Southern California Edison Company

23 PARKER STREET

IRVINE, CALIFORNIA 92718

F. R. NANDY
MANAGER, NUCLEAR LICENSING

July 31, 1990

TELEPHONE
(714) 587-5400

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
Washington, D. C. 20555

Gentlemen:

Subject: **Docket No. 50-206**
ECCS Single Failure Analysis
San Onofre Nuclear Generating Station, Unit 1

Enclosed is an interim report on the new emergency core cooling system (ECCS) single failure analysis, which we committed to perform in our letter dated March 17, 1989, "Technical Issues Impacting San Onofre Unit 1 Restart." This letter describes the analysis, provides a summary of the results, and identifies plant changes (i.e., modifications, Technical Specification revisions, procedural changes, etc.) that will be implemented as corrective actions to resolve the issues identified by the analysis.

Background

We submitted a single failure analysis of the ECCS on December 21, 1976. That analysis was submitted in response to issuance of Appendix K to 10 CFR 50, "ECCS Evaluation Models," which required that ECCS used to mitigate Loss of Coolant Accidents (LOCA) meet the single failure criterion. The original analysis was performed prior to the evolution of current analysis criteria and methodology. Plant modifications were subsequently implemented to correct the single failure susceptibilities identified by that analysis.

As a result of the 1986 failure of main steam pressure transmitter, PT-459, Reactor Protection System and Engineered Safety Features (ESF) single failure analyses were performed in 1987. Resultant modifications were implemented during the Cycle 10 refueling outage.

Additional single failures and other failures which occur as a direct consequence of the event, i.e., common cause failures, were identified in the component cooling water system as a result of our response to Generic Letter 88-14. A follow-up review of other ESF systems for similar susceptibilities identified further issues. As a result of these additional single failure issues, we decided to reanalyze the 1976 single failure analysis as committed in our letter to the NRC Region V dated March 17, 1989, "Technical Issues Impacting the San Onofre Unit 1 Restart."

A001
1/1

Description

The analysis reported in this letter is completely new. We did not limit ourselves to the scope of the 1976 analysis which addressed only the LOCA required ECCS functions. Rather, we expanded our review and evaluated the ECCS functions required to mitigate LOCA, Main Steam Line Break, and Steam Generator Tube Rupture. By including these three bounding design basis accidents in the analysis, we evaluated all required ECCS functions for the worst combinations of single failure and common cause failure conditions.

The new single failure analysis consists of a boundary valve analysis and a failure modes and effects analysis. These analyses evaluated more than three thousand postulated component single failures. Enclosure 1 provides a detailed description of the scope, criteria, and methodology used for the single failure analysis.

The new single failure analysis is based on current design criteria including ANSI Standard N658-1976, "Single Failure Criteria for PWR Fluid Systems," and IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." Consistent with current practice, common cause failures or pre-existing conditions were evaluated concurrent with a random single active failure.

Since this is a new analysis based on current practice, we will validate the analysis assumptions prior to restart from the current outage to confirm that the plant is operated in the configuration assumed in the analysis. For example, our analysis established system boundaries, including identification of all manual boundary valves. We will verify that these boundary valves can be operated consistent with the assumptions of the analysis.

Results

The new single failure analysis concluded that ECCS functions were not adversely affected by the vast majority of the component single failures evaluated. The single failure analysis, however, identified several issues which require corrective actions. These corrective actions will be implemented prior to plant restart from the current outage. A summary of these issues and a description of our preliminary plans for corrective actions are provided in Enclosure 2.

Issues Under Review

The new single failure analysis also identified the following four issues which remain under review:

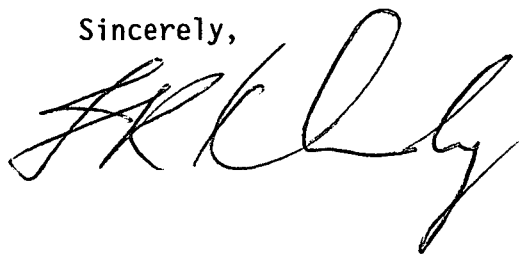
- Recirculation flow imbalances due to failure of the flow monitoring instruments or control valves,

- Time dependent and interactive failures affecting containment recirculation and spray,
- Reactor Coolant Pump overcurrent protection failure resulting in loss of containment electrical penetration integrity,
- Vital Bus loss of power resulting from lack of retransfer capability.

The resolution of these issues will be addressed with the NRC prior to restart from the current outage.

If you have any questions or desire additional information, please contact me.

Sincerely,



Enclosures

cc: J. B. Martin, Regional Administrator, NRC Region V
C. Caldwell, NRC Senior Resident Inspector, San Onofre Units 1, 2 and 3

ENCLOSURE 1

DESCRIPTION OF THE 1990 ECCS SINGLE FAILURE ANALYSIS

ENCLOSURE 1

SCOPE, CRITERIA, AND METHODOLOGY FOR THE EMERGENCY CORE COOLING SYSTEMS SINGLE FAILURE ANALYSIS, SAN ONOFRE NUCLEAR GENERATING STATION, UNIT 1

TABLE OF CONTENTS

EMERGENCY CORE COOLING SYSTEMS SINGLE FAILURE ANALYSIS SAN ONOFRE NUCLEAR GENERATING STATION, UNIT 1

I. INTRODUCTION AND BACKGROUND

In response to an NRC letter to SCE dated April 8, 1976, a single failure analysis was performed for the systems required to mitigate a postulated loss of coolant accident (LOCA), including safety injection, charging, containment spray and recirculation, component cooling water, salt water cooling, and the auxiliary power system. This analysis, which used failure modes and effects methodology, was submitted by SCE to the NRC in a letter dated December 21, 1976.

On July 30, 1986, a failure of main steam pressure transmitter PT-459 caused a transient in all three channels of the feedwater control system and affected all three channels of the steam/feedwater flow mismatch scram in the Reactor Protection System (RPS). In response to this event, SCE committed to several actions, including completion of a single failure analyses for the SONGS 1 RPS and Engineered Safety Features (ESF) System to determine the susceptibility of the SONGS 1 design to single failures in these systems.

The RPS single failure analysis, submitted to the NRC by SCE in a letter dated March 11, 1987, identified single failure and event specific failure susceptibilities in the steam/feedwater flow mismatch and RCS low flow scram functions.

The ESF single failure analysis, submitted to the NRC by SCE letter dated November 6, 1987, included: 1) a failure modes and effects evaluation of the ESF design changes which had been implemented to correct the single failure susceptibilities identified by the 1976 ECCS single failure analysis; 2) a failure modes and effects analysis of the ESF functions not addressed by the 1976 ECCS single failure analysis, including containment isolation, main feedwater isolation, overpressure mitigation, and auxiliary feedwater; and 3) an event specific single failure response analysis of those ESF functions identified as having potential common cause, time or event dependent failure susceptibilities. Single failure and event specific failure susceptibilities were identified in the main feedwater isolation function and

in realignment of swing 480 V Switchgear 3 affecting recirculation and charging. Resultant modifications were implemented during the Cycle 10 refueling outage.

Additional single failure and common cause failure susceptibilities were identified in the component cooling water system as a result of our response to Generic Letter 88-14. A follow-up review of other ESF systems for similar susceptibilities identified further issues. As a result of these additional single failure issues, we decided to reanalyze the 1976 single failure analysis as committed in our letter to the NRC Region V dated March 17, 1989, "Technical Issues Impacting the San Onofre Unit 1 Restart."

II. SCOPE

The 1990 ECCS single failure analysis addresses the following ECCS functions for LOCA, SGTR, and MSLB:

- Safety Injection, including main feedwater isolation and auto-termination of SI/FW flow on low RWST level
- Cold Leg Recirculation (required for LOCA only)
- Hot Leg Recirculation (required for cold leg LOCA only)
- Secondary Recirculation (required for MSLB inside containment only)
- Containment Spray and Hydrazine Injection (required for LOCA or MSLB inside containment only)
- Component Cooling Water System
- Saltwater Cooling System
- Safety Injection Actuation System
- Containment Spray Actuation System (required for LOCA or MSLB inside containment only)
- Standby Power System (Diesel Generators)
- Vital and Regulated Power System
- Auxiliary Power System

III. METHODOLOGY

A. The ECCS Single Failure Analysis was performed per the criteria discussed in Section IV below, in five sequential, overlapping parts:

- Boundary valve analysis of each ECCS fluid system function.
- Failure modes and effects analysis (FMEA) of each ECCS fluid system function, including interface device and power supply dependencies.
- FMEA of each ECCS actuation system.
- FMEA of the vital, regulated and auxiliary power systems common to the ECCS fluid and actuation systems.
- Identification of ECCS functions potentially susceptible to time or event specific single failures (as discussed in Section IV, below).

B. The detailed methodology was as follows:

1. The piping and instrumentation diagrams (P&IDs) for each ECCS function were marked to show process flow path and boundary devices based on the Emergency Operating Instructions (EOIs) and other applicable references. Instruments essential to the ECCS function (e.g., flow rate indication required for valve modulation) were included as flow path devices.

2. A boundary valve analysis was performed for each ECCS function. This analysis tabulated the branch line isolation valve configurations as to:

   - Normal valve position (open, closed or automatically closed).
   - Whether the valve is locked.
   - Safety related backups (valves, caps or blind flanges) with associated normal positions.
   - Non-safety related backups with associated normal positions.

   Boundaries were taken at the first normally or automatically closed safety related valve or at the

safety related/non-safety related class boundary valve, whichever came first. Check and relief valves were included but treated as passive devices. A computer program was then used to automatically sort the boundary valve analysis data base and identify those configurations which do not meet single failure criteria.

3. For each power-operated device (including essential instruments) identified in Step 1 above, the applicable elementary diagrams were marked to show interface devices and dependencies (e.g., sequencer inputs, interlock inputs/outputs, power supplies, etc.). The circuits were otherwise treated as black boxes for simplicity.

4. For each train, the flow path and boundary devices, including interface device and power dependencies, were evaluated in the FMEA. To limit the FMEA data base to a manageable size, manual valves and check valves for each function were grouped into flow path and boundary entries for each train and backup boundary devices were included in the FMEA data base only if both the first boundary device and its backup were power-operated. Check valves were included in the data base, but identified as "passive" devices. The electrical devices from Step 3 above as well as the applicable power sources (air, backup nitrogen, electrical bus, etc.) were included as "loop" devices for each power-operated item, similar to the RPS single failure analysis. Differences between SIS and SISLOP actuation and common cause (e.g., environmental qualification or seismic) susceptibility were identified where applicable.

5. An automated sort of the FMEA data base for all ECCS functions was performed to identify ECCS actuation device dependencies.

6. The applicable elementaries, load schedules, etc. for the ECCS actuation systems were marked similarly to Steps 1 and 3 above. Using the automated sort from Step 5, the applicable devices were evaluated in the FMEA, including differences between SIS and SISLOP actuation and common cause susceptibility.

7. An automated sort of the FMEA data base for all ECCS functions was performed to identify the control and motive power dependencies.

8. The one line diagrams and applicable elementaries for the Vital/Regulated Power and Auxiliary Power systems were marked similarly to Steps 1 and 3 above. Using the automated sort from Step 7, the applicable devices were evaluated in the FMEA, including differences between SIS and SISLOP events and common cause susceptibility.

9. Using the criteria discussed in Section IV below, the ECCS functions which are potentially susceptible to time or event specific single failures were identified for further evaluation.

IV. CRITERIA

A. To the extent practical, the single failure analyses for the ECCS functions were performed using notation, format and assumptions consistent with the RPS and ESF single failure analyses submitted to the NRC on March 11, 1987 and November 6, 1987, respectively. Specifically:

1. The module level FMEA's were performed in accordance with IEEE Standard 279-1971. Specifically, Parts 2, 4.2 and 4.7 of the standard were applied as follows:

a. Single failures were postulated at the level of tag numbered devices (modules) which resulted in the most limiting effects or combination of effects on the ECCS functions. No credit was taken for module internal design features (components) which could preclude such failures except where specifically identified. All tag numbered and interface devices which could affect the ECCS output functions (i.e., not excluded by the "black box" methodology and criteria addressed in paragraph III.B.3 above and IV.A.1.c below) were addressed.

b. The failure modes for each device which result in the most limiting effects or combination of effects were selected so that all pertinent ECCS output and interface (including isolation device) failure combinations were bounded. The failure modes typically considered for each type of device were:

- Transmitter (e.g., PT, LT, FT): SIGNAL HIGH or LOW

- Power Supply (e.g., YE): OUTPUT VOLTS HIGH or ZERO

- Indicator (e.g., PI, LI, FI): INPUT OPEN or SHORT
- Test Switch (e.g., Y): OPEN or SHORT (CLOSED)
- Controller or Bistable (e.g., PC, LC, FC): INPUT OPEN or SHORT; OUTPUT TRIPPED or UNTRIPPED, HIGH or LOW
- Relay: INPUT OPEN or SHORT; OUTPUT TRIPPED or UNTRIPPED, ON or OFF, CONTACTS OPEN or CLOSED as applicable. Combinations such as CONTACTS OPEN (ON) were used as needed for clarity.
- Valve/Actuator: OPEN or CLOSED
- Pump/Motor: OUTPUT LOW

In addition, single pole or phase GROUNDS were postulated in all grounded circuits. In some cases, another failure mode (e.g., INPUT SHORT) was identified as bounding for the affected circuit, rather than creating a separate data base entry.

c. Where a portion of a channel had only a single output and the net effect of the failures could be expressed in terms of that output, the devices in that portion of the circuit were permitted to be treated as a single entity. For example: a) postulated failures of the pressure regulating valve or solenoid operated pilot valve for a pneumatically actuated isolation valve are bounded by failures of the isolation valve itself, and b) postulated failures of control components in a manually controlled power-operated valve are bounded by those of the valve/actuator and its control power and interlock dependencies.

d. The failure modes for any channel common or train common devices (e.g., selector switches, transfer switches, auctioneering or signal comparison devices) were conservatively considered to result in channel common or train common failures, respectively, if unisolated signals were present in the device and channel/train separation and identity were not maintained through the device. The postulated failure modes were:

- OPEN (at all input channels/trains)

- SHORT (of all like poles or phases, resulting in paralleling of all inputs)

- GROUND (of all like poles or phases)

e. It was assumed that events requiring ECCS actuation could be initiated from any applicable plant condition.

f. The only applicable ECCS actuation instrumentation which have control functions are associated with the RPS, and have been previously analyzed for control/protection interactions. Accordingly, a control/protection system interaction (multiple failure) analysis was not performed as part of the ECCS evaluation.

B. Because the ECCS systems include fluid system components as actuated devices, ANSI Standard N658-1976 (Single Failure Criteria for PWR Fluid Systems) was also applied to the single failure analyses for these functions. Specifically, Parts 2, 3.4, 3.5, 3.6, 3.7, 3.10 and 4 of the standard were applied as follows:

1. Single failures were postulated in all ECCS process flow path and flow path boundary devices, including manual valves and applicable valve control circuits. Both failure to actuate and spurious actuation events (e.g., due to operator error), except as provided in item 2 and as follows, were considered:

   a. Passive devices such as orifice plates, flanges and similar pressure boundary parts were excluded.

   b. Check valves were included, but considered as passive devices.

   c. Credit was taken for administrative controls under the valve locking program to preclude spurious actuation of applicable manual valves.

   d. Credit was taken for the provisions of NRC Branch Technical Position ICSB-18 to preclude spurious actuation of applicable manually controlled electrically operated valves.

2. Only active failures were considered as single failures, in accordance with the SONGS 1 design basis. Failure of passive devices or process pressure boundaries were not postulated in addition to the initiating event.

3. Compressed air (ISA) system failure was considered as a potential failure for pneumatically actuated valves. Failure of non-seismic systems, including ISA, was conservatively considered as a common cause effect except where credit was specifically permitted by the Standard Review Plan (e.g., SRP Section 15.1.5 for MSLB inside containment).

C. Common Cause and Pre-Existing Failures

1. Except as specifically provided above, loss of non-seismic systems and of any devices not qualified for the applicable post-accident harsh environment were considered to be potential common cause failures.

2. The probability of a loss of offsite power (LOP) to the San Onofre switchyard due to failure of the offsite distribution system was previously determined to be less than 10^{-12} per year (e.g., San Onofre Units 2/3 UFSAR, Section 8.2.2.3), which is insignificant relative to the probability of a LOP due to failure of onsite equipment. Consequently, common cause failure of non-safety related Auxiliary Transformer C was considered as a potential cause of the postulated LOP for SISLOP events.

3. Transfer switches, disconnect switches, etc. whose positions are not alarmed, indicated or otherwise supervised in the control room were considered to be potential pre-existing failures unless included in an administratively controlled locking and/or periodic surveillance program.

4. Credit was taken for indirect indication of failures to preclude an undetected pre-existing condition. For example, loss of power ("VOLTS LOW") to a valve or pump control circuit is considered detectable by the dimming or loss of the associated control room status indication, and is therefore identified as CONTROL ROOM INDICATION in the method of detection field in the FMEA.

5. Common cause and pre-existing failures were considered to occur in addition to the random single active failure, consistent with the provisions of ANSI Standard N658-1976.

D. Screening Criteria for Event Specific Susceptibilities

An evaluation of event specific single failure response is required when:

1. The flow requirements for a system are dependent on the response of another system which is actuated from separate instrumentation. This requires an event dependent evaluation of the integrated response of the applicable systems.

2. The system has two or more safe states for the same equipment (e.g., must be on during one part of the accident but off during another part, or in different alignments for different events, etc.) This requires a time dependent evaluation of the response to applicable single failures.

3. System components or supporting equipment are susceptible to location dependent common cause failures (e.g., due to the environment for inside vs. outside containment line breaks). This requires a location dependent evaluation of the response to applicable single failures.

4. The system has train common suction or discharge piping in which misoperation of one train could divert flow from or otherwise adversely impact operation of the redundant train. This requires a time dependent evaluation of the response to applicable single failures.

encleccs.rep

ENCLOSURE 2

RESULTS OF THE 1990 ECCS SINGLE FAILURE ANALYSIS

ENCLOSURE 2

1. SPURIOUS ACTUATION OF RECIRCULATION PUMP DISCHARGE ISOLATION VALVES (MOV-866A AND MOV-866B)

INTRODUCTION

Spurious actuation of either recirculation pump discharge motor-operated isolation valve could lead to loss of post-accident recirculation and containment spray.

BACKGROUND

Emergency core cooling is provided in two phases. The injection phase consists of injecting borated water from the Refueling Water Storage Tank (RWST) into the Reactor Coolant System (RCS) and into the Containment Spray (CS) header. The recirculation phase is initiated once the RWST inventory is depleted. Recirculation pumps provide borated water from the containment sump to the RCS and CS header for long-term post-accident cooling as shown in Figure 1.

During the injection phase, the refueling and charging pumps take suction from the RWST. The suction line to the RWST includes a check valve (CRS-301) which seats to isolate the tank when the line becomes pressurized during initiation of recirculation flow.

Each of the two recirculation pumps has a motor-operated discharge isolation valve, MOV-866A and MOV-866B. The flow from the two pumps combine in a common header downstream of the valves. A charging pump draws suction from the common header to recirculate sump water to the RCS loops. The refueling water pumps also draw suction from the common header to recirculate sump water to the CS header.

During normal operation MOV-866A and MOV-866B are closed and the upstream piping and pumps are dry. After sufficient RWST inventory has accumulated in the sump from safety injection and CS in an accident, recirculation pumps are started to purge the air and any post-accident steam from the pump casings and discharge piping. The air in the pumps and piping is purged through a permanently open vent, located just upstream of the discharge valves, by running the recirculation pumps for at least two minutes prior to opening the valves.

SINGLE FAILURE

Spurious opening of either discharge valve during the injection phase could introduce a mixture of air and steam into the suction of the charging pumps and refueling water pumps. This could

cause these pumps to fail. A spurious valve opening could also pressurize the refueling water pump suction piping to the post-accident containment pressure level. This pressure could cause the RWST discharge check valve (CRS-301) to seat and result in loss of CS during the injection phase.

RESOLUTION

Plant modifications will be installed during the Cycle 11 refueling outage to eliminate the potential for spurious opening of MOV-866A and MOV-866B.

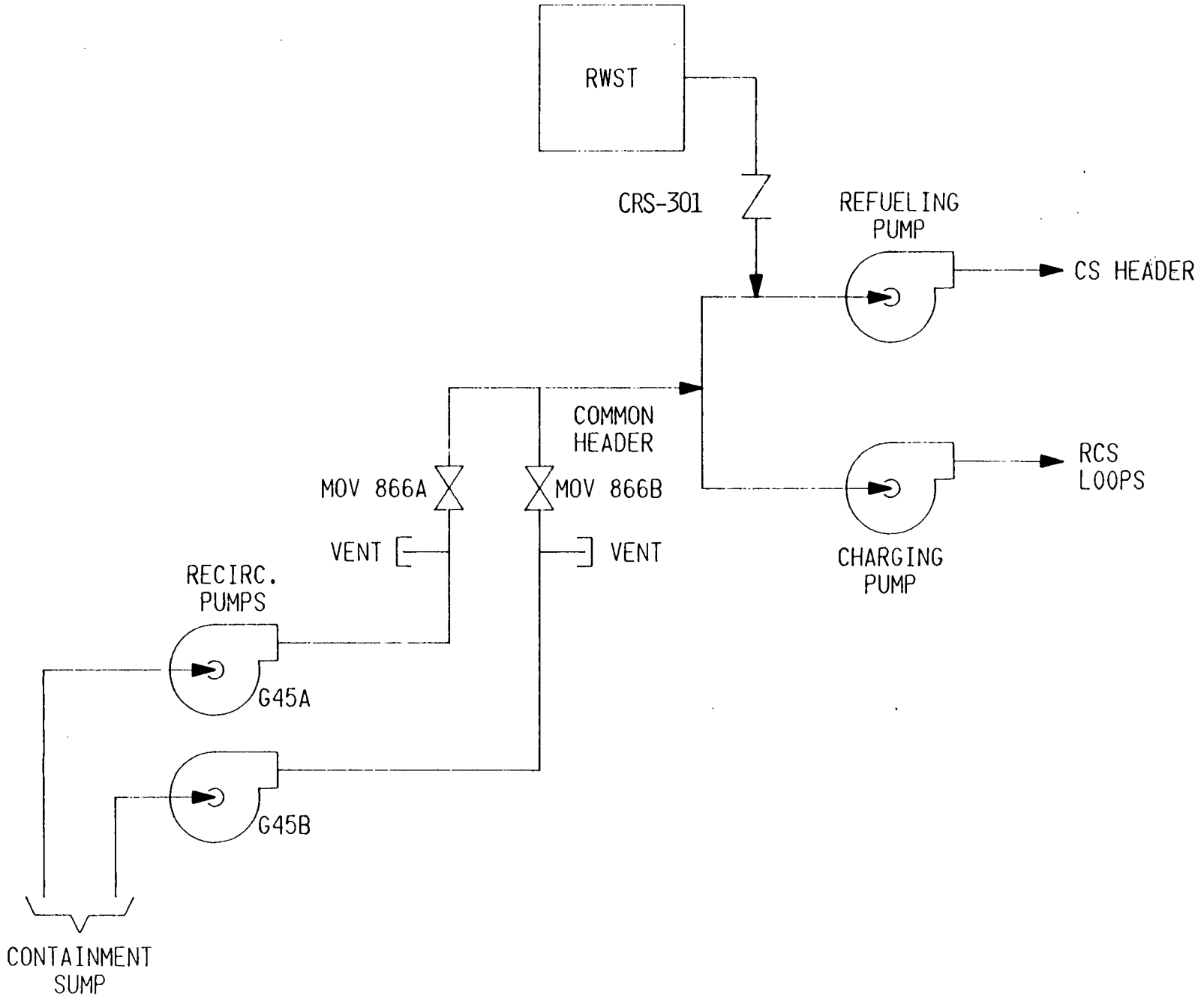


Figure 1. Recirculation System

2. LOSS OF SUCTION TO THE CHARGING PUMPS PRIOR TO SAFETY INJECTION SIGNAL

INTRODUCTION

Misoperation of the Volume Control Tank (VCT) isolation valve or level controller could lead to loss of suction to the charging pumps resulting in pump failure.

BACKGROUND

The VCT and the Refueling Water Storage Tank (RWST) supply water for the charging system. During normal operation, one of the charging pumps operates continuously and takes suction from the VCT. The redundant charging pump normally remains on standby and will start automatically upon failure of the operating pump. However, a safety injection signal (SIS) will lock out the second pump from starting automatically.

As shown in Figure 2, there are two safety related isolation valves for the RWST, MOV-1100B and MOV-1100D, and one for the VCT, MOV-1100C. These isolation valves are interlocked with a single VCT level controller so that only one source, either the VCT or RWST, is aligned to the charging pumps. There is also a non-safety related valve in parallel with MOV-1100B and MOV-1100D that was installed for Fire Protection (Appendix R) safe shutdown. This valve, FCV-5051, opens automatically on low charging pump suction pressure. On a VCT low-low level signal or a SIS, MOV-1100B and MOV-1100D automatically open while MOV-1100C automatically closes. Closure of MOV-1100C prevents hydrogen gas entrainment in the charging pump suction. A hydrogen gas blanket is maintained in the VCT for chemistry control.

SINGLE FAILURE

1. During small break LOCA's, decreasing pressurizer level results in automatically increased charging flow and reduced letdown flow. The pressure in the pressurizer decreases slowly. As a result, the charging pump, which is providing RCS makeup, could empty the VCT before a SIS occurs. Failure of the charging pump could occur due to hydrogen entrainment, with subsequent autostart and failure of the second pump if: a) the VCT level controller fails to initiate a low-low level signal, or b) VCT isolation valve MOV-1100C fails to close upon receipt of a low-low level signal.

2. Spurious closure of MOV-1100C would not generate an open signal to MOV-1100B and MOV-1100D. Were this failure to occur prior to a SIS for a LOCA of any size, the loss of

suction would result in failure of the operating charging pump with subsequent autostart and failure of the second charging pump.

RESOLUTION

1. Design modifications will be implemented prior to the Cycle 11 restart to prevent loss of charging pump suction due to hydrogen entrainment.

2. The existing non-safety related parallel suction path from the RWST will be credited to prevent loss of charging pump suction due to closure of MOV-1100C. Although the valve controls are classified non-safety related fire protection (NSRFP), the valve provides an independent method to prevent loss of charging as a result of loss of suction. We will take credit for this feature for one fuel cycle (Cycle 11). A PRA will be performed to evaluate the need for additional modifications. Additional modifications will be installed in Cycle 12, if warranted.

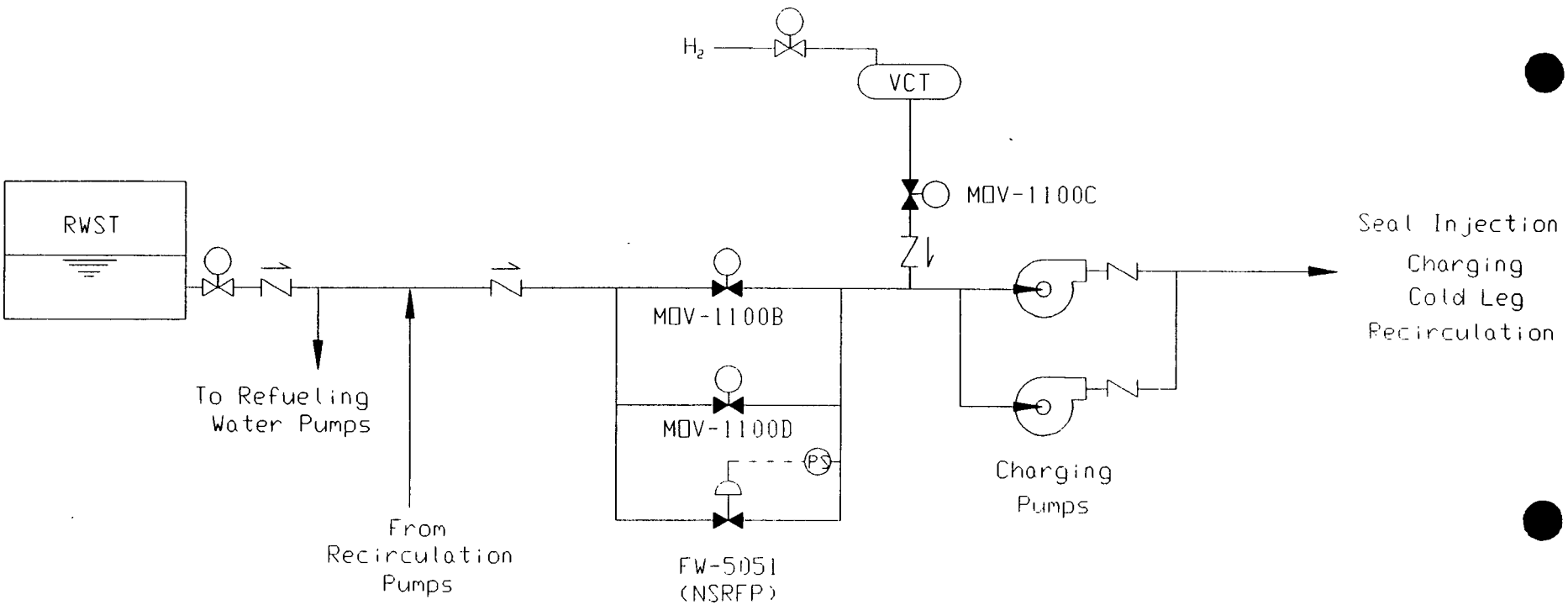


Figure 2. Water Supply for Charging Pumps

3. DIVERSION OF ALTERNATE HOT LEG RECIRCULATION FLOW

INTRODUCTION

Common cause failure of an alternate Hot Leg Recirculation (HLR) flow path boundary valve could cause diversion of HLR flow.

BACKGROUND

Emergency core cooling is provided by injection followed by recirculation. If the event that initiates Emergency Core Cooling System (ECCS) operation is a break in a Reactor Coolant System (RCS) cold leg, recirculation via the RCS hot leg prevents boron precipitation in the core region.

The plant design includes two independent HLR paths (See Figure 3). These paths are redundant and use different systems. The primary HLR flow path recirculates containment sump water, using the recirculation and charging pumps, to the Loop B RCS hot leg. The alternate HLR flow path recirculates containment sump water to the Loop C RCS hot leg using the recirculation and refueling water pumps. The refueling water pump draws water from the recirculation pump discharge piping to provide flow to the Containment Spray (CS) system. Some of the recirculation flow is diverted from the CS path into the Residual Heat Removal (RHR) where it is injected into the RCS Loop C hot leg.

SINGLE FAILURE

A potential flow diversion path exists in the alternate HLR path due to the potential common cause failure of a non-qualified boundary valve (CV-413). Single failure of the other path of HLR could lead to insufficient flow to prevent boron precipitation in the core.

RESOLUTION

A check valve will be installed upstream of the non-qualified boundary valve in the alternate HLR path to eliminate the potential for flow diversion. This modification will be completed during the Cycle 11 refueling outage.

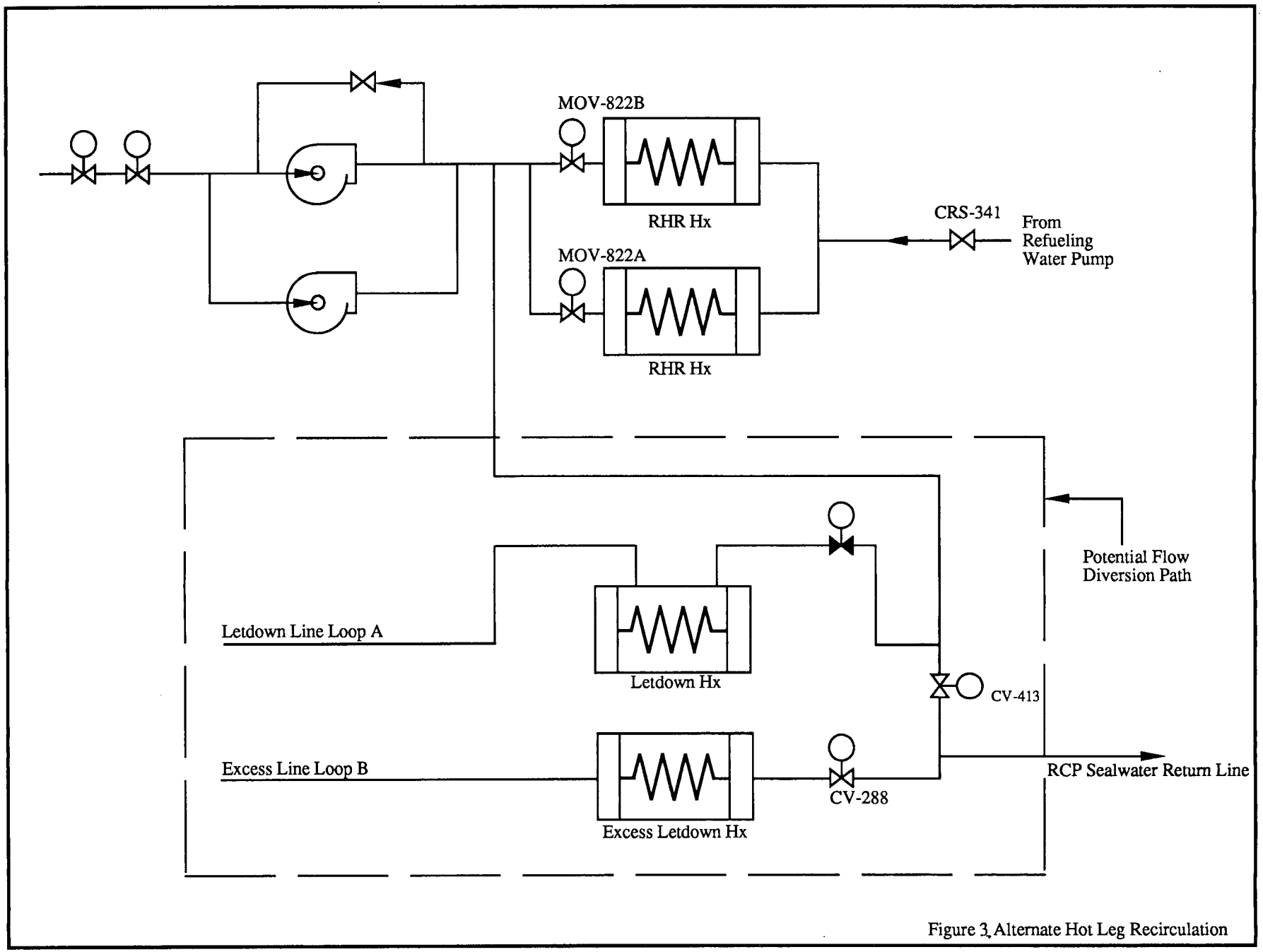


Figure 3. Alternate Hot Leg Recirculation

4. LOSS OF NPSH TO BOTH CHARGING PUMPS DURING RECIRCULATION

INTRODUCTION

Failure of a flow control or spray flow limiter valve to the open position, or failure of a recirculation pump could result in failure of both charging pumps during recirculation.

BACKGROUND

Following a Loss of Coolant Accident, the Safety Injection (SI) and Containment Spray (CS) Systems deliver borated water from the RWST for emergency core cooling. Borated water from SI and CS collects in the sump, and is recirculated for long-term post-LOCA cooling. Since charging is not needed during the injection phase, a lockout feature is provided to prevent the standby charging pump from automatically starting upon loss of the operating pump. The lockout is reset once recirculation is established.

Only one recirculation pump is started when recirculation is initiated. This pump provides suction to both a refueling water pump and a charging pump during the recirculation phase of a LOCA. The combined flow capacity of a charging and a refueling water pump exceeds that of one recirculation pump. Hence, flow to the containment spray header is restricted to limit the total flow of the system to the recirculation pump capacity (See Figure 4).

For cold leg recirculation, charging pump flow is throttled by a pair of flow control valves for each of the three RCS loops as shown in Figure 4. When the primary hot leg recirculation path is also being used, an additional flow control valve is open from the charging pump discharge.

SINGLE FAILURE

Failure of a recirculation flow control valve or a spray flow limiter valve to the open position may allow charging or CS flow to exceed the capacity of a single recirculation pump. Since only one recirculation pump is running, failure of that pump or one of the above described valves would result in failure of the running charging pump due to loss of NPSH. Upon failure of the first charging pump, the second pump would autostart and similarly fail.

RESOLUTION

Plant modifications or procedural changes will be implemented during the current outage to mitigate the consequences of these potential single failures.

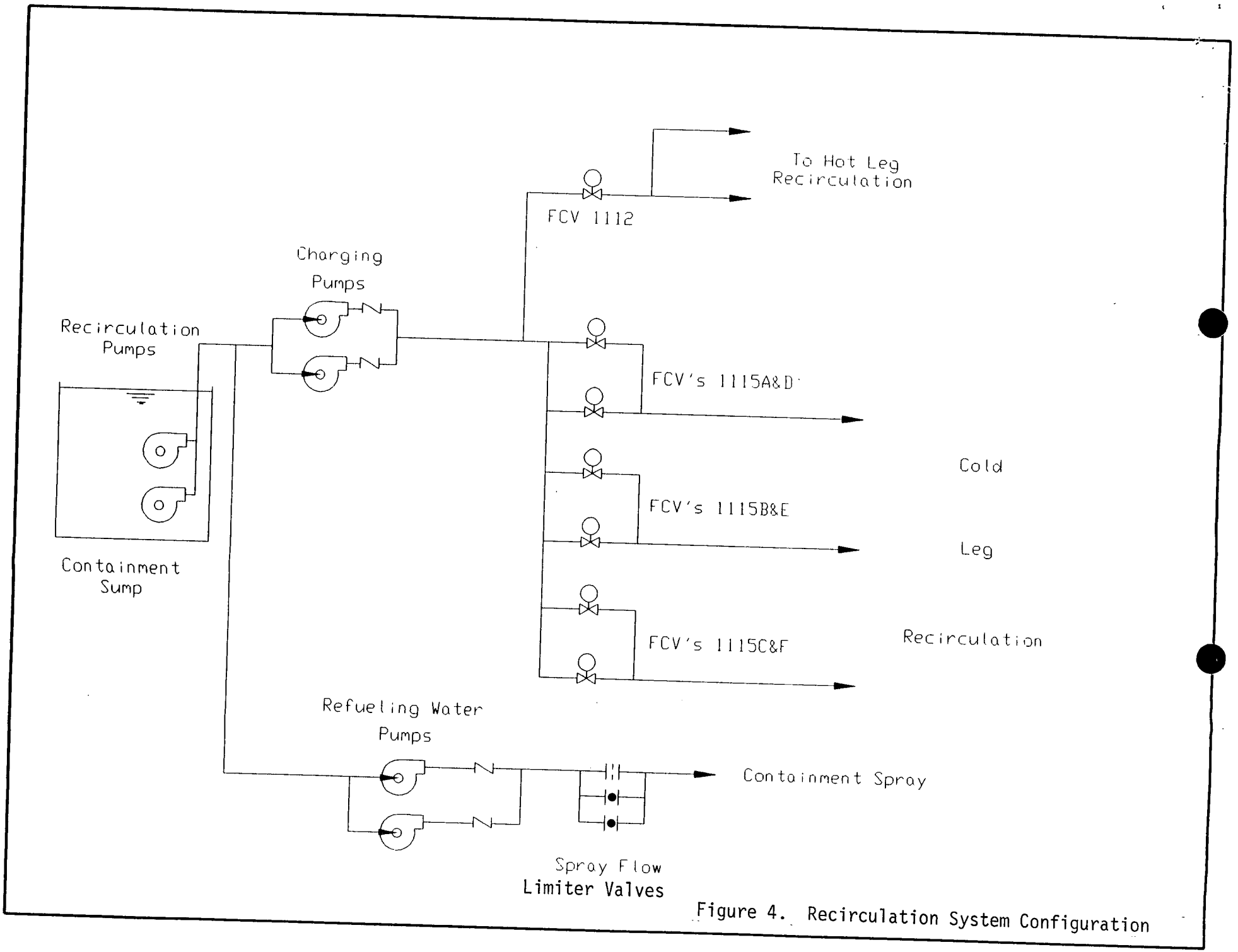


Figure 4. Recirculation System Configuration

5. POTENTIAL LOSS OF FLOW CONTROL FOR SECONDARY RECIRCULATION FOLLOWING A MAIN STEAM LINE BREAK

INTRODUCTION

A common mode failure of the three bypass flow control valves in the feedwater system could prevent cooling water flow to the steam generators following a main steam line break (MSLB) inside containment during secondary recirculation.

BACKGROUND

An MSLB inside containment is initially mitigated by injection of borated water to the RCS for reactivity control and injection of auxiliary feedwater to the steam generators for heat removal. The residual heat removal system is located inside containment and is not qualified for post-MSLB conditions. Long-term heat removal for this event is provided by secondary recirculation. Secondary recirculation is provided by pumping containment sump water to the steam generators. The recirculation pumps transfer sump water (including spilled secondary side water from the break and containment spray water) to the Refueling Water Storage Tank (RWST). Water from the RWST is then pumped through connections between the Safety Injection System and Main Feedwater System into the steam generators. The flow through the Main Feedwater System is directed through the three feedwater bypass control valves (one for each feedwater flow path)(See Figure 5).

The three bypass control valves close upon receipt of a Safety Injection Signal (SIS) or an Auxiliary Feedwater Actuation Signal (AFWAS) from either train. Both trains of the SIS and AFWAS must be reset before the valves can be opened to provide long-term cooling flow.

SINGLE FAILURES

If either train of AFWAS or SIS fails to reset, all three valves would remain closed, thereby preventing long-term cooling.

RESOLUTION

Plant modifications or procedural changes will be implemented during the Cycle 11 refueling outage to mitigate the effects of these single failure susceptibilities so that the bypass valves can be reopened on demand and secondary recirculation capability assured.

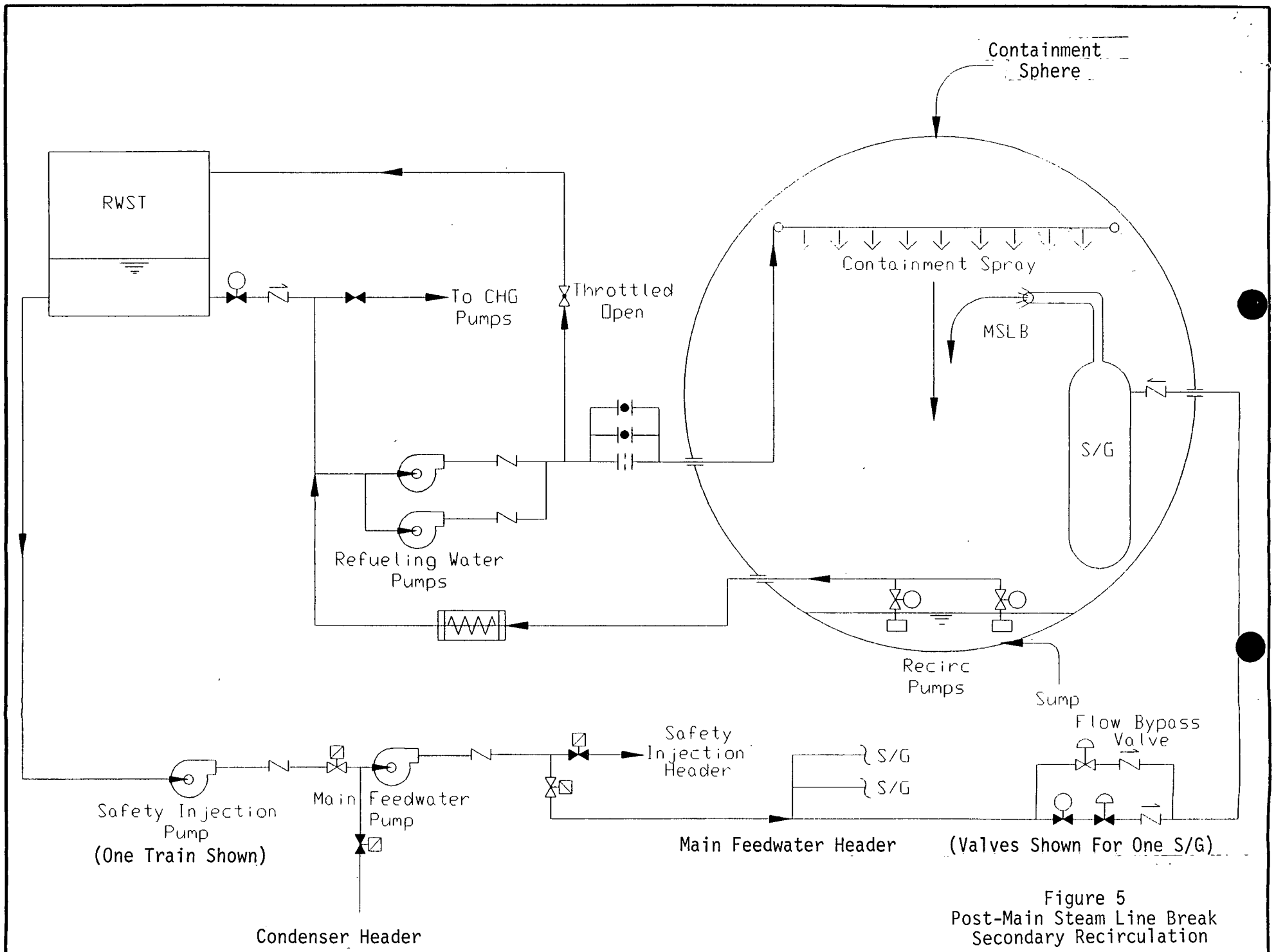


Figure 5
Post-Main Steam Line Break
Secondary Recirculation

6. PARTIAL LOSS OF COMPONENT COOLING HEAT REMOVAL DUE TO LOSS OF SALT WATER COOLING FLOW TO ONE HEAT EXCHANGER

INTRODUCTION

Failure of one train of electrical power could lead to a condition in which Component Cooling Water (CCW) flow is provided to two CCW heat exchangers while cooling is supplied by Salt Water Cooling (SWC) to only one heat exchanger.

BACKGROUND

The SWC system transports heat from the CCW system to the ultimate heat sink. The CCW system is an intermediate cooling loop that transfers heat from safety related systems to the SWC system. Both trains of CCW and SWC are initiated on a Safety Injection Signal (SIS).

Both the SWC and CCW systems are powered from redundant electrical trains. Mechanically, the SWC system has two independent trains, but the CCW system has a common pump discharge header which interconnects the two CCW heat exchangers. The CCW heat exchanger isolation valves on the CCW side (MOV-720A and MOV-720B) fail as-is on loss of power. Figure 6 illustrates both the electrical and mechanical arrangement of the two systems.

SINGLE FAILURE

Loss of either electrical train after a SIS would simultaneously disable one train of the CCW system and one train of the SWC system. As a result, SWC flow through one CCW heat exchanger would cease. However, CCW flow would continue to be split between the two heat exchangers since MOV-720A and MOV-720B fail as-is on loss of power. This would result in a reduction in heat removal capability since the SWC system would be cooling only 50% of the CCW flow.

RESOLUTION

The cooling provided to the CCW system in this configuration may be sufficient to meet post-accident requirements. Further analysis is being performed to determine the acceptability of the current plant configuration. If the analysis does not demonstrate the acceptability of the current plant configuration, plant modifications to correct this condition will be implemented prior to restart from the current outage.

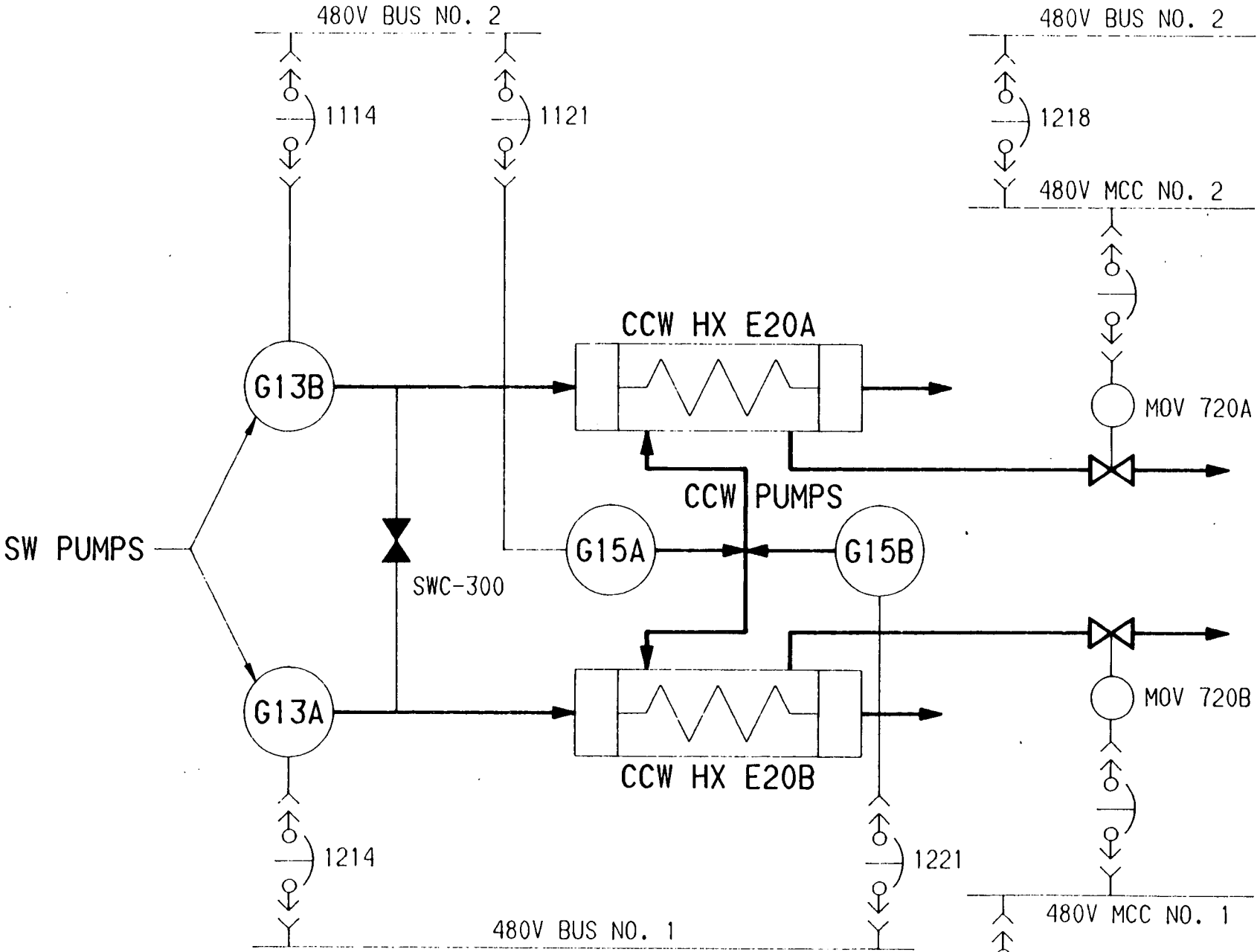


Figure 6. Component Cooling Water and Saltwater Cooling Systems

7. POTENTIAL LOSS OF SALT WATER COOLING

INTRODUCTION

An electrical or mechanical failure which causes the intake structure gates to close and which does not cause the circulating water pumps to stop could lead to loss of Salt Water Cooling (SWC).

BACKGROUND

The SWC system takes suction from the intake structure and provides cooling to safety related systems and components. The intake structure also houses the Circulating Water (CW) system pumps which provide cooling water to the condensers and other non-safety related systems and components (See Figure 7).

The pump arrangement is such that the CW pumps draw suction from a lower level in the intake structure than do the SWC pumps. Seawater inflow passes through an intake tunnel and enters the intake structure via a single gate, either the gate controlled by MOV-9 (during normal operation) or that controlled by MOV-11 (during heat treatment). The gates are suspended above the intake tunnel. The gates close by sliding down slots in the tunnel walls. A stop is provided for MOV-9 to prevent full closure of the gate assuring that approximately 6% of normal seawater inflow is available. No stop is necessary for MOV-11 since this gate is located in parallel with MOV-9. The 6% flow provided through MOV-9 is sufficient to allow continued operation of the SWC pumps. Movement of each gate is controlled by its own motor-operator.

SWC pump operation is required to transfer primary side heat to the ultimate heat sink. CW pump operation is not required post-accident.

SINGLE FAILURE

One intake tunnel supplies seawater to the intake structure. Failure of the open intake gate or its motor-operator could cause the gate to lower and block the majority of flow from entering the intake structure. Since the CW pumps share the intake bays with the SWC pumps and have a lower suction point, operation of the CW pumps would draw down the intake structure seawater to a level below the SWC pumps suction. Both SWC pumps would thereby lose suction and safety related salt water cooling would be lost.

RESOLUTION

Electrically induced failure of the gate motor-operators will be precluded by the addition of an administratively controlled power lockout prior to restart. An engineering evaluation is in progress to determine the need for modifications to the gates. Modifications will be implemented prior to plant restart, if required.

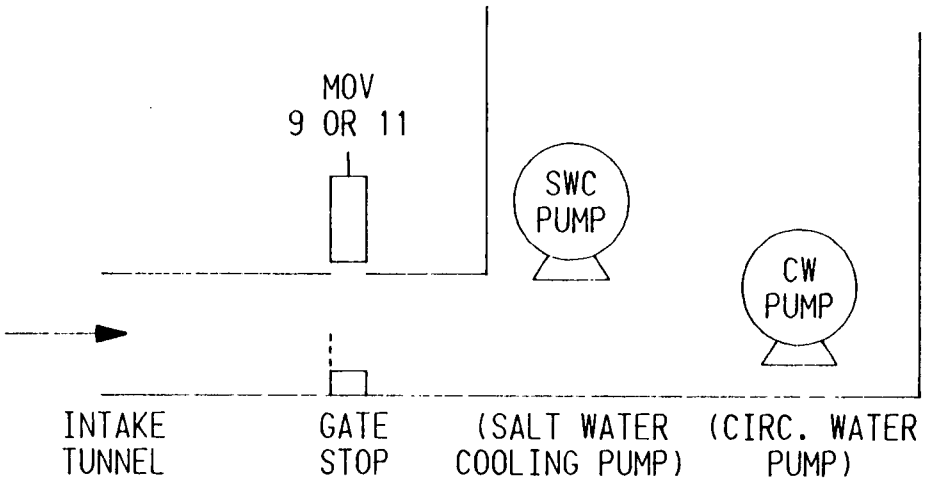


Figure 7. Intake Structure Configuration

8. SEQUENCER LOGIC DEFICIENCY

INTRODUCTION

There are three single failures for which emergency core cooling system (ECCS) initiation may be delayed longer than currently assumed in the safety analysis. These failures affect detection of a loss of power in the Safeguards Load Sequencing System (SLSS) logic.

BACKGROUND

There are two independent safety related 4160 VAC electrical distribution trains consisting of Buses 1C and 2C. These buses supply electrical power to systems and components that are required for normal operation, safe plant shutdown, and mitigation of design basis events. These two 4160 VAC distribution systems are energized by off-site electrical sources through Auxiliary Transformer C. Figure 8 illustrates normal bus alignments (after completion of 480 VAC modifications being implemented during the current outage).

In the event electrical power is not available from off-site sources, each of the two 4160 VAC distribution systems is powered by an emergency Diesel Generator (DG). SLSS Nos. 1 and 2 are designed to automatically start Diesel Generator (DG) Nos. 1 and 2, respectively, upon a loss of offsite power (LOP) signal, a safety injection signal (SIS) or a Loss of Bus (LOB) signal. The LOB signal is provided by under-voltage relays which respond when the voltage on the respective bus decreases to a preset voltage setpoint. A LOB on both Buses 1C and 2C is required for a SLSS to generate a LOP signal.

Upon a SIS with a LOP signal present (i.e., SISLOP), the SLSS trip all loads on the buses, close the DG output breakers, and sequence safety related loads. For a SIS without a LOP, the loads on the bus are not tripped, and all ECCS loads except the Main Feedwater Pumps are loaded in a single block. (The Main Feedwater Pumps have their own time delay relay controlling their restart.) The DGs do not automatically load upon a SIS, LOB, or SISLOB signal.

SINGLE FAILURE

There are three potential conditions in which a single failure could cause a delay in ECCS actuation:

- During emergency diesel generator surveillance testing, the DG is paralleled to its respective 4160 VAC bus. A failure of the DG breaker to trip concurrent with a SIS and loss of offsite power could result in neither SLSS detecting a

SISLOP condition. The SLSS on the affected train would see only a SIS because the diesel generator would maintain the bus energized. This SLSS would attempt to block-start ECCS loads while maintaining power to the NSR loads on its bus. This results in DG overload and a degraded bus voltage condition leading to failure of this train. The other train initially sees a SISLOB condition and will not connect its DG or sequence its ECCS loads until the first train fails. This delay in ECCS initiation is beyond that assumed in the accident analysis.

- During ground fault detection activities on Bus 1C or 2C, the bus is isolated from Auxiliary Transformer C and is repowered from the offsite grid, connected to the main generator, via Bus 1A or 1B. If a SIS event occurs coincident with a loss of offsite power, the SLSS initially detect only a SISLOB since the bus connected to the main generator would not detect an LOB condition. Eventually, voltage on the train connected to the main generator will decrease sufficiently to result in an LOB signal, at which time ECCS loads would be sequenced. This delay in ECCS initiation is beyond that assumed in the accident analysis.

- Failure of the main feeder breaker to open on Bus 1C or 2C concurrent with a SIS event and degraded grid voltage could lead to a failure of ECCS loads to properly sequence. The bus with the failed breaker would remain connected to the grid and would have a degraded voltage condition. Since it would still have voltage, it would not send a LOB signal to the SLSS and thus a SISLOP would not be detected. As a result, the ECCS loads would be block loaded on the train with the degraded voltage and would not be sequenced on the redundant train. The loads on the train with the degraded voltage would not start in the time required by the safety analysis.

RESOLUTION

The first two issues will be resolved by submittal of a proposed technical specification change to enter appropriate action statements during diesel generator surveillance testing and ground fault detection activities.

The third failure identified above is due to a SIS coincident with a degraded grid condition and single failure. Degraded grid protection is the subject of an FTOL issue. Additional degraded grid voltage relays and logic are scheduled for implementation during the Cycle 12 outage in accordance with the FTOL schedules. These modifications will resolve this issue. In addition, this event is due to very low probability coincident events. A PRA analysis will be conducted to reconfirm the acceptability of the current schedule for these modifications.

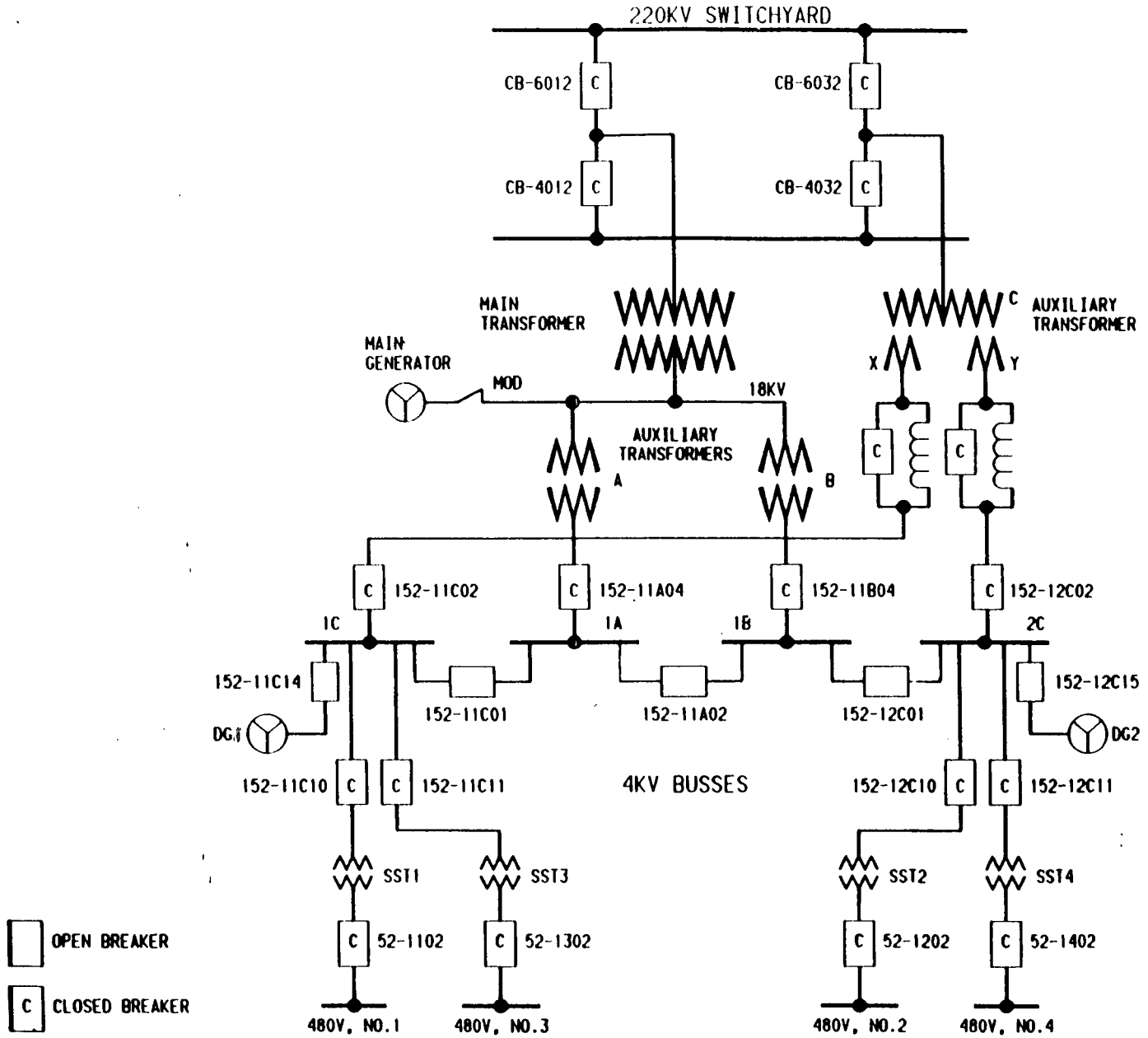


Figure 8. Normal Operational Bus Alignment