and the small amount of reactor coolant inventory that could have been lost. The operators are expected to isolate the letdown containment isolation valves (CV-525 and CV-526) within 30 minutes of a LOCA. The volume of water diverted is dependent on whether the event is a Small or Large Break LOCA.

Large Break LOCA

During a Large Break LOCA (LBLOCA), the high containment radiation alarm would occur quickly. Emergency Operating Instruction (EOI) SO1-1.5-3 requires the operator to close CV-525 and CV-526 in the event of a high containment radiation alarm. This would isolate the diversion within approximately 30 minutes of the event.

During the LBLOCA, the RCS rapidly depressurizes from over 2000 psig to the containment pressure (less than 52 psig). The amount of flow possible through the letdown path during this reduced RCS pressure condition is low (less than 5 gpm). The total estimated amount of reactor coolant inventory lost through the letdown diversion path during the LBLOCA is approximately 150 gallons. This small volume would not have had a significant effect on containment sump level or recirculation pump NPSH.

The diverted reactor coolant water would have been contained in the RWS hold-up tank. Even though these tanks were not upgraded as part of the seismic reevaluation program, they are expected to maintain structural integrity. In addition, the likelihood of a design basis seismic event coincident with these other failures is remote. Therefore, there would have been no effect on the off-site radiological consequences.

Small Break LOCA

During a Small Break LOCA (SBLOCA), the high containment radiation alarm setpoint would not be reached as quickly as during a LBLOCA. However, there are other alarms (such as VCT high level, letdown diversion, or auxiliary building radiation monitor) which are indications of letdown flow diversion. As mentioned above, not all of this equipment was upgraded as part of the seismic program. However, the equipment does have inherent resilience to a seismic event, and the likelihood of a seismic event coincident with these other failures is remote. Since there are significantly fewer actions to perform during a SBLOCA, it is expected that the operators would have reacted to these other alarms within 30 minutes to close CV-525 and CV-526.

During a SBLOCA, the RCS does not depressurize as quickly as for a LBLOCA. Accordingly, the letdown diversion flow rate (approximately 100 gpm) would be higher for a SBLOCA. The amount of reactor coolant inventory lost during a SBLOCA due to diversion of letdown flow is estimated to be 3000 gallons. Calculations have shown that up to 85,000 gallons of inventory could be lost without significantly affecting the recirculation pump NPSH. Therefore, the loss of 3000 gallons of reactor coolant during a SBLOCA would not have had a significant effect on recirculation pump NPSH.

The estimated 3000 gallons of reactor coolant lost during a SBLOCA would have been diverted to the RWS Hold-up Tank. The inventory in the RWS Hold-up Tank is normally maintained at least 6000 gallons below the overflow. Therefore, the tank would not have overflowed, and there would have been no effect on the off-site radiological dose consequences.

A PRA (attached) was performed to estimate the contribution of this single failure to the overall core damage frequency. The PRA results determined the probability of core damage as 2.3E-7 per year. This accounts for less than 0.2% of the total overall core damage frequency.

Based on operator action to isolate the post-LOCA letdown flow in response to alarms and the low contribution to overall core damage frequency, this issue has low safety significance.

RESOLUTION

Plant modifications and an additional administrative control were implemented during this outage to ensure redundant letdown isolation capability. Specifically, letdown control valve LCV-1112 was modified so that it fails closed rather than open. Additionally, automatic safety injection closure signals were provided to LCV-1112 and to excess letdown valves CV-287, CV-412, and CV-413. As an added safety measure, the EOI's are being revised to require closure of CV-525 and CV-526 prior to initiation of recirculation. These changes ensure that redundant automatic isolation valves are available to isolate letdown in the event of a single failure.

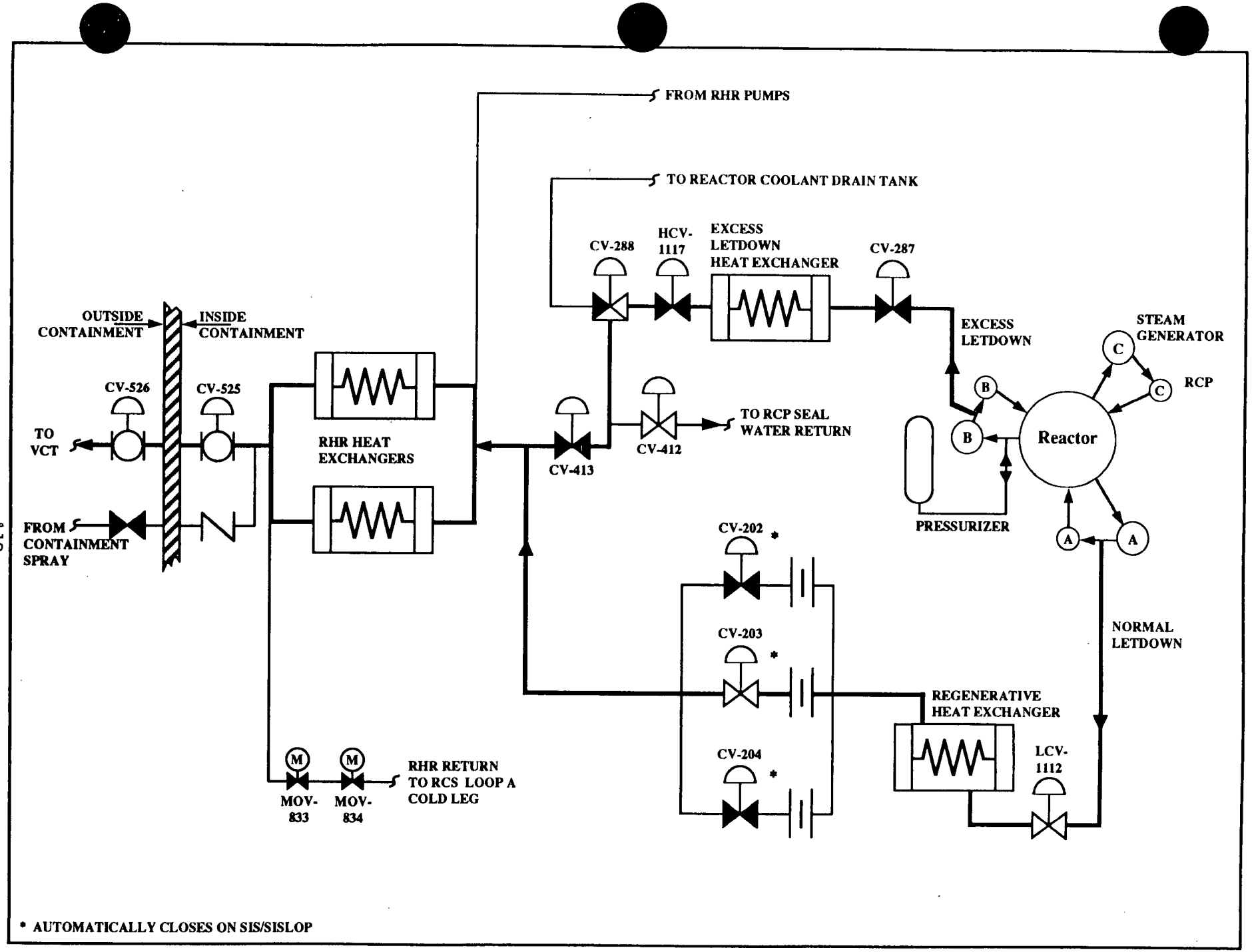


Figure A3. Letdown And Excess Letdown Systems

PRA FOR LOSS OF REACTOR COOLANT INVENTORY DUE TO FAILURE OF LETDOWN ISOLATION VALVES

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of a postulated letdown valve single failure resulting in loss of post-LOCA reactor coolant.

ASSUMPTIONS

The following assumptions were utilized in the analysis:

- In a large LOCA, the potential open letdown path flow is sufficiently small (less than 5 gpm) that adequate time is available for operator action to close the letdown isolation valves prior to affecting recirculation system operation. Although the operator is expected to close the valve within 30 minutes, in reality, he will have significantly more than 30 minutes before any core damage would take place. The probability of operator failure to detect and close the available letdown isolation valves is assumed to be 1E-3 based on the time available for operator action.

- In a small break LOCA, the potential open letdown path flow is small (approx. 100 gpm) and the RWST inventory which could be lost is large (85,000 gallons). Therefore adequate time is available for operator action to detect the flow diversion and close any of the many available letdown isolation valves prior to affecting recirculation system operation. Although the operator is expected to close the valve within 30 minutes; in reality, he would have significantly more than 30 minutes before any core damage would occur. Multiple indications of inventory depletion (e.g. VCT level, letdown diversion, and radiation monitors in the Auxiliary Building) are available to the operators to detect letdown flow diversion. However, since the cause of these indications may not be apparent in all cases, a conservative operator failure probability of 1E-2 to detect the diversion is assumed.

- Letdown control valve LCV-1112 was a fail open valve in the normal letdown path. All other letdown flow control valves considered in the analysis are fail closed valves. Operation of instrument air is required to close LCV-1112. The probability of instrument air failure given a large and small break LOCA is assumed to be 1E-1 and 1E-2, respectively. This is based upon a previous analysis of instrument air vulnerability in large and small break LOCAs.

- Letdown isolation valves CV-202, 203, and 204 are air-operated and fail closed on loss of instrument air or power. The only likely modes for failure to close following a LOCA were: failure of solenoid valve to isolate instrument air and bleed air off the valve actuator, or failure of the air-operated valve to close due to mechanical

problems. Based upon previous plant experience, it is assumed that one of these valves may not close upon demand. Therefore, the isolation capability of these valves is not credited in the analysis.

- The excess letdown path is normally in service only during periods where letdown line valves are stroked per surveillance requirements. The average time per month that the excess letdown path was in service is assumed to be two hours based upon discussions with operations personnel.

- Leakage through closed letdown isolation valves is not assumed to lead to critical loss of recirculation coolant inventory resulting in core damage. Sufficient time would be available for operator actions to close other valves in the letdown paths to further limit the letdown leakage and add additional borated water to the RCS via the injection systems.

- In the event the normal letdown isolation valves failed open, Letdown System containment isolation valves CV-525 or CV-526 could have been closed to prevent recirculation inventory from leaving the containment and normal recirculation flow path. CV-525 and 526 fail closed on loss of power and drift closed on loss of air. Since the operators are directed in the EOIs to close valves CV-525 and 526 on a high containment radiation alarm, there is a high likelihood (assumed to be 3E-3) that the operators would have closed these valves in a large break LOCA event.

- The benefit of containment pressurization following a LOCA in providing additional NPSH to the recirculation pumps is not quantitatively credited. It is assumed to add additional time to that available for operator detection and mitigation of an inventory diversion.

ANALYSIS

The frequency of loss of recirculation coolant inventory outside the recirculation system boundary leading to core damage is estimated by the following equation:

F(CD) = F(CD FROM LARGE LOCA) + F(CD FROM SMALL LOCA)

Large Break LOCA Analysis:

F(CD LARGE LOCA) = F(LARGE LOCA) *
[P(NORM LETDOWN ISOL VALVES FAIL TO CLOSE IN LARGE LOCA)*
P(CONTAINMENT ISOL VALVE FAIL TO CLOSE IN A LARGE BREAK LOCA)] +
[P(EXCESS LETDOWN IS IN SERVICE) *
P(EXCESS LETDOWN ISOL VALVES FAILS TO CLOSE)]

where:

F(LARGE LOCA) = 9E-4 per year (NSAC/60, Oconee PRA)

P(NORMAL LETDOWN ISOL VALVES FAIL TO CLOSE IN LARGE LOCA) =
= P(LCV-1112 FAILS TO CLOSE) *
[P(CV-202 FAILS TO CLOSE) +
P(CV-203 FAILS TO CLOSE) +
P(CV-204 FAILS TO CLOSE)]

P(LCV-1112 FAILS TO CLOSE) = P(INSTR. AIR FAILS GIVEN A LARGE BREAK LOCA) +
P(SOLENOID FAILS TO OPERATE ON DE-ENERGIZE)+
P(NO OPERATOR ACTION TO CLOSE)+
P(AIR-OPERATED VALVE FAILS TO CLOSE)
= 1E-1 + 1E-3 + 1E-3 + 1E-3
(SEE ASSUMPTIONS AND NUREG/CR-2728)
= 1.0E-1

P(CV-203 FAILS TO CLOSE) = 1.0 (BASED ON ABOVE ASSUMPTION)

P(CV-204 FAILS TO CLOSE) = (SAME FAILURE MODES AS CV-203)
= 1.0

P(CV-202 FAILS TO CLOSE) = (SAME FAILURE MODES AS CV-203)
= 1.0

P(NORMAL LETDOWN ISOL VALVES FAIL TO CLOSE IN LARGE BREAK LOCA) = 1.0E-1 * 1
= 1.0E-1

P(CONTAINMENT ISOL VALVES FAIL TO CLOSE IN LARGE BREAK LOCA) =
= P(CV-525 FAILS TO CLOSE) * P(CV-526 FAILS TO CLOSE GIVEN CV-525 FAILS TO CLOSE)

P(CV-525 FAILS TO CLOSE) = P(PNEUMATIC/HYDRAULIC VALVE FAILS TO CLOSE) + P(OPERATOR FAILS TO CLOSE VALVE)
= 3E-3 (NUREG/CR-2728) + 3E-3 (NUREG/CR-1278)
= 6E-3

P(CV-526 FAILS TO CLOSE GIVEN CV-525 FAILS TO CLOSE) = (SAME AS CV-525)
= 0.1 (COMMON CAUSE BETA FACTOR)

P(CONTAINMENT ISOL VALVES FAIL TO CLOSE IN LARGE BREAK LOCA) =
= 6E-3 * 0.1
= 6E-4

P(EXCESS LETDOWN IN SERVICE) = 2 HOURS / MONTH *
1 MONTH/730 HOURS (SEE ABOVE ASSUMPTIONS)
= 2.74E-3

P(EXCESS LETDOWN ISOLATION VALVE FAIL TO CLOSE) =
P(NO OPERATOR ACTION TO CLOSE EXCESS LETDOWN VALVES) +
[P(CV-287 FAILS TO CLOSE) *
P(CV-412 OR CV-413 FAIL TO CLOSE)]

P(CV-287 FAILS TO CLOSE) = P(AIR-OP. VALVE FAILS TO CLOSE) +
P(SOLENOID VALVE FAILS TO OPERATE ON DE-ENERGIZE)
= 3E-3 + 1E-3 (NUREG/CR-2728)
= 4E-3

P(CV-412 OR CV-413 FAIL TO CLOSE) = 2 * 4E-3 (SAME AS CV-287 FAILURE MODES)
= 8E-3

P(EXCESS LETDOWN ISOLATION VALVES FAIL TO CLOSE) =
= 1E-3 + (3E-3 * 8E-3)
= 1E-3

Thus:

F(CD FROM LARGE BREAK LOCA) = 9E-4 * [(1.OE-1 * 6E-4) +
(2.74E-3 * 1E-3)]
= 5.7E-8 PER YEAR

Small Break LOCA Analysis:

F(CD SMALL LOCA) = F(SMALL LOCA) *
[P(NORM LETDOWN ISOL VALVES FAIL TO CLOSE IN SMALL LOCA) *
P(CONTAINMENT ISOL VALVES FAIL TO CLOSE IN SMALL LOCA)] +
[P(EXCESS LETDOWN IS IN SERVICE) *
P(EXCESS LETDOWN ISOL VALVES FAILS TO CLOSE)]

F(SMALL LOCA) = 3E-3 per year (NSAC/60, Oconee PRA)

P(NORMAL LETDOWN ISOL VALVES FAIL TO CLOSE IN SMALL LOCA) =
= P(LCV-1112 FAILS TO CLOSE) *
[P(CV-202 FAILS TO CLOSE) +
P(CV-203 FAILS TO CLOSE) +
P(CV-204 FAILS TO CLOSE)]

P(LCV-1112 FAILS TO CLOSE) = P(INSTR. AIR FAILS) +
P(SOLENOID FAILS TO OPERATE ON DE-ENERGIZE)+
P(NO OPERATOR ACTION TO CLOSE)+
P(AIR-OPERATED VALVE FAILS TO CLOSE)
= 1E-2 + 1E-3 + 1E-2 + 1E-3
(SEE ASSUMPTIONS AND NUREG/CR-2728)
= 2.2E-2

P(CV-203 FAILS TO CLOSE) = 1.0 (SEE ABOVE ASSUMPTION)

P(CV-204 FAILS TO CLOSE) = (SAME FAILURE MODES AS CV-203)
= 1.0

P(CV-202 FAILS TO CLOSE) = (SAME FAILURE MODES AS CV-203)
= 1.0

P(NORMAL LETDOWN ISOL VALVES FAIL TO CLOSE IN SMALL LOCA) =
= 2.2E-2 * 1.0
= 2.2E-2

P(CONTAINMENT ISOL VALVES FAIL TO CLOSE IN SMALL LOCA)=
=P(CV-525 FAILS TO OPEN) * P(CV-526 FAILS TO CLOSE GIVEN CV-525 FAILS TO CLOSE)

P(CV-525 FAILS TO CLOSE) = P(PNEUMATIC/HYDRAULIC VALVE FAILS TO CLOSE) + P(OPERATOR FAILS TO CLOSE VALVE)
= 3E-3 (NUREG/CR-2728) + 1E-2 (SEE ABOVE ASSUMPTION)
= 1.3E-2

P(CV-526 FAILS TO CLOSE GIVEN CV-525 FAILS TO CLOSE) = 0.1
(COMMON CAUSE BETA FACTOR)

P(CONTAINMENT ISOL VALVES FAIL TO CLOSE IN SMALL LOCA) =
= 1.3E-2 * 0.1
= 1.3E-3

P(EXCESS LETDOWN IN SERVICE) = 2 HOURS / MONTH *
1 MONTH/730 HOURS (SEE ABOVE ASSUMPTIONS)
= 2.74E-3

P(EXCESS LETDOWN ISOLATION VALVE FAIL TO CLOSE) =
P(NO OPERATOR ACTION TO CLOSE EXCESS LETDOWN VALVES) +
[P(CV-287 FAILS TO CLOSE) *
P(CV-412 OR CV-413 FAIL TO CLOSE)]

P(CV-287 FAILS TO CLOSE) = P(AIR-OP. VALVE FAILS TO CLOSE) +
P(SOLENOID VALVE FAILS TO OPERATE ON DE-ENERGIZE)
= 3E-3 + 1E-3 (NUREG/CR-2728)
= 4E-3

P(CV-412 OR CV-413 FAIL TO CLOSE) = 2 * 4E-3 (SAME AS CV-287 FAILURE MODES)
= 8E-3

P(EXCESS LETDOWN ISOLATION VALVES FAIL TO CLOSE) =
= 1E-2 + (3E-3 * 8E-3)
= 1E-2

Thus:

F(CD FROM SMALL LOCA) = 3E-3 * (2.2E-2 * 1.3E-3)+(2.74E-3 * 1E-2)]
= 1.7E-7 per year

THE TOTAL SMALL AND LARGE LOCA CORE DAMAGE FREQUENCY FROM LETDOWN LINE DIVERSION IS THEN:

F(CD) = F(CD FROM SMALL BREAK LOCA) + F(CD FROM LARGE BREAK LOCA)
= 5.7E-8 per year + 1.7E-7 per year
= 2.3E-7 per year

CONCLUSIONS

The probability of core damage resulting from loss of recirculation coolant through letdown flow paths was low. The contribution (2.3E-7 per year) to the overall core damage frequency, estimated to be 2E-4 per year, was low, accounting for less than 0.2% of the total. If this scenario did occur, other operator actions not considered in the analysis such as re-initiating injection from the RWST or other borated water sources would have been possible to preclude these single failures from leading to core damage.

A4. LOSS OF PUMPS DURING RECIRCULATION

INTRODUCTION

A failure of a spray flow limiter valve or a recirculation flow control valve could have resulted in loss of recirculation and/or containment spray due to run-out of the recirculation and/or refueling water pumps. However, procedural guidance requires operator responses which would have mitigated the event. Therefore, the safety significance of this susceptibility is low. To eliminate this susceptibility, design modifications and additional administrative controls have been implemented during the current outage which ensure adequate NPSH is available to the pumps.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the Refueling Water Storage Tank (RWST) to the Reactor Coolant System (RCS) and the Containment Spray System (CSS). After the RWST inventory has been depleted, recirculation is initiated to utilize the water which accumulates in the containment sump for containment spray and long term cooling.

Both recirculation pumps are initially started for recirculation. One recirculation pump would have been secured six hours into the event. The remaining recirculation pump would have continued to supply both a refueling water pump for containment spray and a charging pump for recirculation.

During the recirculation phase, the recirculation pumps take suction from the containment sump and discharge into a common header. This header supplies suction to both the charging pumps and refueling water pumps (see Figure A4), therefore, the NPSH available at the suction of the charging pumps and refueling water pumps is dependent upon the discharge pressure and flow of the recirculation pumps.

The combined flow capacity of a charging pump and a refueling water pump exceeds that of one recirculation pump. To prevent failure of the recirculation pump due to run-out, the flow through the containment spray header is restricted by an orifice to limit the total flow of the system to within the recirculation pump capacity (see Figure A4). Two parallel spray flow limiting valves, CV-517 and CV-518, work in conjunction with the flow orifice to obtain the optimum spray flow. During the injection phase, the valves are open so that maximum spray flow is achieved. The valves are closed to place the orifice in service when recirculation is initiated.

Charging pump cold leg recirculation flow to each of the three RCS loops is throttled by flow control valves, FCV-1115D, E, and F. The flow control valves are in parallel with reactor coolant pump (RCP) seal injection valves, FCV-1115A, B, and C. Motor

operated valves, MOV-356, 357, and 358, are located downstream of the flow control valves and may be closed to reduce recirculation flow to RCS loops A, B, and C, respectively.

SINGLE FAILURE

During single recirculation pump operation, failure of a spray flow limiter valve (CV-517 or CV-518) or a recirculation flow control valve (FCV-1115D, E, or F) in the open position could have caused the running recirculation pump to run-out and fail. This would have lead to a loss of NPSH to the charging pumps and refueling water pumps. Both charging pumps could be lost since the second charging pump would have started upon failure of the first and subsequently failed, resulting in the loss of recirculation and containment spray. However, operator action in accordance with procedural guidelines would have mitigated the event.

During the initial six hours of recirculation two recirculation pumps are operating. Failure of either CV-517 or CV-518 in the open position could have resulted in run-out of a refueling water pump. If operator action had not been taken to mitigate this failure, loss of recirculation or containment spray would have resulted.

SAFETY SIGNIFICANCE

This single failure susceptibility has been eliminated with the plant modifications and administrative controls discussed in the Resolution Section below. The safety significance of the condition which existed prior to these modifications and administrative controls is evaluated below. The evaluation concluded that this issue had low safety significance because of their low probability of occurrence and operator actions which could have prevented pump failures.

These single failures would not have resulted in run-out or failure of the recirculation pumps during the first six hours of recirculation. During this time, both recirculation pumps are operated as directed by the Emergency Operating Instructions (EOIs). Even considering the single failures, their capacity exceeds that of the running refueling water and charging pumps, even considering the single failures.

During the initial six hour recirculation period, failure of CV-517 or CV-518 in the open position could have resulted in run-out of a refueling water pump. Within a few minutes the affected pump motor would have tripped due to excessive power demand. The standby pump would have been started by the operators and within a few minutes would also have tripped. The first pump would then have been restarted by the operators. This sequence of alternating pumps would have continued until the operators could have diagnosed the valve failure and closed an alternate isolation valve. As such, containment spray flow would have continued throughout the sequence at a rate greater than the minimum required. Some pump degradation ma;y have been possible during the periods

that the pump was operated beyond its design flow condition. However, it is expected the degradation would have been expected to be negligible in the time reasonably postulated for operator action.

After six hours, EOI's would have directed the operator to stop one of the recirculation pumps. If one of these single failures had occurred at that time, it could have caused recirculation and/or refueling water pump run-out. However, EOI SO1-1.0-25, "Loss of Recirculation Flow," would have provided guidance for the operator to mitigate loss of recirculation flow. This procedure would have been followed if a recirculation pump were to have tripped, or if recirculation flow had been unstable. The procedure would have required the operators to perform a series of specific checks to verify system alignment. These specific checks include verifying that the spray flow limiting valves are closed and that charging flow is properly adjusted through each injection line. The operators would have been directed to stop both the charging pumps and refueling water pumps, if necessary, to protect the pumps while proper alignment was re-established. It is expected therefore that the control room staff would have monitored plant conditions and would have taken corrective action as procedurally required.

A PRA (attached) was performed to evaluate the impact on core damage frequency of single failure scenarios involving the postulated failing open of FCV-1115D, FCV-1115E, FCV-1115F, CV-517, or CV-518 following a LOCA. The results of the PRA indicate that the probability of core damage resulting from these postulated valve failures is low (1.2E-6), and is only a small fraction of the overall estimated core damage frequency. The likelihood of loss of containment spray leading to containment failure due to spurious opening of CV-517 or CV-518 during the first six hours of recirculation is estimated to be extremely low (4.7E-10 per year).

Based on procedural guidance for responding to loss of recirculation and due to the low probability of core damage from these single failures, this issue has low safety significance.

RESOLUTION

Design modifications and administrative controls were implemented during this outage to ensure that the recirculation and refueling water pumps will not run-out, and that sufficient NPSH is available to the refueling water pumps and charging pumps.

Design Modifications

The recirculation flow control valves, FCV-1115D, E, and F, have been modified to restrict the amount the valves can open. Flow restricting collars will limit flow to within charging pump and recirculation pump capacity if the valves fail open.

The flow restricting orifices in the containment spray lines were resized to limit the flow through the line to within the capacity of a single refueling water pump in the event either CV-517 or CV-518 fails open.

Additional Administrative Controls

The Emergency Operating Instructions were revised to direct the operators to ensure both recirculation pumps are running during recirculation until containment spray is secured. This will preclude run-out of the recirculation pump and/or refueling water pump. Procedure changes were made to require the second charging pump to be locked-out when only one recirculation pump is in operation thus preventing a failure of the standby charging pump if the operating pump fails.

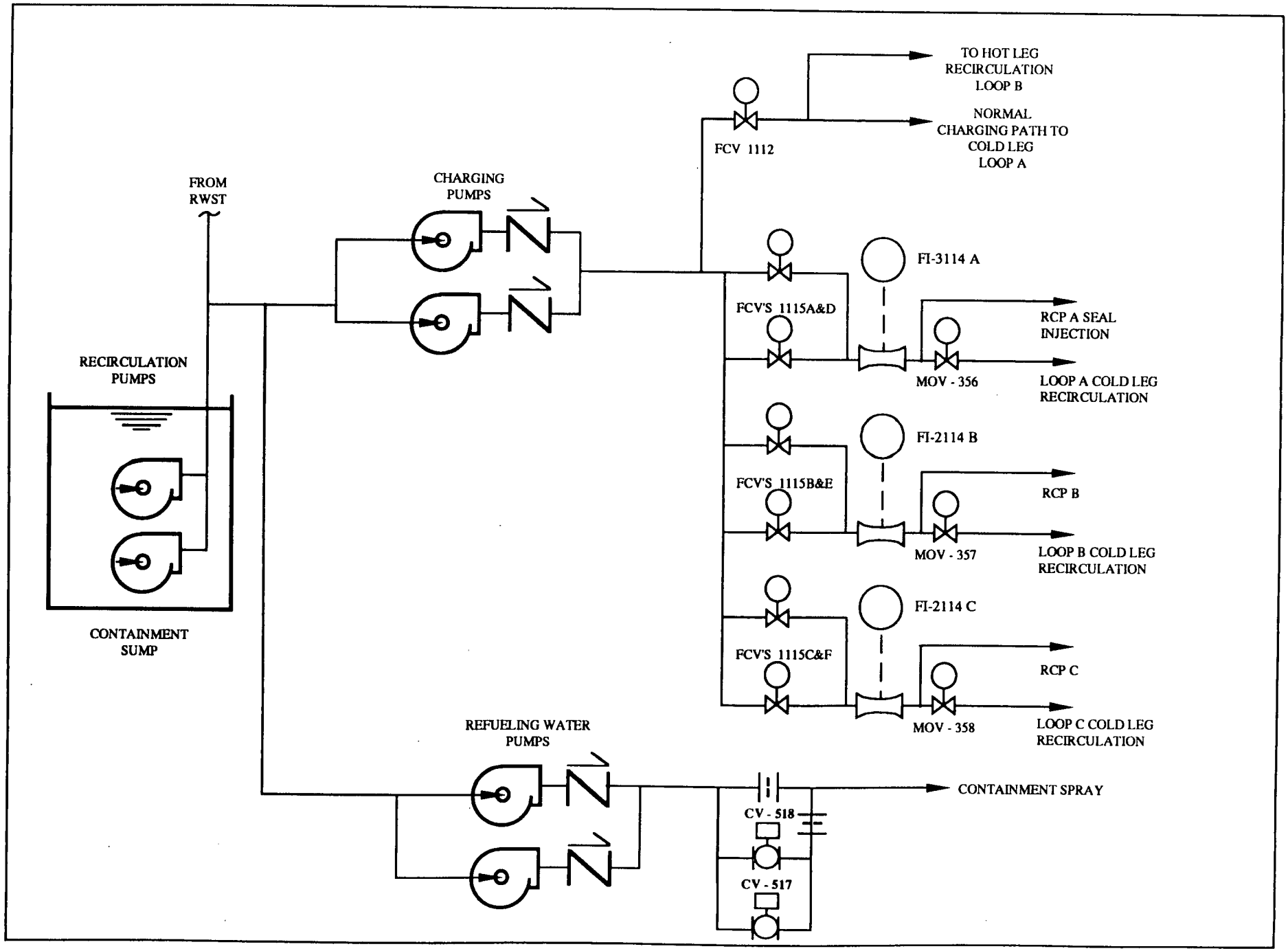


Figure A4. Recirculation System Configuration

PRA FOR LOSS OF PUMPS DURING RECIRCULATION

PURPOSE

The purpose of this analysis is to assess the impact on core damage and containment failure frequency of postulated single failure scenarios concerning failing open of FCV-1115D, E, F or CV-517, 518 following a LOCA.

ASSUMPTIONS

The following assumptions were used in the analysis:

- Once the RWST volume has been depleted, long term recirculation cooling is initiated. For this analysis it is assumed that recirculation is required for a period of 30 days following a LOCA. It is assumed that the charging pump would be damaged with failure of a recirculation flow control valve or the recirculation pump. Upon failure of the first charging pump, the redundant charging pump could automatically start on a low discharge pressure of the first charging pump and could subsequently fail.

- Emergency Operating Procedure SO1-1.0-25 ('Loss of Recirculation Flow') directs the control room crew to carefully monitor the status of the charging and recirculation pumps. If recirculation flow becomes unstable due to excessive flow demands, the required action is to stop both charging and recirculation water pumps and then go through a series of specific checks to verify the system alignment. These specific checks include verifying that the spray flow limiting valves are shut and that charging flow is properly adjusted through each injection line. It is assumed that sufficient time is available for operator action if the valve failure is detected prior to pump failure and procedures to correct a flow problem are followed. The probability that the operators will not detect the failed flow control valve prior to charging pump failure is assumed to be 5E-2, based on engineering judgement.

- If both charging pumps fail, the operators are instructed to utilize the alternate recirculation path via the refueling water pumps. Failure of the alternate recirculation path is assumed to be 0.5 within the first five days of the LOCA and 0.05 thereafter. Higher credit is given to the alternate recirculation path after five days since: (1) the refueling water pump discharge head would be sufficient for recirculation following both small and large break LOCAs after five days and (2) there would be more time available after five days to effect the alternate recirculation flow path lineup before core uncovery.

- The failure of CV-517 or CV-518 to close on demand when required in the EOIs would have been recognized by the operators. The operators were directed in the

EOI "RESPONSE NOT OBTAINED" to locally close the valves. The probability that the operators would have failed to close the failed valve locally requires omission of a procedure step in an EOI, which has a probability of 3E-3 per NUREG/CR-1278.

- The spurious opening of CV-517 or CV-518 would have only been possible from shorting of the control handswitch or mechanical failure of the valve integrity. The likelihood of this failure mode is so low that it is not reported in generic failure rate databases (NUREG/CR-2728, IEEE Std. 500-1984). Therefore, the failure rate for motor-operated valve fails to remain open, 1E-7 /hr from NUREG/CR-2728, is used for conservatism. Operator recovery from spurious opening is not assumed since the operator may have a limited time to diagnose the problem before recirculation pump failure.

- The spurious opening of CV-517 or CV-518 during the first six hours of the recirculation phase could have resulted in runout and trip of the operating Refueling Water Pump within approximately eight minutes. The operators would have likely started the second Refueling Water Pump to maintain containment spray operation. The second Refueling Water Pump could have also tripped within another eight minutes on motor overload. The operators probably would have attempted restart of the first Refueling Water Pump to maintain containment spray operation. While the pumps' impeller and housing subcomponents would not have been expected to have been significantly affected by the runout condition, the restart of a hot, recently tripped motor may have eventually led to motor damage. It is assumed that if the operators did not close CV-517 or CV-518 within 30 minutes, the Refueling Water Pumps would have been damaged. The likelihood of operator failure to diagnose the opening of CV-517 or CV-518 and locally close the valve within 30 minutes is conservatively assumed to be 0.1.

ANALYSIS

The frequency of core damage and containment failure resulting from the failure of recirculation due to flow control valve failures, F(CD), is calculated by solving the following equation:

F(CD) = F(LOCA) *

{[P(FCV FAILS OPEN) + P(RECIRC PUMP FAILS)] *
P(NO RECOVERY OF FCV BY OPERATORS)*
P(ALT. RECIRCULATION FAILS)} +

{[P(EITHER CV FAILS TO CLOSE) *
P(NO RECOVERY OF CV BY OPERATORS)] +

[P(EITHER CV SPURIOUSLY OPENS) *
(MISSION TIME)]}

where:

F(LOCA) = small and large LOCA frequency
= 3.9E-3 per year (NSAC/60, Oconee PRA)

P(FCV FAILS OPEN) = FCV FAILURE RATE * MISSION TIME
= 3E-7 per hour * 3 valves * 30 days
* 24 hours/day (failure rate taken from IEEE Std.500-1984, pg. 487)
= 6.5E-4

P(RECIRC PUMP FAILS) = RECIRC PUMP FAILURE RATE * MISSION TIME
= 3E-5 per hour * 30 days * 24 hours/day (failure rate taken from NUREG/CR-2728)
= 2.2E-2

P(NO RECOVERY OF FCV BY OPERATORS) = 5E-2 (as indicated above)

P(ALT RECIRC FAILS) = 0.5 (as assumed above)

P(EITHER FCV FAILS OPEN) = CV FAILURE TO OPERATE PROBABILITY
= 2 * 3E-3 / demand (failure rate taken from NUREG/CR-2728 for air operated valve)
= 6E-3 / demand

P(NO RECOVERY OF CV BY OPERATORS) = 3E-3 (as indicated above)

P(EITHER CV SPURIOUSLY OPENS) = 2 * 1E-7 / hr (as indicated above)
= 2E-7 / hr

MISSION TIME = 30 days * 24 hrs / day = 720 hrs

Thus, F(CD) = 3.9E-3 per year * {[6.5E-4 + 2.2E-2] * 5E-2 * [(0.5 * 5/30) + (0.05 * 25/30)]} + {[6E-3 * 3E-3] + [2E-7 * 720]}
= 1.2E-6 per year

The likelihood of containment failure given the spurious opening of CV-517 or CV-518 in the first six hours of the recirculation phase, F(CF), is calculated by solving the following equation:

F(CF) = F(LOCA) *
P(EITHER CV SPURIOUSLY OPENS) *
(MISSION TIME) *
P(NO RECOVERY OF SPURIOUS CV OPEN BY OPERATORS WITHIN 30 MINUTES)

where:

P(NO RECOVERY OF SPURIOUS CV OPEN BY OPERATORS WITHIN 30 MINUTES) = 1E-1 (see above assumption)

Thus, F(CF) = 3.9E-3 per year * 2E-7 * 6 * 1E-1
= 4.7E-10 per year

CONCLUSIONS

The probabilistic evaluation indicates the likelihood of core damage and containment failure resulting from flow control valve failures in the recirculation system is low (1.2E-6) and a small fraction of the overall estimated core damage frequency. The likelihood of containment spray failure leading to containment failure due to the spurious opening of CV-517 or CV-518 during the first six hours of recirculation is estimated to be insignificant (4.7E-10 per year).

A5. SPURIOUS ACTUATION OF RECIRCULATION PUMP DISCHARGE VALVES

INTRODUCTION

A spurious actuation of either recirculation pump discharge valve shortly before or during the initial phase of a Loss of Coolant Accident or Main Steam Line Break could have resulted in failure of the charging pumps, and containment spray. However, the operators had the means to detect this condition under most circumstances and take necessary corrective action. A modification was made to lock-out the power to these valves so that a spurious actuation cannot occur.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the Refueling Water Storage Tank (RWST) to the Reactor Coolant System (RCS) and the Containment Spray System (CSS). After the RWST inventory has been depleted, recirculation is initiated to utilize the water which accumulates in the containment sump for containment spray and long-term cooling.

Two recirculation pumps supply a common suction header to the refueling water pumps (for containment spray) and charging pumps (for recirculation) as shown in Figure A5-1. The recirculation pumps and refueling water pumps may also be aligned for secondary recirculation to the steam generators. Secondary recirculation is a back-up means of removing decay heat if a Main Steam Line Break (MSLB) inside the containment disabled the Residual Heat Removal System (RHR). As shown in Figure A5-2 during secondary recirculation, the flow from the recirculation pumps would be directed through the refueling water pumps to the RWST for cooling the RCS via the steam generators.

As shown in Figure A5-1, there is a check valve (CRS-301) in the supply line from the RWST to the common containment spray and charging pump header. This valve is open during safety injection while water from the RSWT is flowing to the containment spray and charging pump suction lines. During recirculation, flow from the recirculation water pumps closes the check valve to prevent flow from the containment into the RWST.

Each of the two recirculation pumps has a motor-operated discharge isolation valve, MOV-866A and MOV-866B. Permanently open vents, each with a flow restricting orifice, are located upstream of the discharge valves. During normal operation, the recirculation pump discharge valves are closed and the upstream piping and pumps are dry. Prior to initiating recirculation, the pumps are operated for a minimum two minutes with the discharge valves closed. The vents are sized to allow accumulated air or steam to be purged through the vents without damaging the pumps. After the lines are cleared, the discharge valves are opened to start recirculation.

SINGLE FAILURE

The spurious opening of either recirculation pump discharge valve, just prior to or during the injection phase of a LOCA or MSLB, could have allowed air or steam into the common suction line of the charging pumps and refueling water pumps. It is likely that the operators would have taken corrective action, if this had occurred. However, if not corrected, the condition would have resulted in the failure the charging pumps, due to gas binding, and may have temporarily blocked containment spray.

SAFETY SIGNIFICANCE

This potential single failure has been eliminated with the plant modification discussed in the Resolution Section below. The safety significance of the condition which existed prior to those modifications is evaluated below. The evaluation concluded that this issue has low safety significance because it is likely operator action would have detected this condition and corrective action would have been taken. If the condition had not been detected, the result would have been a failure of the charging pumps, and a temporary blockage of containment spray. However, this scenario requires a specific sequence of low probability events to result in actual equipment failure. Entrained air/steam in the line would be expected to cause the charging pumps to fail before the refueling water pumps, since the refueling water pumps are of a single stage, durable design.

Spurious Actuation During Normal Operation

If the recirculation pump discharge valves were to have spuriously opened under normal operating conditions, the operators would have had the opportunity to detect the incorrect valve position. The operators verify valve position indication once per shift. Therefore the incorrect position of these valves would probably have been detected within one shift. In addition to direct observation of the valve indication, there would have been a noticeable affect on the RSWT (level decrease) and sump (level increase).

Because of the elevation difference between the RWST and the suction piping, water from the RWST would have flowed through the line towards the recirculation pumps. Check valves on the pumps block flow through the pumps to the containment sump. However the permanently open vents, upstream of the discharge valves, are located such that there would have been flow from the RWST into the sump. The change in water level in the RWST and sump would have been indicated on the associated level instrumentation and would have eventually caused alarms in the control room.

Therefore, opening of the valves during normal plant operation would have been detected.

Spurious Actuation During Safety Injection

If the recirculation pump discharge valves would have opened just prior to an accident, or during injection, the operators may not have had the opportunity to review the control board and detect the condition. Depending on the conditions inside containment, air or steam could have become entrained in the common suction line to the refueling water pumps and charging pumps. With sufficient containment pressure, this condition could have closed the RWST check valve, and blocked containment spray and charging flow. This could have led to a failure of both charging pumps. However, the operators monitor the injection flow, and verify the containment spray system is functional during an accident. Therefore, operator action could have been expected to detect the condition before it led to equipment failure or loss of recirculation, or containment spray.

Only one of two charging pumps would have been affected by the single failure. One charging pump is operated during the injection phase, and one is reserved for use during recirculation. The safety injection signal trips one of the two charging pumps and prevents it from automatically restarting, thereby ensuring the remaining pump it is not started if the operating pump fails. Since charging is not required for injection, the operators are directed to reserve the remaining pump for the recirculation phase. As a result, it would have been unlikely for operators to start the pump during the injection phase.

Spurious Actuation During Recirculation

In the recirculation phase, the safety injection signal would have been reset. The second charging pump could have automatically started if the operating pump were to fail. However, the failure of the operating pump would have alerted the operators to closely monitor the operation of the remaining charging pump. Therefore, it is unlikely this condition would have continued long enough for both pumps to have failed.

A PRA (attached) was completed to evaluate the probability of core damage due to this scenario. The contribution to overall core damage frequency of these events was estimated to be about 9E-8 per year. This is less than 0.05% of the estimated total core damage probability (2E-4 per year). Since this event had a low contribution to plant risk, the safety significance of this single failure is low.

RESOLUTION

A second contactor and pushbutton for each of the recirculation pump discharge valves (MOV-866A and B) was installed during this outage to provide a power lockout for the valves. This modification ensures the recirculation pump discharge valves cannot spuriously open due to a single failure.

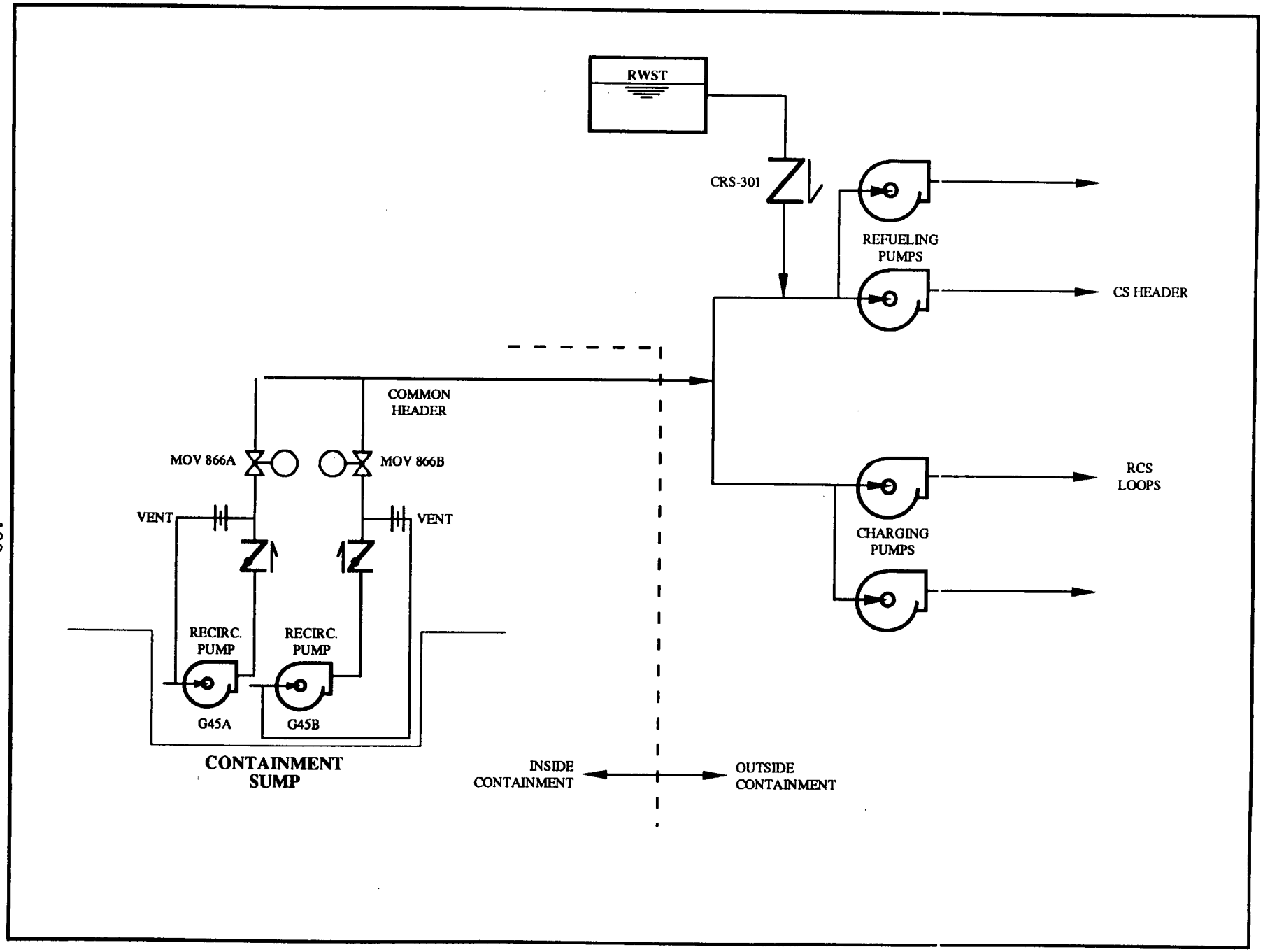


Figure A5-1. Recirculation System

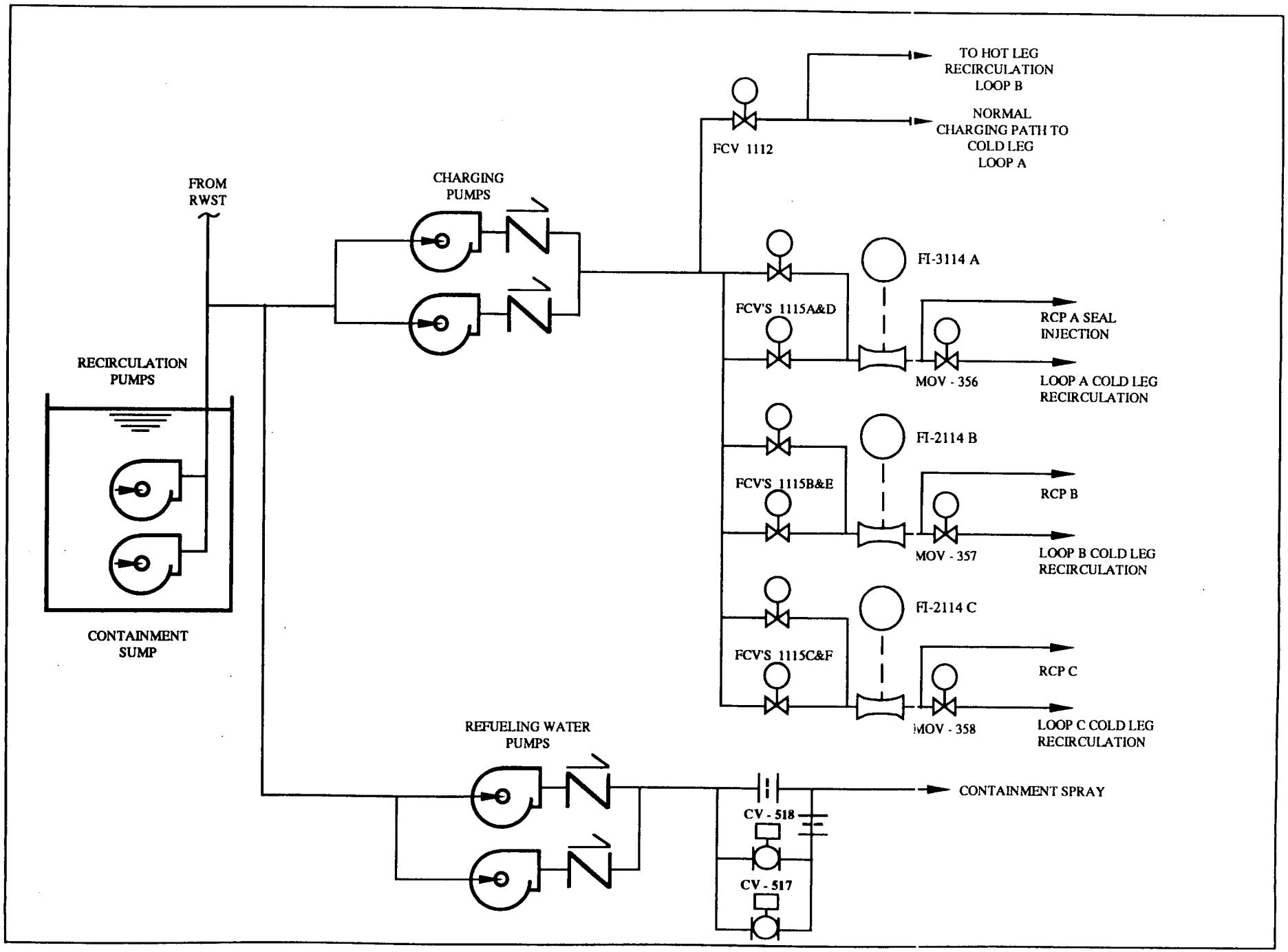


Figure A5-2. Recirculation System Configuration

PRA FOR SPURIOUS ACTUATION OF RECIRCULATION PUMP DISCHARGE VALVES

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of postulated single failure scenarios concerning the recirculation pump discharge isolation valves, MOV-866A and MOV-866B.

ANALYSIS

Assumptions:

- The spurious opening of MOV-866A or B can occur from the following: (1) electric failure resulting in motor-operator actuation, (2) mechanical failure of the valve structure, or (3) operator error in selecting a valve resulting in opening of MOV-866A or B.

  The inadvertent operation of a component by an operator is termed an error of commission in human reliability analysis. Operator errors of commission are not typically included in PRA analyses since their quantification is difficult and there are a large number of unintentional operators errors that could be postulated. Except for specific errors of commission that have been observed to occur in past operation and affect accident initiation or mitigation, errors of commission are not included in PRA analyses. Furthermore, there are no human reliability analysis methods which attempt to predict the likelihood of errors of commission (Reference: NUREG/CR-1278, "Handbook for Human Reliability Analysis"). Therefore, the inadvertent operator actuation of MOV-866A or B is not considered quantitatively in the PRA.

- Operator actions to recover from this failure are conservatively assumed to be unsuccessful. Switchover to the recirculation system is assumed to occur six hours after the LOCA. (Large break LOCAs require switchover in as little as ten minutes). The spurious closure of the MOV-866A or B prior to a LOCA would have been noted by the operators at a shift change when the control boards were reviewed. The average time prior to a LOCA that the incorrect position of MOV-866A or B could have existed is assumed to be four hours (i.e., half of the shift duration). Since MOV-866A and B are opened after switchover to recirculation, the average time the valves could have spuriously opened and caused recirculation failure is ten hours (6 hours + 4 Hours).

The probability of this scenario, which is assumed to lead to core damage, can be calculated as follows:

P(CD) = P(SMALL OR LARGE LOCA) * P(866A or 866B opening spuriously)

The probability of a SMALL OR LARGE BREAK LOCA is 3.9E-3 per year (NSAC/60, Oconee PRA).

From the IREP Procedures Guide (NUREG/CR-2728), the likelihood of a MOV spuriously opening is estimated at 1E-7/hr and the likelihood of a switch or electric circuit failure at 1E-6/hr. Over the ten hour window of concern, the likelihood of mechanical failure is 6E-7 and the likelihood of electrical failure is 6E-6.

The probability of core damage from this sequence can then be calculated as follows:

P(CD) = 3.9E-3/yr * 2 valves * [(1E-7 * 10 hours)+ (1E-6 * 6 hours)]
= 8.6E-8/year

CONCLUSIONS

The likelihood of occurrence of core damage from this scenario is low. This contribution (8.6E-8 per year) to the overall core damage frequency, estimated to be 2E-4 per year, is low, and accounts for less than 0.05% of the total.

A6. CHARGING PUMPS SUCTION LOSS PRIOR TO SAFETY INJECTION SIGNAL

INTRODUCTION

A failure of the Volume Control Tank (VCT) isolation valve or level controller prior to a Safety Injection Signal (SIS), could have caused a loss of suction to the charging pumps. However, this single failure would have been mitigated by either operator action, or actuation of back-up components. Modifications have been made to install redundant components, and upgrade existing equipment to eliminate this potential single failure.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the Refueling Water Storage Tank (RWST) to the Reactor Coolant System (RCS) and the Containment Spray System (CSS). After the RWST inventory has been depleted, recirculation is initiated to utilize the water which accumulates in the containment sump for containment spray and long-term cooling.

The VCT and the RWST supply water to the charging pumps. One charging pump normally operates continuously to supply make-up water to the Reactor Coolant System (RCS) from the VCT. The other charging pump is placed in the standby mode to start automatically on a low charging pump discharge pressure to backup the operating pump. In the event of a safety injection, one charging pump operates, and the SIS prevents the other pump from automatically operating until the SIS has been reset. This lock-out ensures the remaining charging pump does not auto-start to ensure that it will be available when required for post-accident mitigation.

As shown in Figure A6, there were two safety related charging pump suction isolation valves for the RWST, MOV-1100B and MOV-1100D, and one for the VCT, MOV-1100C (note that MOV-1100E was added during the Cycle 11 refueling outage). In addition to providing a signal to control the VCT level, the VCT level controller provided a low-low level signal (20%) to close MOV-1100C, and a low-low-low level signal (10%) to trip charging pump G-8A (the other charging pump did not receive a VCT associated trip signal).

A hydrogen gas blanket, normally between 18-22 psig, is maintained in the VCT for chemistry control. It is necessary for MOV-1100C to close before the VCT is empty to prevent entrainment of gas in the suction of the charging pumps. On a low-low VCT level, MOV-1100C received a signal to close, and the RWST suction valves would have opened. MOV-1100C was interlocked to close after either MOV-1100B or D had opened.

An alternate supply from the RWST to the charging pumps is also available through FCV-5051. Valve FCV-5051 was installed in parallel with MOV-1100B and MOV-1100D to comply with Appendix R (Fire Protection) requirements for safe shutdown. Valve FCV-5051 opens automatically on low charging pump suction pressure.

SINGLE FAILURE

Normally, this single failure issue would not result in a loss of charging pump suction, since it would be mitigated by operator action, and operation of back-up components. During a small break LOCA, the pressurizer level may decrease slowly and allow the charging system to empty the VCT before a SIS is initiated. If the SIS occurred before the VCT was empty, the SIS would close MOV-1100C, and open the RWST suction valves to preclude damage to the charging pumps. The SIS would also lock-out one charging pump to prevent it from automatically starting. If the VCT emptied before the SIS, and the mitigating actions were not successful, these failures would have led to a loss of recirculation flow.

The following single failures could have caused a loss of suction to the charging pumps, prior to the SIS:

Failure to Isolate Empty VCT

1. The VCT level controller failed to initiate a low-low level signal to close MOV-1100C, or

2. VCT isolation valve MOV-1100C failed to close upon receipt of a low-low level signal.

Spurious Isolation of VCT

If MOV-1100C were to spuriously close, there would not have been a signal generated to open the charging pump RWST suction valves, MOV-1100B and D. However, FCV-5051 would have been expected to open on low charging pump suction pressure to provide a suction supply from the RWST. This would not have been a concern during a large break LOCA, as the SIS would provide a signal to open the valves from the RWST.

SAFETY SIGNIFICANCE

These single failures have been resolved with plant modifications discussed in the Resolution Section below. The safety significance of the condition which existed prior to these modifications is discussed below. The evaluation concluded that the safety significance is low because these single failures would have been mitigated by operator action and operation of back-up components.

Failure to Isolate Empty VCT

Failure to isolate an empty VCT could have led to a loss of charging pump suction, if the mitigating actions were unsuccessful. The single failure of the VCT level controller could have resulted in MOV-1100C not closing when required on a low-low VCT level. This would have had the same result as a single failure of MOV-1100C to close. Either event could have caused entrainment of the VCT hydrogen gas blanket in the charging pump suction. This would have caused the operating charging pump to fail, followed by the failure of the second pump when it automatically started. However, operator action would have likely mitigated either event, since the low VCT level would have caused an alarm in the control room. The VCT level alarm is independent of the level controller and would not have been affected by a failure of the level controller, or MOV-1100C. Therefore, it is likely the operators would have taken action to stop the charging pumps, or align the RWST to the pump suction before damage had occurred.

Spurious Isolation of VCT

A spurious isolation of the VCT would have led to a loss of charging pump suction, if the back-up components did not operate as expected. If the VCT isolation valve (MOV-1100C) had spuriously closed, there would not have been a signal generated to open the RWST charging pump suction valves (MOV-1100B and D). The RWST suction valves would have been opened by a SIS. If this had occurred before the SIS, the charging pumps would have been supplied from the RWST through valve FCV-5051. This valve was installed to meet 10 CFR 50 Appendix R fire protection requirements, and would have opened automatically on low charging pump suction pressure to align the RWST to the charging pumps. Although this valve was not considered to be safety related, the valve would have been expected to operate because it was designed, purchased, and installed to safety related standards (except for some of the back-up air system components, which were upgraded during Cycle 11).

When FCV-5051 opens, an audible alarm and indicator light actuate in the control room. FCV-5051 has a back-up air accumulator tank, sized to provide a minimum of thirty minutes of air pressure to maintain the valve open following a loss of the instrument air system. This allows sufficient time for the operators to manually open MOV 1100B and/or D. Therefore, a single failure of MOV-1100C, or the associated circuitry, would not have been expected to cause a failure of the charging pumps.

A PRA (Attached) determined that the frequency of core damage for these scenarios is less than 6E-7 per year. This represents a low safety significance since it is a small fraction (0.3%) of the overall plant risk (2E-4/year). These single failures had a low safety significance, since mitigating actions, and back-up components were available.

RESOLUTION

The following corrective actions to eliminate this single failure have been taken during this outage:

- To prevent autostart and failure of the second charging pump, a second low-low-low VCT level trip has been added. This modification ensures that each train of charging has a separate trip.

- A new charging pump suction isolation valve (MOV-1100E) was added in series with MOV-1100C (Figure A6). Train separation was provided by pairing MOV-1100E with MOV-1100B, and MOV-1100C with MOV-1000D. Each pair of valves has a separate level controller and is powered by separate electrical divisions. Operation of either train of valves will ensure that the charging pumps are aligned to either the VCT or RWST.

- The air supply components for alternate charging pump suction isolation valve FCV-5051 were upgraded and the valve has been re-classified as safety related.

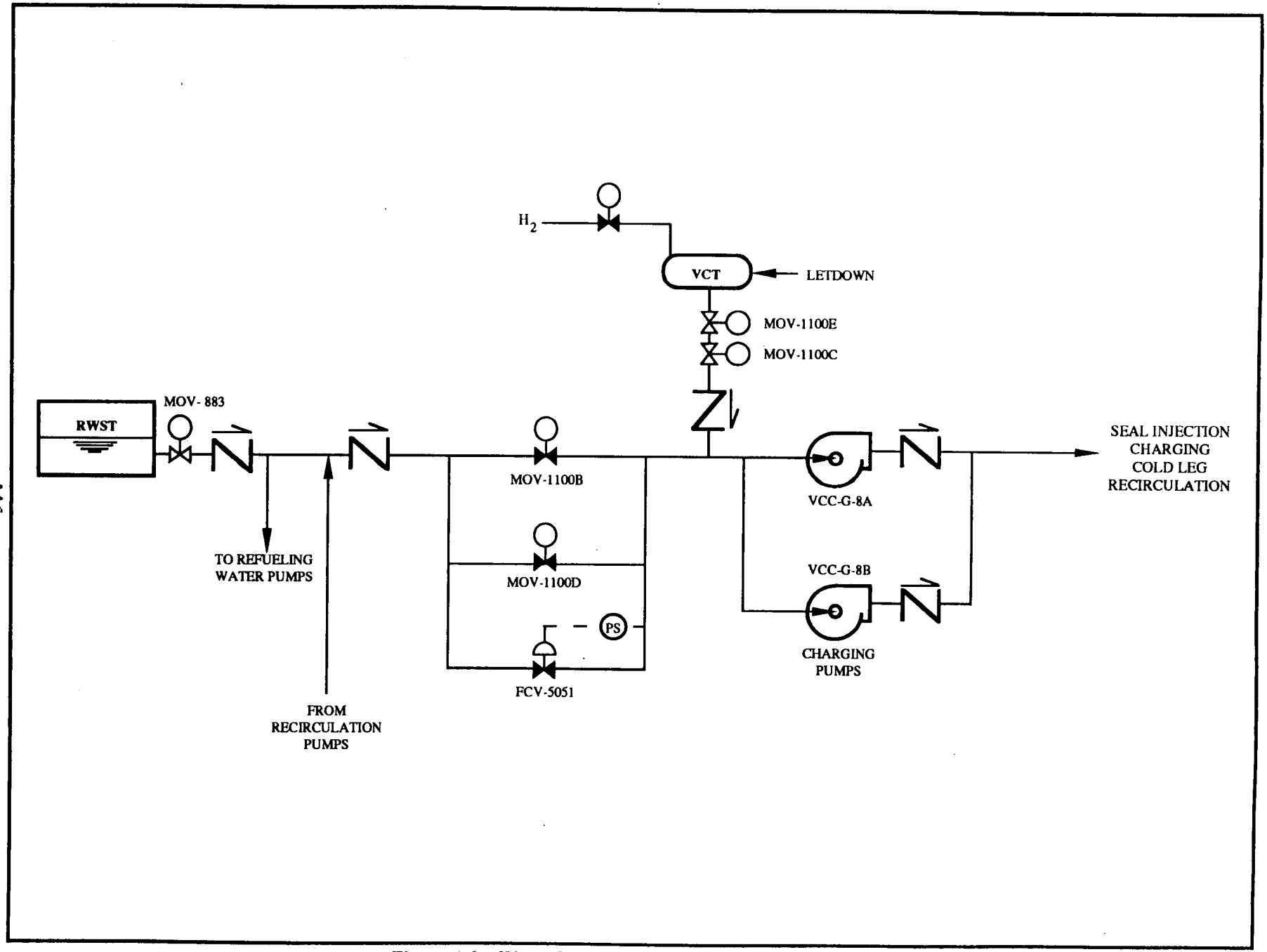


Figure A6. Water Supply for Charging Pumps

PRA FOR MISOPERATION OF THE VCT ISOLATION VALVE OR LEVEL CONTROLLER

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of postulated failures of the Volume Control Tank (VCT) level controller and isolation valve.

ANALYSIS

Scenario 1

For failures of MOV-1100C to close, the scenarios of concern are conservatively assumed to be both small and large break LOCAs. Only one single failure is assumed at a time; either the level controller fails and MOV-1100C would close on receipt of a SIS, or the level controller functions and MOV-1100C fails to close. Additionally, if MOV-1100C is the single failure, then the SIS signal would be assumed to lock-out one charging pump, thereby preventing a common cause failure of the two pumps due to gas binding.

Should the VCT level drop below 30%, a control room alarm is initiated from a diverse instrument, LC-1100D. The alarm would have alerted the operators to potential gas binding of the charging pumps. The alarm would be particularly effective in the case of MOV-1100C failing to close, since both level instruments would indicate low at the time of the alarm. In addition, charging pump G-8A would be tripped on low-low-low VCT level by the level controller. The probability of core damage due to VCT level controller failure to detect low level can be calculated as follows:

P(small or large LOCA) * [P(level controller failure) + P(low-low level trip failure)] * P(No operator action given alarm) * P(Failure of alternate recirculation)

The probability of a small or large break LOCA is estimated to be 3.9E-3 per year (NSAC/60, Oconee PRA). From the IREP Procedures Guide (NUREG/CR-2728), the likelihood of an instrument failure such as a level controller is 1E-6 per hour. If it is conservatively assumed that a level controller could be failed for up to eight hours (four hours prior to the LOCA and four hours during the LOCA), then the failure probability is calculated to be 8E-6. Operation of the level controller would have been noted during normal operation at least every shift change by makeup and depletion of the VCT. The probability of failure of the low-low level trip component (LC-1100BX) to close MOV-1100C, is assumed to be 3E-4 per demand (NUREG/CR-2728), since its design resembles a relay. It is conservatively assumed that there is a 0.1 likelihood of unsuccessful operator action to prevent charging pump failure. Failure of the alternate recirculation path (through the refueling water pumps) is assumed to be 0.5. This estimate is conservative, since the alternate path is specifically addressed in the EOIs, and would not be affected by a failure of the charging pumps.

Therefore, the likelihood of core damage is calculated as follows:

$$3.9E\text{-}3/yr * (8E\text{-}6 + 3E\text{-}4) * 0.1 * 0.5 = 6.0E\text{-}8/year$$

The probability of core damage due to MOV-1100C failure to close can be calculated as follows:

P(LOCA) * P(MOV failure) * P(No operator action given alarm) * P(Failure of alternate recirculation)

From the IREP Procedures Guide, the failure probability of a MOV is 3E-3 per demand. Therefore the probability of core damage due to this scenario is calculated as follows:

$$3.9E\text{-}3/yr * 3E\text{-}3 * 0.1 * 0.5 = 5.8E\text{-}7/year$$

Scenario 2

For spurious failures of MOV-1100C to remain open, the scenarios of concern are LOCAs. The probability of charging pump damage due to this scenario is calculated as follows:

P(LOCA) * P(MOV closure) * P(FCV-5051 failure to open)

From the IREP Procedures Guide, the likelihood of spurious MOV closure is 1E-7/hour. If the period of concern post-LOCA is assumed to be 4 hours, then the likelihood of MOV closure is 4E-7. FCV-5051 was not considered to be entirely safety-related, prior to the Cycle 11 refueling outage. Therefore, it will be conservatively assumed that its failure likelihood was 0.01. (The recommended failure probability for a valve of this type would be on the order of 0.001).

Therefore, the likelihood of this scenario is calculated as follows:

$$3.9E\text{-}3/yr * 4E\text{-}7 * 0.01 = 1.56E\text{-}11/yr$$

The likelihood of core damage is expected to be several orders of magnitude less.

CONCLUSIONS

The probabilistic risk assessment indicates that the likelihood of these scenarios is low. The contribution from all of the scenarios to overall core damage (estimated to be approximately 2E-4 per year), is low accounting for less than 0.3% of the total.

A7. LOSS OF VITAL BUSES

INTRODUCTION

A common cause failure of vital bus loads not qualified for a post accident environment could have resulted in the loss of redundant components required for accident mitigation after transfer of Train A vital bus power to the Train B backup power source due to a subsequent single failure of the backup power source. However, since the probability of the postulated scenario is very low, the risk of adverse consequences to plant operation with the existing vital bus configuration is extremely low. Plant modifications to eliminate this single failure susceptibility are scheduled for Cycle 12.

BACKGROUND

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB) the adverse environmental conditions in the area of the pipe break can impact operability of plant components which are not environmentally qualified for these conditions. Vital Buses 1, 2, and 3/3A power redundant safety related components required for accident mitigation. These vital buses also power components which are not environmentally qualified and not required for accident mitigation.

Vital Buses 1, 2, and 3/3A are normally energized by inverters connected to their Train A primary power source, DC Bus 1 as shown in Figure A7. These Train A vital buses are equipped with transfer switches to automatically transfer the vital buses to the backup power source (Train B 480 MCC2) on bus low voltage. The transfer switches for Vital Buses 1, 2, and 3/3A are not designed to automatically retransfer from the backup power source back to the primary power source. This retransfer can be performed manually from the control room.

SINGLE FAILURE

Vital Buses 1, 2, and 3/3A will be able to perform their safety related function, unless a very low probability scenario is postulated to occur. This scenario includes a LOCA or an MSLB which produces an environment which could cause failure of the environmentally unqualified loads on Vital Buses 1, 2, and 3/3A. These vital buses would then transfer to their backup source which is Train B power MCC2. A subsequent single failure of the backup power source including its vital buses could result in loss of all vital bus powered components necessary to mitigate an accident (e.g., no safety injection).

SAFETY SIGNIFICANCE

This single failure scenario will be eliminated during the Cycle 12 refueling outage, as discussed in the Resolution Section below. The safety significance of the conditions which existed prior to these modifications is evaluated below. The evaluation concluded that the safety significance is low since the circumstances leading to core damage are very improbable. The following sequence of events would have to occur in order to lose power to all vital buses:

1. LOCA or MSLB,

2. Multiple short circuiting of unqualified electrical loads on the vital buses leading to automatic transfer to the backup power source, and

3. Random failure of the vital bus backup power source after an automatic transfer.

Past Operation (Prior To Cycle 11)

We have analyzed the safety significance of past plant operation (prior to Cycle 11) with this single failure susceptibility. We performed a Probabalistic Risk Assessment (PRA) and calculated the risk of core damage with this single failure susceptibility to be 8.0E-7 per year of operation. This risk accounts for less than 0.4% of the SONGS 1 overall core damage frequency. Therefore, the risk of adverse consequences from past plant operation with the existing vital bus configuration was extremely low.

Future Operation (During Cycle 11)

We have also analyzed the safety significance of plant operation during Cycle 11. We performed a PRA which reflects the procedures now in place to improve operator response for accident mitigation and calculated the risk of core damage with this single failure susceptibility to be 6.0E-7. Therefore, the risk of adverse consequences from continued plant operation until the modifications scheduled for the Cycle 12 refueling outage are implemented are also insignificant. This PRA was submitted to the NRC by letter dated January 30, 1991, as part of Amendment Application No. 189. This submittal served as the basis of our PRA for past operation discussed above.

RESOLUTION

A plant modification to eliminate the vital bus single failure susceptibility is scheduled for implementation during the Cycle 12 refueling outage. Amendment Application No. 189 has been submitted to obtain NRC concurrence with this proposed schedule. Procedure changes were also implemented to improve operator response to this event, as discussed above.

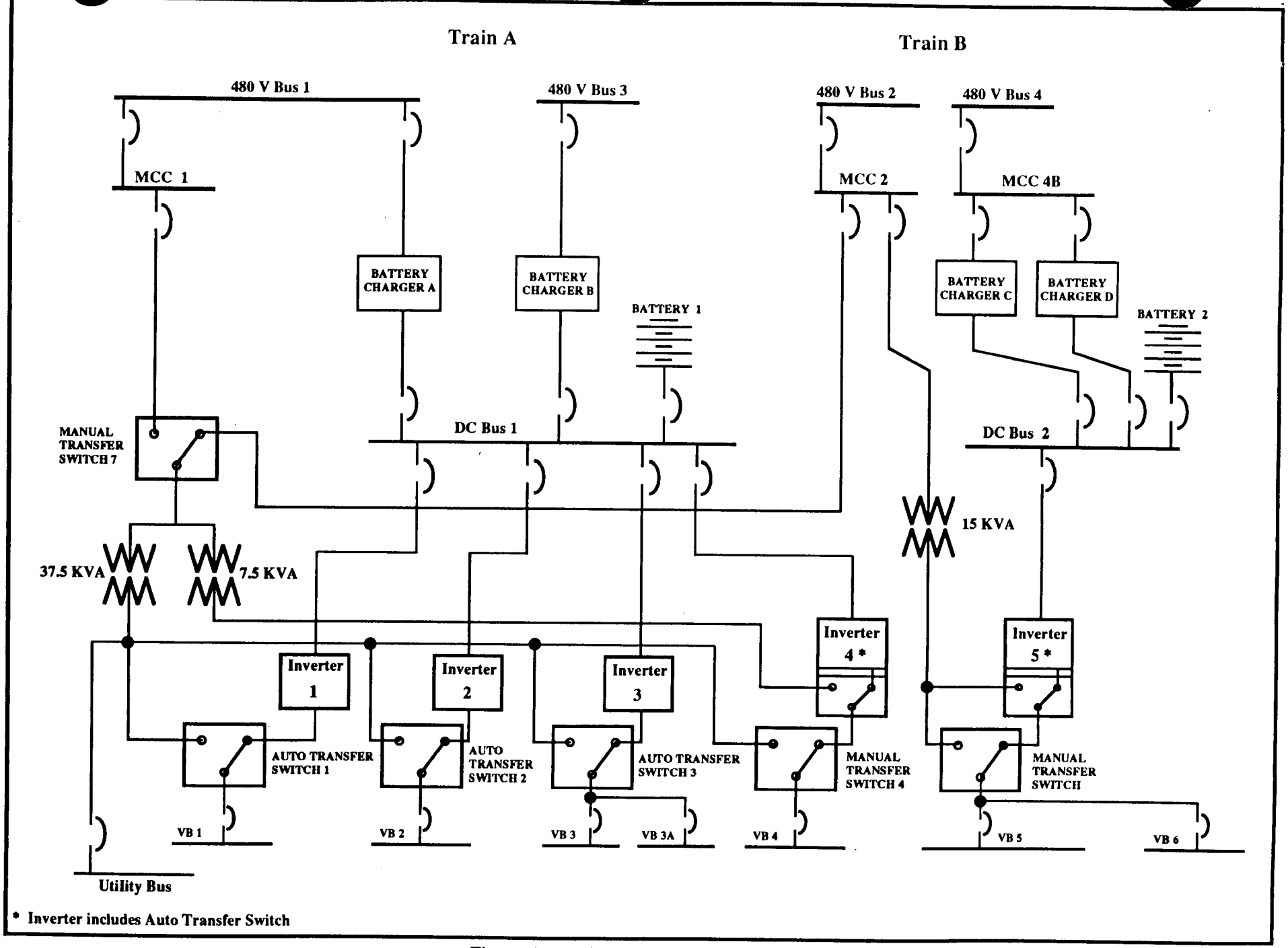


Figure A7. Vital Bus Arrangement

A8. SEQUENCER LOGIC DEFICIENCY

INTRODUCTION

Three separate single failure scenarios affected detection of a loss of off-site power by the Safeguards Load Sequencing System (SLSS). These single failure scenarios could have delayed ECCS initiation longer than currently assumed in the safety analysis and therefore adversely affected core cooling after an accident. However, each of the three scenarios had a low safety significance because of their low contribution to the overall core damage frequency. In addition, plant modifications were completed during this outage to eliminate all three of the single failure susceptibilities.

BACKGROUND

There are two independent safety related 4160 volt electrical distribution buses: 1C and 2C. These buses supply electrical power to systems and components that are required for normal operation, safe shutdown, and mitigation of design basis events. These two electrical distribution systems are normally energized by off-site electrical sources through Auxiliary Transformer C. Figure A8 illustrates normal bus alignments (after completion of modifications to the 480 volt electrical distribution system being implemented during the current outage).

In the event of a loss of off-site power, each of the two 4160 volt distribution systems is powered by an emergency diesel generator. Upon receipt of a Safety Injection Signal (SIS) with loss of both Buses 1C and 2C, the SLSS starts the diesel generators, trips all loads on the buses (including the diesel generator breaker if the diesel was connected to the bus), closes the diesel generator output breakers, and sequences the ECCS loads.

For a SIS without a loss of off-site power, the loads on the buses are not tripped, and additional ECCS loads except the Main Feedwater pumps are loaded at one time. The Main Feedwater pumps have their own time-delay relay controlling their restart. Both diesel generators are automatically started for this case but not loaded. Prior to the plant modification completed during this outage, the diesel generators would also have automatically started but would not have been connected to the buses for a SIS with a coincident loss of a single 4160 volt bus.

SINGLE FAILURES

Three separate low probability single failure scenarios could have delayed actuation of the ECCS longer than assumed in the safety analysis:

Diesel Generator Breaker Failure During Surveillance Testing

During diesel generator surveillance testing, the diesel generator is paralleled to its respective 4160 volt bus. Failure of the diesel generator breaker to trip concurrent with a SIS and loss of off-site power would result in one of the 4160 volt buses remaining energized by the diesel generator. Therefore, the SLSS would not have initially detected the complete loss of off-site power.

The SLSS would attempt to start ECCS loads while maintaining power to the non-essential loads on the bus. This would result in diesel generator overload and a degraded bus voltage condition sufficient to prevent starting of the ECCS loads. The other SLSS would initially sense a SIS and loss of its respective electrical bus, but would not have connected its diesel generator or started the ECCS loads until a loss of off-site power (LOP) occurred when the voltage on the first bus reduced sufficiently for its sequencer to sense low bus voltage (i.e., loss of both buses would then be sensed). This would have delayed ECCS initiation beyond the timing assumed in the safety analysis.

4160 Volt Bus Failure During Ground Fault Detection

During ground fault detection on Bus 1C or 2C, the grounded bus is isolated from Auxiliary Transformer C and is connected to the main generator via Bus 1A or 1B. These buses are not capable of starting ECCS loads. Single failure of the other bus, with or without the loss of off-site power, would have resulted in loss of the ECCS.

A concern related to ground fault detection (which is not a single failure issue) was identified during the single failure analysis. This issue is described below for completeness. ECCS initiation may be delayed if a SIS event occurred coincident with a loss of off-site power during ground fault detection on Bus 1C or 2C. The SLSS initially would not have detected a SIS with loss of off-site power (SISLOP) since there would have been voltage on the bus connected to the main generator. The SIS would result in a turbine trip which would cause the main generator to coast down. The SLSS for the bus transferred from Auxiliary Transformer C (i.e., the bus with the ground) would have detected a SIS only and would have attempted to start ECCS loads while maintaining non-essential loads on the bus. However, this train may not have been able to start all of the ECCS loads because of the reduced bus voltage and frequency. The voltage and frequency reduction would be caused by the non-essential loads and the bus continuing to be energized by the main generator during its coast down rather than from off-site sources. The main generator voltage would eventually decrease sufficiently to result in an undervoltage signal on the bus being tested. The loss of both buses would then have been sensed and the ECCS loads would have been connected and sequenced. This would have delayed ECCS initiation beyond the timing assumed in the safety analysis.

Bus Feeder Breaker Failure During Degraded Grid Condition

Failure of either of the Bus 1C or 2C feeder breakers to open in response to a degraded grid condition concurrent with a SIS could have led to a failure of ECCS loads to properly start.

The bus with the failed breaker would remain connected to the grid in a degraded voltage condition. The SLSS would not have sensed the loss of the bus with the failed breaker and would not have generated a LOP signal since the bus would still have voltage. As a result, the SLSS would have attempted to start the ECCS loads on the bus with the degraded voltage. These loads would not have started in the time required by the safety analysis. The loads on the other bus would not have been started because its feeder breaker would have tripped and its diesel generator would not have been loaded.

SAFETY SIGNIFICANCE

These single failures have been eliminated with the plant modifications and administrative controls discussed in the Resolution Section below. The evaluation concluded past operation with these single failure susceptibilities did not significantly compromise plant safety because of their low contributions to the overall core damage frequency.

The impact on core damage frequency of each of the three single failure scenarios was evaluated in the attached PRA. The evaluation focuses on the effects of a large break LOCA and MSLB since delayed ECCS operation is of greatest significance for these events. Large break LOCAs and MSLBs are of concern because rapid actuation of the Safety Injection System is necessary to avoid core damage. Small break LOCAs and other plant transients are slower to develop and minor time delays in starting and loading safety loads would have a less severe impact. The results of the probabilistic risk assessment are summarized below for each of the three single failure susceptibilities.

SINGLE FAILURE SUSCEPTIBILITY	PROBABILITY OF CORE DAMAGE PER YEAR OF OPERATION	SAFETY SIGNIFICANCE
1. Diesel Generator Breaker Failure During Surveillance Testing	6E-10	Low
2. 4160 Volt Bus Failure During Ground Fault Detection	1E-7	Low
3. Bus Feeder Breaker Failure During Degraded Grid Condition	2E-7	Low

The total probability of any of these three single failure susceptibilities leading to core damage is less than 4E-7 per year of reactor operation. This is less than 0.2% of the SONGS 1 core damage risk. Therefore, because of the low probabilities estimated for the occurrence of core damage and the conservative assumptions made in the PRA, the safety significance of this condition was low.

RESOLUTION

The logic for each SLSS has been modified during this outage to sequence upon a SIS with the loss of the respective 4160 volt bus (rather than a SIS and loss of both buses). In addition, the duration of ground detection activities has been limited to an eight hour period. The SLSS logic change and limitation of the duration of ground fault detection eliminate the potential for these three single failure susceptibilities to delay sensing the loss of off-site power. Therefore, ECCS will be actuated for these three scenarios within the time frame assumed in the safety analysis. Amendment Application No. 189 proposed changes to the SONGS 1 Technical Specifications that are necessary to reflect the SLSS modification.

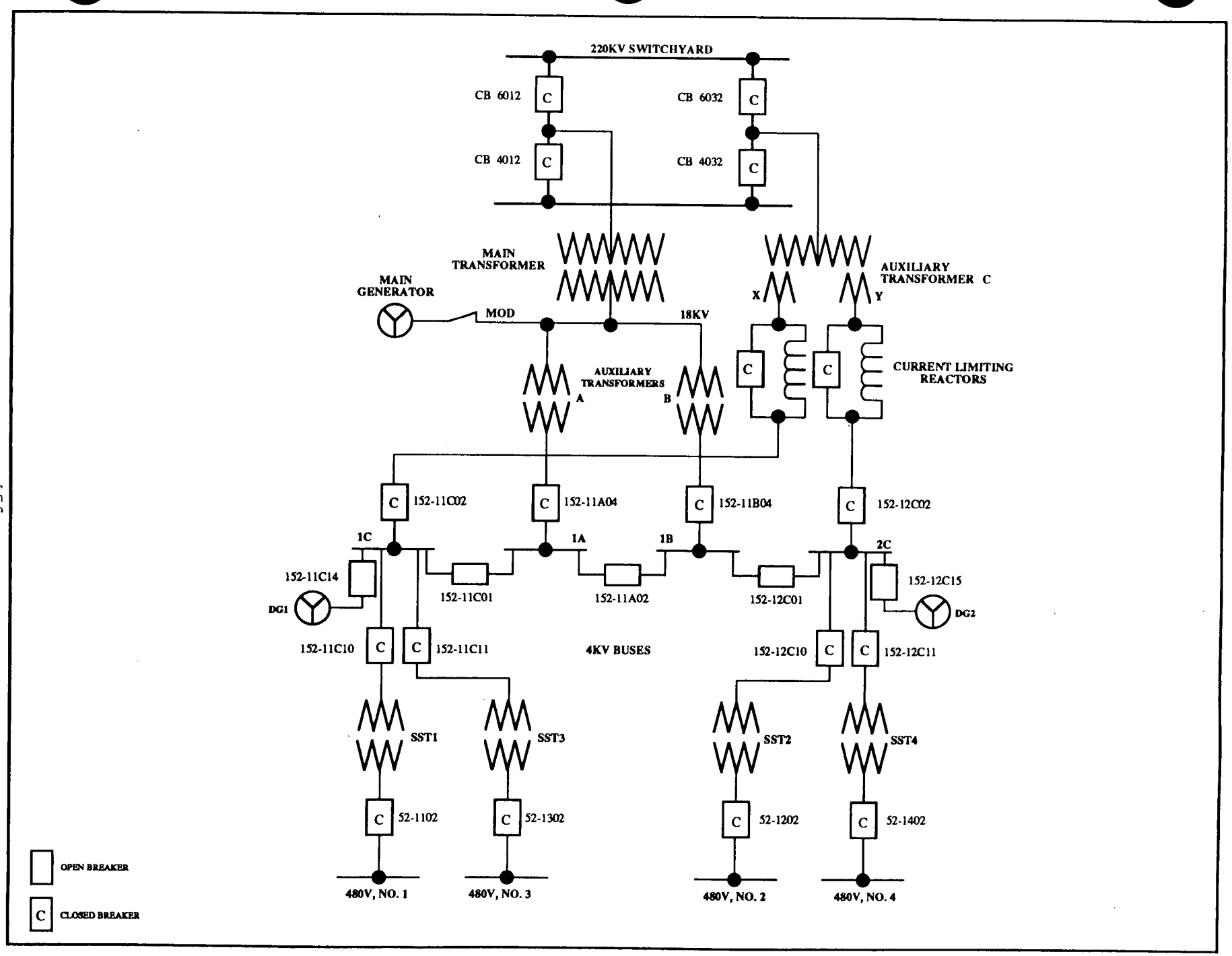


Figure A8. Normal Electrical Bus Arrangement

PRA FOR SEQUENCER LOGIC DEFICIENCIES

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of three single failure susceptibilities concerning the SLSS.

ANALYSIS

Scenario 1, Diesel Generator Surveillance Testing

In order for core damage to occur, the following sequence of events must exist: one of the two diesel generators is undergoing surveillance testing and is connected to the 4160 volt bus; a large break LOCA or MSLB occurs concurrent with a loss of off-site power; and the diesel generator output breaker fails to trip.

From the Oconee PRA (NSAC/60), the frequency of a large LOCA is estimated to be 9.3E-4 per year and the probability of an MSLB is estimated to be 3E-3 per year. A conservative estimate for concurrent loss of off-site power is 1E-3 per turbine trip (WASH-1400). From the Interim Reliability Evaluation Program (IREP) Procedures Guide (NUREG/CR-2728), the probability of a circuit breaker failing to trip on demand is 3E-3.

The two diesels are each tested once per month. The test duration is less than eight hours and the diesel generators are connected to the 4160 volt bus for only a fraction of the testing period (a minimum of one hour). Therefore, we conservatively assumed that a diesel generator is connected to a bus 5% of the time. The probability of occurrence for this scenario is calculated as follows:

$$P(\text{scenario 1}) = (9.3E\text{-}4/\text{yr} + 3E\text{-}3/\text{yr}) * 0.001 * 0.05 * 3E\text{-}3 = 6E\text{-}10/\text{year}$$

Hence, the likelihood of this single failure scenario is negligible.

Scenario 2, Ground Fault Detection

For this plant condition to lead to core damage, a large break LOCA or MSLB must occur while ground fault detection activities are underway with either a concurrent loss of off-site power or the loss of the safety injection train aligned to the other bus. As noted above, the frequency of a large LOCA is estimated to be 9.3E-4 per year, while the probability of a MSLB is approximately 3E-3 per year. The chance of losing off-site power is assumed to be 1E-3 per turbine trip. Failure of a train of safety injection is conservatively estimated to be 3E-2 per demand (SONGS 1 Partial PRA).

In order to determine how frequently Bus 1C and 2C are aligned to the main transformer (via Buses 1A and 1B) during ground fault detection, operations records from early 1982 to the present were reviewed and interviews with operations personnel were conducted. Based upon these reviews, only three instances were identified in which Buses 1C and 2C were connected to the main transformer. In each case, less than ten hours was spent in an alternate alignment during testing. Therefore, we conservatively assumed that the duration of bus realignments does not exceed eight hours per year (i.e., 0.001 likelihood of occurrence).

The probability of this plant condition leading to core damage is calculated below:

$$\begin{aligned} P(\text{scenario 2}) &= (9.3E\text{-}4/yr + 3E\text{-}3/yr) * 0.001 * (0.001 + 0.03) \\ &= 1.2E\text{-}7/year \end{aligned}$$

Hence, the likelihood of this single failure susceptibility is low.

Scenario 3, Bus Feeder Breaker Failure

For this scenario to cause core damage, a large LOCA or MSLB must occur concurrent with a degraded voltage condition, and one of the two 4160 volt bus feeder breakers must fail to open. As noted above, the frequency of a large LOCA is approximately 9.3E-4 per year and the probability of a MSLB is estimated to be 3E-3 per year. The occurrence of a degraded grid voltage condition (less than 70% of normal voltage) is conservatively assumed to be ten times more likely than loss of the grid following the plant trip, or 1E-2 per turbine trip. From the IREP Procedures Guide, the likelihood of a circuit breaker failing to trip is 3E-3 per demand. Since either breaker failing to trip is a concern, the probability of a circuit breaker failure contributing to this scenario is 6E-3.

The probability of this scenario occurring is calculated below:

$$P(\text{scenario 3}) = (9.3E\text{-}4/yr + 3E\text{-}3/yr) * 0.01 * 6E\text{-}3 = 2.4E\text{-}7/year$$

Hence, the likelihood of this single failure scenario is low.

CONCLUSION

The scenarios described above have a minimal impact on total plant risk. Therefore, the existence of these single failure susceptibilities did not significantly compromise plant safety.

A9. SAFETY INJECTION SEQUENCER BLOCK PERMISSIVE FAILURE

INTRODUCTION

A common cause failure due to electrical faults in the safety injection sequencer block permissive circuits could have resulted in the loss of both trains of the Safeguards Load Sequencing System (SLSS) and the inability to block a safety injection signal (SIS) from the control room. If these failures occurred shortly before an accident, they could have prevented automatic initiation of Reactor Coolant System (RCS) cooling and of Containment Spray System (CSS) operation. However, the safety significance of this potential failure was determined to be low. The sequence of events necessary to prevent ECCS initiation was highly unlikely and long term ECCS operation would have been assured by manual operator actions. Plant modifications were completed during this refueling outage to achieve redundancy and physical separation between the two safety injection sequencer block permissive circuits.

BACKGROUND

ECCS Operation

During a Loss of Coolant Accident (LOCA) or a Main Steam Line Break (MSLB), the Emergency Core Cooling System (ECCS) injects borated water from the Refueling Water Storage Tank (RWST) to the Reactor Coolant System (RCS) and the CSS. After the RWST inventory has been depleted, recirculation is initiated to utilize the water which accumulates in the containment sump for containment spray and long term cooling.

For a MSLB, borated water is injected into the RCS for reactivity control, and auxiliary feedwater is pumped to the two available steam generators to provide heat removal. The Residual Heat Removal (RHR) system is normally used to reach cold shutdown. RHR is located inside containment but is not environmentally qualified for post-accident conditions. Long term heat removal for this event is achieved by secondary recirculation through the two available steam generators.

Secondary recirculation after a MSLB is provided by pumping containment sump water to the available steam generators. The recirculation pumps transfer sump water, including spilled secondary side water from the break and containment spray water, to the RWST. Water from the RWST is then pumped into the available steam generators through connections between the Safety Injection System and Main Feedwater System. The flow from the Main Feedwater System to each of the three steam generators is individually balanced by positioning three Feedwater Bypass Control Valves (FBCVs) (see Figure A9). The three FBCVs automatically close upon receipt of a SIS or an Auxiliary Feedwater Actuation Signal (AFWAS) from either train. Both trains of the SIS and AFWAS must be manually reset in the control room before the FBCVs can be

opened for secondary recirculation. The SIS generated by each train of the SLSS is reset by enabling the block switches for the two safety injection sequencer block permissive circuits. The SIS block circuitry for each sequencer has common inputs from the Train A pressurizer pressure logic and relays. After the SIS and AFWAS have been reset, the FBCVs are opened from the control room to allow secondary recirculation. The FBCVs can also be operated locally with handwheels.

SLSS Operation

ECCS operation is automatically initiated in response to an accident by the SLSS based upon the following input signals: 1) low pressurizer pressure or 2) high containment pressure, with or without low voltage on either or both 4160 volt buses 1C and 2C. The SLSS actuates and sequences the various safety related electrical loads in the event of a SIS or SIS with concurrent LOP (SISLOP). The sequencing is designed to ensure timely initiation of safety related loads without causing overloading of the diesel generators.

The SLSS is composed of two redundant sequencer trains. In the event of a SIS, the required ECCS loads are block loaded to the respective buses. On a SIS, the SLSS also automatically starts the diesel generators but does not automatically close the diesel generator output breakers.

SINGLE FAILURE

An unlikely electrical fault scenario associated with the safety injection sequencer block permissive circuits in the control room could have prevented: 1) both trains of the SLSS from generating a SIS in response to an accident and/or 2) the operators from resetting the SIS after a MSLB to allow secondary recirculation RCS cooling. This could have prevented automatic initiation of the ECCS and CSS. Long term ECCS operation could also have been affected.

SAFETY SIGNIFICANCE

This single failure scenario has been eliminated with the plant modification discussed in the Resolution Section below. The safety significance of the condition which existed prior to those modifications is evaluated below. The evaluation concluded that this issue had low safety significance because: 1) the sequence of events necessary to cause core damage had a low probability of occurrence; and 2) alternate means to assure long term RCS cooling existed.

ECCS Initiation

This single failure susceptibility had low safety significance because the following low probability sequence of events would have had to occur to lead to core damage:

- Electrical fault in one of the safety injection sequencer block circuits shortly[1] before an accident,
- Postulated fault generates sufficient heating and/or electrical arching to induce an electrical fault in the other block circuit,
- Block circuit faults result in sufficient current to trip circuit breakers for both sequencers,
- Occurrence of a LOCA, MSLB, or Feedwater Line Break following the electrical fault.

A probabilistic risk assessment (PRA) was performed to evaluate the likelihood of the above scenario (see attachment). The results of that analysis demonstrate this scenario had low safety significance since its core damage frequency was estimated to be 2.4E-7 per year. This is a small fraction (approximately 0.1%) of the plant overall core damage frequency.

Secondary Recirculation After MSLB

Prior to the initiation of secondary recirculation after a MSLB, the RCS is cooled through heat removed by steam generator blowdown through the postulated pipe break and by injection of auxiliary feedwater into the available steam generators. Long term RCS cooling is normally achieved by operation of the RHR system. However, if RHR had been unavailable, secondary recirculation flow for long term RCS cooling would have been initiated through the FBCVs after the auxiliary feedwater storage tank emptied.

The switchover to long term cooling is not required until several hours after the secondary pipe rupture has occurred. Thus, sufficient time would have been available for the operators to open the FBCVs locally by using the valves' manual handwheels. Although the option of using the handwheels was not explicitly identified in Emergency Operating Instruction (EOI) S01-1.0-32, "Loss of Residual Heat Removal Due to Loss of Secondary Coolant in Containment," instructions to ensure that the FBCVs are open were included.

[1] The time period of interest is the sum of the following time intervals: 1) the maximum outage time allowed by the Technical Specifications for the loss of both sequencer block circuits (one hour) and 2) the time necessary to enter Mode 4 (12 hours). The operators would have been alerted to the failure of the sequencer block circuit by the block alarm in the control room.

Therefore, this single failure susceptibility had low safety significance due to: 1) its low contribution to the overall core damage frequency (approximately 0.1%) and 2) adequate time would have been available for the operators to recognize the need to take manual action to assure secondary recirculation cooling after a MSLB.

RESOLUTION

Plant modifications were completed during this outage to achieve redundancy and physical separation between the two safety injection sequencer block permissive circuits. These modifications ensure that a failure in one of these circuits cannot affect the ability of the SLSS to perform its safety function in response to an accident. Additionally, EOI S01-1.0-32 was revised to specifically direct contingent use of local valve manual handwheels to ensure long term RCS cooling after a MSLB.

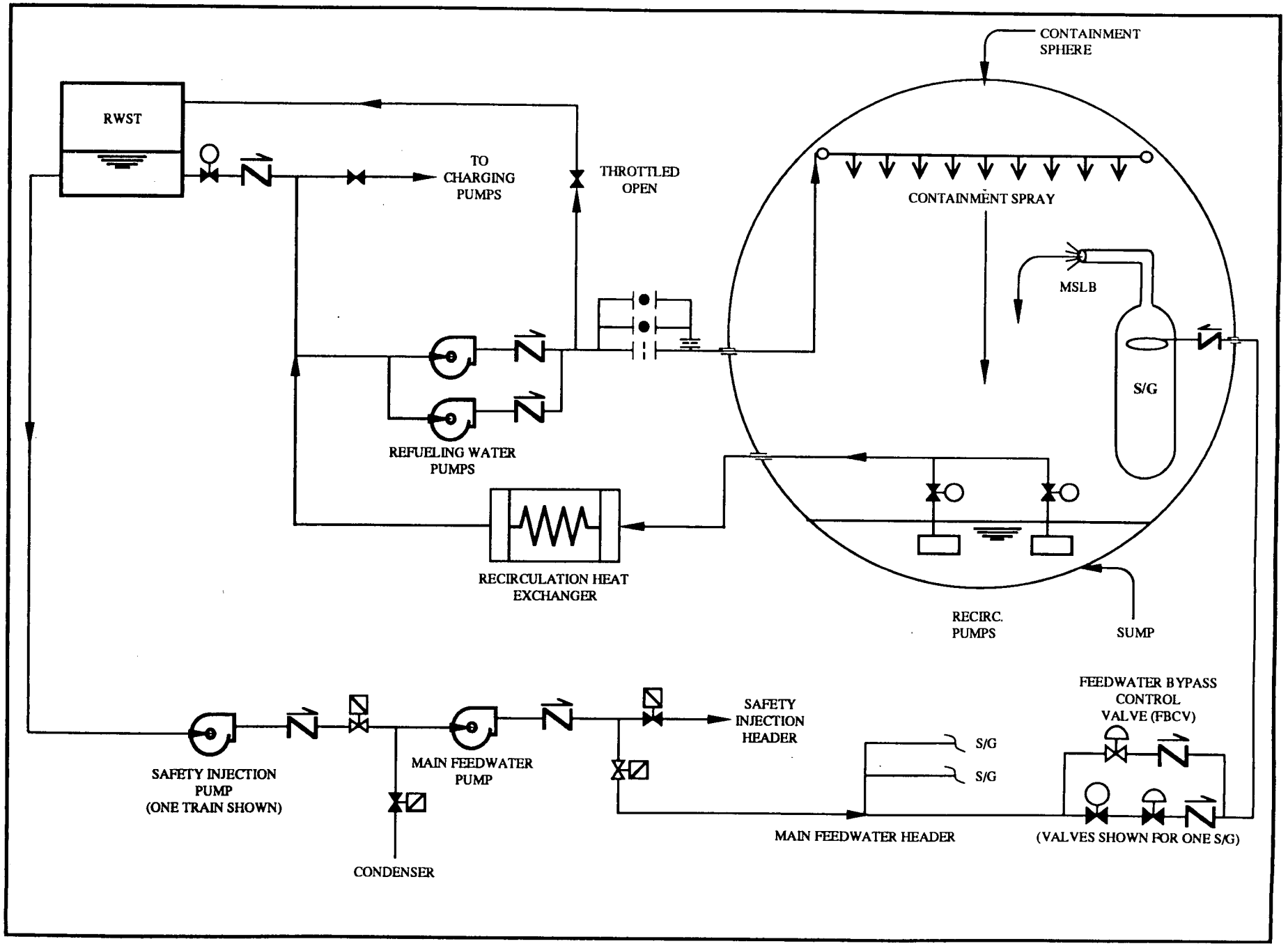


Figure A9. Post-Main Steam Line Break
Secondary Recirculation

PRA FOR SEQUENCER BLOCK CIRCUIT DEFICIENCIES

PURPOSE

The purpose of this analysis is to assess the impact on core damage frequency of a single failure susceptibility concerning the safety injection sequencer block circuits. Specifically, Train A and B sequencers are postulated to lose power due to electrical faults in the safety injection block permissive circuits.

ANALYSIS

In the event a random short occurred on the Train A or B sequencer block relay coil or associated circuit wiring during normal operation, the damage to the circuit could have propagated to the other block circuit train due to the close proximity of the associated Train A and B block circuit wiring and relay contacts. The resulting damage to the Train A and B block circuits could have resulted in a trip of both sequencer 125 VDC protection breakers (72-124 and 72-212) and a loss of automatic safety injection signal actuation (SIS) operability.

The events of concern where a loss of the sequencers could have resulted in core damage are large LOCAs, MSLBs, or FWLBs. For small LOCAs, MSLBs, and FWLBs, manual operation of the Safety Injection System could have prevented core damage. However, in this analysis, it is conservatively assumed that small breaks also result in core damage from this failure.

The likelihood of a short on a relay is assumed to be 4.3E-7 per hour (NSAC/60, Oconee PRA). The likelihood of a short on the control wiring in the block circuit is assumed to be 1E-5 per hour (NSAC/60, Oconee PRA). The probability of a short on one train of block circuit affecting the other train is assumed to be 0.9, based on the close proximity of the wiring between trains and use of a common relay. The probability of both damaged block circuits causing trip of both sequencer 125 VDC protection breakers is assumed to be 0.1. The period of time following such a short, where the occurrence of a LOCA, MSLB, or FWLB could have resulted in an inability to automatically initiate the sequencer, is conservatively assumed to be the Technical Specification action statement allowed outage time for loss of both sequencer channels (one hour) plus the time required to bring the unit to a Mode 4 condition (12 hours). The total time following the short where the unit could have been vulnerable to this failure would have been 13 hours.

The frequency of the scenario where both sequencers are failed and a LOCA, MSLB, or FWLB occurs, can be calculated using the following equation:

F(CD) = 2* [P(SHORT ON A BLOCK CIRCUIT RELAY) +
P(SHORT ON BLOCK CIRCUIT WIRING)] *
P(SHORT AFFECTS OTHER BLOCK CIRCUIT TRAIN) *
P(BOTH SEQUENCER 125 DC BREAKERS TRIP DUE TO DAMAGE)*
F(LOCA+MSLB+FWLB)

where:

P(SHORT ON A BLOCK CIRCUIT RELAY) = 4.3E-7 per hour * 13 hours
=5.6E-6

P(SHORT ON BLOCK CIRCUIT WIRING)= 1E-5 per hour * 13 hours
= 1.3E-4

P(SHORT AFFECTS OTHER BLOCK CIRCUIT TRAIN) = 0.9 (above assumption)

P(BOTH SEQUENCER 125 DC BREAKERS TRIP DUE TO DAMAGE) = 0.1

F(LOCA+MSLB+FWLB)=3.9E-3 per year + 3E-3 per year + 3E-3 per year
(NSAC/60, Oconee PRA)
=9.9E-3 per year

Thus, F(CD) =2* (5.6E-6 + 1.3E-4) * 0.9 * 0.1 * 9.9E-3 per year
=2.4E-7 per year

CONCLUSIONS

The likelihood of the above scenario involving the shorting of the sequencer block circuits leading to core damage is low. Therefore, the existence of this single failure susceptibility did not significantly compromise plant safety.

A10. LOSS OF INSTRUMENT AIR TO CONTAINMENT SPRAY ISOLATION VALVES

INTRODUCTION

A failure of the check valves in the containment spray line outside containment following a common cause failure of the isolation valves inside containment could lead to a loss of containment isolation during the initial stages of a small break accident. However, since these check valves do not have to change position to complete their containment isolation function, they are passive components which would not have failed. Due to the nature of these valves, they are treated as passive containment isolation valves and are not assumed to fail.

BACKGROUND

Isolation for the containment spray line is provided by two parallel check valves outside containment (CRS-304 and CRS-305) and two parallel remote manual valves inside containment (CV-82 and CV-114) as depicted in Figure A10.

In accordance with the SONGS 1 design basis, check valves used for containment isolation are treated as active components even though other check valves are treated as passive components. However, CRS-304 and CRS-305 are only needed for containment isolation during the initial stages of a small break accident and do not move from their closed position to accomplish this function. Therefore, in accordance with the definition of an active failure as described in ANSI N658-1976, "American National Standard Single Failure Criteria for PWR Fluid Systems," these check valves are treated as passive containment isolation valves and are not assumed to fail.

SINGLE FAILURE

As discussed above, the containment isolation check valves are considered passive components and are not assumed to fail.

SAFETY SIGNIFICANCE

Although the containment spray check valves are not considered to fail, leakage through these valves during an accident could drain the spray riser (see Figure A10) allowing containment gases to escape to the atmosphere. However, this will not occur because the system configuration is such that a water column will exist between the containment spray check valves and the containment spray nozzles when isolation is required. This water column combined with the check valves will prevent leakage of the containment atmosphere during both a large and small break accident, even if the instrument air system fails, causing CV-82 and CV 114 to open.

Large Break Accident

During a large break Loss of Coolant Accident (LOCA) or Main Steamline Break (MSLB), where the containment pressure rises rapidly, CRS-304 and CRS-305 open almost immediately when the containment spray system actuates. The spray flow keeps the check valves open until the containment spray system is turned off late in the accident after the containment pressure has been reduced. When the containment spray system is turned off, CV-82 and CV-114 are closed to isolate the line.

In the event that CV-82 and CV-114 are unable to be closed due to a common cause failure of the instrument air system, isolation of the containment spray line would be maintained by the recirculation pump flow. At the stage in the accident when the containment spray system is turned off, the recirculation system would be in operation to provide long term cooling. The recirculation pumps take suction from the containment sump and supply flow to the charging pumps through a header which is common to the refueling water pumps. If CV-82 and/or CV-114 were open, water being provided to the charging pumps from the recirculation pumps would also be forced through the idle containment spray pumps and into the containment spray lines. The recirculation pumps would maintain forward flow through the spray line to the spray nozzles preventing back leakage of the containment atmosphere. Therefore, due to system operating characteristics, isolation of the containment spray line will be maintained when required during a large break accident and the check valves are not depended upon to provide containment isolation.

Small Break Accident

During a small break accident, isolation of the containment spray line is required during the time that containment pressure is slowly rising to the setpoint for automatic spray actuation (up to four hours in some cases). An analysis has confirmed that a column of water will exist in the containment spray line during this time. The water column will prevent leakage of the containment atmosphere and will exist as long as the containment pressure is below the setpoint for automatic containment spray actuation (10 psig) assumed in the safety analysis. CRS-304 and CRS-305 ensure that the water column will remain in the pipe until spray is actuated. This has been verified by measurement of the leakage through the check valves.

Once containment spray is actuated, the check valves open and will remain open until the containment spray system is turned off. At this stage in the accident, the recirculation pumps are running to provide long term cooling and leakage of the containment atmosphere is prevented by the forward flow through the spray system, as discussed for the large break accident.

Therefore, based on the containment spray system operation and the passive nature of the check valves, this issue has a low safety significance.

RESOLUTION

As discussed above, there is no single failure concern with the containment spray check valves because they are considered passive components which are not assumed to fail.

The common cause failure of CV-82 and CV-114 has been reviewed and it was confirmed that the spray line meets the acceptance criteria of the Systematic Evaluation Program (SEP) due to the existence of a water column during periods when containment isolation is required. Although this line still meets the SEP requirements, as part of the planned Cycle 12 ECCS modifications, an upgrade to the containment isolation capability of the line will be implemented to further increase plant safety.

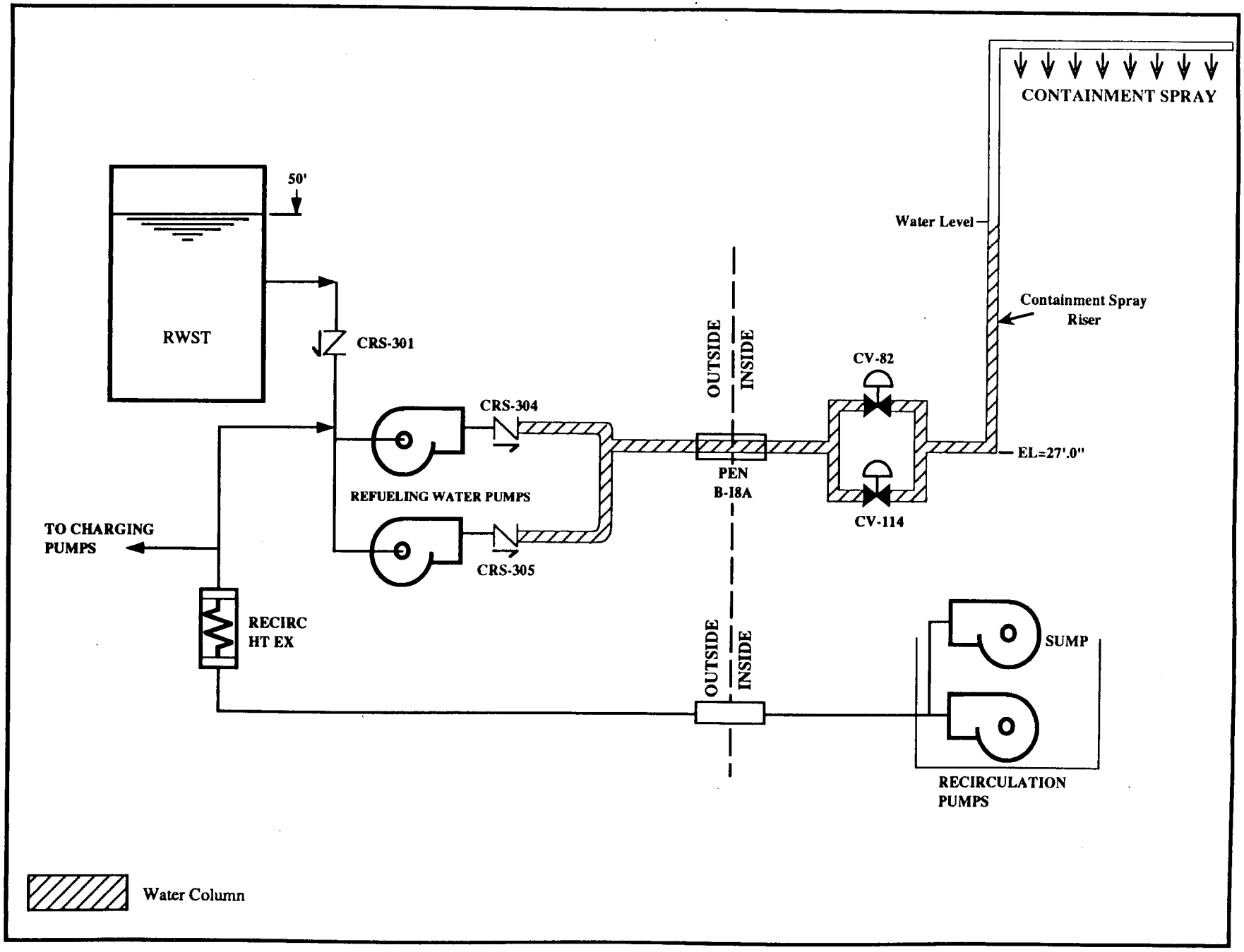


Figure A10. Containment Spray System Configuration