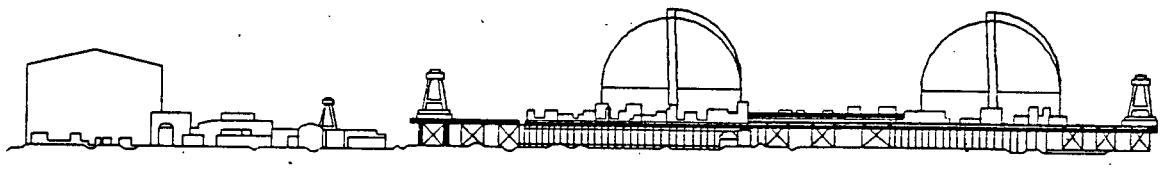
SAFETY ASSESSMENT

SONGS 1 RESTART

March 17, 1989



Southern California Edison Company

San Onofre Nuclear Generating Station

SDGE

TABLE OF CONTENTS

I. SUMMARY

This report evaluates and assesses the readiness of San Onofre Nuclear Generating Station Unit 1 (SONGS 1) to restart from the current Cycle 10 refueling outage in view of the number of design issues and problems which have been identified since the commencement of the outage in November 1988. NRC letters dated January 31, 1989 and February 8, 1989 required that SONGS 1 remain shutdown until all technical issues identified in the letters were resolved.

There are twelve recent technical issues which SCE has identified and resolved prior to return-to-service from the current outage. These specific issues and their resolution to allow restart are listed below:

1. Potential Overloading of 480 VAC Supply Breakers to Busses 1 and 2 - An equivalent breaker was tested and found to be within emergency overload allowances and, therefore, together with the qualification of the associated cables, could serve their safety functions. Additional maintenance, procedure changes and supply cable improvements are being implemented prior to restart.

2. Incorrect Steam Generator Wide Range Level Instrumentation Safety Classification/ Environmental Qualification - The existing safety related, environmentally qualified Steam Generator Narrow Range level instruments are being converted to provide wide range indication.

3. Lack of Charging Pump Motor Rewind Qualification Documentation - Documentation has been assembled to justify continued operation.

4. Incorrect Residual Heat Removal Piping Wall Thickness - The "as found" piping has been analyzed and shown to meet the design requirements for this system. All affected documents have been revised.

5. Residual Heat Removal (RHR) Heat Exchanger Temperature Control Valve Single Failure Causing Potential for Component Cooling Water (CCW) Pump Runout - Both valves are being modified by installing a mechanical stop on the valve stem to allow only partial opening and, therefore, limited flow. In addition, during power operation, one RHR heat exchanger block valve will be closed.

6. Potential Overload of an Emergency Diesel Generator - The design of 480 VAC swing bus 3 has been modified to add automatic isolation from Train A ESF loads for all safety injection events.

7. AFW Tank Volume Requirement - The AFW tank volume calculation is being formally revised to reflect actual requirements.

8. Refueling Water Pump Jumper Wire - The jumper wire was removed and the pump tested satisfactorily for operability.

9. Containment Spray Flow Diversion - Power to CV-92 pilot solenoid valve will be isolated by redundant means, preventing spurious opening of the valve.

10. Core Monitoring Technical Specifications - Proposed changes to affected technical specifications have been submitted which preclude the plant from operating in a potentially unanalyzed condition.

11. RCP Sheared Shaft and Locked Rotor Reactor Trip - Modification of the Reactor Coolant Pumps overcurrent trip (locked rotor events) and addition of an undercurrent trip (sheared shaft events) provide protection for these events as specified by the accident analyses.

12. Diesel Generator (DG) Load Sequencing Logic - Modification to add a time delay upon reset of the undervoltage signal to each sequencer to ensure closure of both DG breakers.

The items above constitute the issues and corresponding actions being taken prior to restart. Additional longer term actions for each of these issues are addressed in detail in

the body of the report. The Thermal Shield issue discussed in the NRC's January 31, 1989 letter is being addressed separately. Items 1 through 6 correspond to the first six items listed in the NRC's February 8, 1989 letter. The seventh issue in the NRC letter (steam generator tube sleeving) is not related to those addressed in this report and has been the subject of separate correspondence and SCE's actions relative to this issue were approved by NRC letter dated February 23, 1989. The additional issues have been identified since issuance of the February 8, 1989 letter or are items SCE feels should be included in the report. SCE has put the scope of these twelve issues into perspective by determining the root cause of each and by evaluating their safety significance.

Nine of the issues identified above were associated with the adequacy of technical support, while three are attributed to other unrelated causes. By performing root cause analyses, it was determined whether historical technical support shortcomings resulted in significant embedded deficiencies. The result of this review confirmed what SCE reported in our October 3, 1988 letter discussing SCE's program for improving engineering and technical support for San Onofre. The identification of these issues is a positive sign that the changes identified, and in the process of being implemented, are having a significant positive effect on the quality of SCE's engineering and technical activities.

By performing safety significance evaluations of all the issues, perspective has been given to the overall impact of potential future issues. All of the issues identified above have relatively minor safety significance. Studies and evaluations performed in the past have identified most obvious issues and it is only the less obvious and less safety significant issues which have been discovered during this outage, primarily due to SCE's recent effort to improve the quality of engineering and technical support to SONGS. While it is likely that similar issues will be identified as implementation of the recommendations identified in our October 3, 1988 letter continues, SCE considers that future issues will have a similarly low safety significance so that continued plant operation will not impact the health and safety of the public.

SCE plans to return SONGS 1 to power (with NRC concurrence) and continue our program to upgrade our technical capabilities and develop design bases documentation. Based upon the recommendations in this report, some minor redirection of our efforts identified

in our October 3, 1988 letter will take place. The primary changes involve an accelerated schedule for reanalyzing the 1976 single failure analysis and prioritizing development of the design bases documents for the component cooling water, electrical and reactor systems.

Considering the successful resolution of the above identified issues, their low probability of occurrence, and given the inherent flexibility of SONGS safety systems to mitigate postulated accidents along with likely operator actions, there is reasonable assurance that operation of SONGS 1 can continue without undue risk to the health and safety of the public.

II. INTRODUCTION

As part of our activities related to the Safety System Functional Inspection (SSFI) conducted by the NRC, in June of 1988 SCE established a Task Force to perform an Independent Assessment of the Engineering and Technical Support to the San Onofre Nuclear Generating Station. One of the primary purposes of the Independent Assessment was to identify and determine the causes of programmatic deficiencies in the engineering and technical support to SONGS and to recommend specific actions to improve quality. The results and recommendations of the Task Force were transmitted to the NRC by letter dated October 3, 1988. As indicated in the October 3, 1988 letter, SCE's nuclear design related activities were consolidated within one department to focus the responsibility for all design-related engineering to more efficiently and effectively utilize resources and improve quality. The increased focus of this new organizational structure has helped to identify many of the issues which have been recently reported to the NRC. In order to assess the effectiveness of our planned corrective actions based on these recently identified issues, a special evaluation was initiated. Shortly after this effort was initiated, SCE received a request from the NRC for a similar study. The SCE effort was then modified to encompass the NRC concerns.

The scope of the evaluation is as follows:

(1) Evaluate the significant SONGS 1 design and configuration issues identified since the organizations responsible for design were reorganized.

(2) Evaluate the adequacy of actions underway to correct the underlying root causes of these issues in order to identify the need for any further programmatic changes.

(3) Evaluate the overall safety significance of these issues in order to determine readiness of SONGS 1 to resume operation.

(4) Identify ongoing or planned evaluations which are likely to result in additional significant issues.

Following this brief introduction, Section III of this report identifies each significant technical and configuration issue. For each, the concern is described, the method of discovery discussed, root cause and corrective action identified, and actual safety significance evaluated.

In Section IV of this report, some of the corrective actions previously undertaken by SCE as indicated in our October 3, 1988 letter are reevaluated in light of the technical issues identified in this report. Specifically, the root cause determinations and corrective actions are evaluated to determine the effectiveness of existing programs to correct these issues and evaluate the need for supplemental activities or enhancements.

Section V of this report evaluates the overall safety significance of these issues in relation to continued operation of SONGS 1. Finally, Section VI provides SCE's overall conclusions regarding these issues and provides the basis for plant restart.

It is important to recognize that SONGS 1 represents a special challenge from a technical perspective. The Unit was designed and built in the middle 1960's as a turn-key plant. Much of the regulatory guidance which has since established a degree of standardization in the industry was not available for SONGS 1. Documents describing the technical basis for some aspects of SONGS 1 design have not been retained (nor were they required to be retained); and what have become the present industry standard methods of analysis are often neither appropriate nor sufficient at SONGS 1.

From a technical standpoint, the different design concepts employed between SONGS 1 and a standard plant impact identification of single failures. Standard plants were designed with train level redundancy and separation criteria and consequently single failures are readily identifiable. However, SONGS 1 was designed with component level redundancy and operational flexibility criteria, resulting in a configuration with redundant components in common-header fluid systems, automatic swing busses and safety related power for non-safety related loads. These SONGS 1 features require evaluating potential failures at various times in given accident scenarios to account for the train interactions through the common header or swing bus configurations. This time dependence of potential failures complicates the identification of single failure susceptibilities at SONGS 1.

Despite this analytical complexity, the component level redundancy and operational flexibility criteria used in SONGS 1 are inherent strengths for responding to the vast majority of events. For example, in standard plants, the Component Cooling Water (CCW) system is composed of two essentially separate piping trains, each with one pump and one heat exchanger. At SONGS 1, the CCW system consists of three pumps with common suction and discharge headers piped to two heat exchangers, also with common suction and discharge headers (Attachments C, D, E, and F provide diagrams of the SONGS 1 Safety Injection, AFW and CCW systems; and the SONGS 2/3 CCW system for illustration purposes).

In a standard plant, taking a heat exchanger out of service for maintenance makes one entire train of CCW and the systems it supports inoperable. At SONGS 1, the impact is minimal since the other (100% capacity) heat exchanger serves all components. Similarly, a CCW pump's failure to start on demand during an accident at a standard plant incapacitates an entire train of CCW and the systems it supports until a "swing" pump can be aligned; at SONGS 1, a standby pump would immediately auto start, again resulting in minimal impact from the failure. Conversely, a pipe break in one of SONGS 1 common headers, would appear to have more significance than a similar break in a standard plant due to its train piping separation. However, SONGS 1 can provide safety-related power to all normal non-safety related loads, to provide diverse means of cooling if needed. Further, previous backfitting of SONGS 1 to meet modern criteria has improved the inherent strengths while making the design more complex and difficult to understand.

In reviewing the succeeding sections of this report, the reader should keep this special nature of SONGS 1 in mind. Issues which might on the surface seem significant, may be easily coped with at SONGS 1 because of the component level redundancy and operational flexibility concepts employed in the original design.

III. SIGNIFICANT TECHNICAL ISSUES

A review was conducted of technical issues which have been reported to the NRC and ongoing evaluations active within SCE. Twelve technical issues were identified which are of concern to SCE. Many of these issues are the result of a prior lack of adequate engineering and technical support which SCE recognized and corrected as indicated in our letter dated October 3, 1988. The issues of thermal shield integrity and steam generator tube sleeving are not addressed here since these issues have limited generic implications. By letter dated February 23, 1989, the NRC indicated that our actions regarding the steam generator tubes were acceptable. NRC review of the thermal shield issue is currently in progress. The twelve issues of concern are:

(1) Supply breakers to 480 VAC busses 1 and 2 could have been overloaded during some design basis scenarios.

(2) Environmental Qualification of steam generator wide range level indication was not performed as required by design documents.

(3) The environmental qualification data package for Charging Pump G-8B did not consider a motor rewind in 1972.

(4) A section of the Residual Heat Removal System was constructed of schedule 120 pipe instead of schedule 160 in apparent conflict with plant drawings.

(5) Component Cooling Water temperature control valves to the Residual Heat Removal System could fail open during certain design basis scenarios and potentially cause runout of CCW pumps.

(6) Configuration of 480 VAC bus 3 following single failure was inconsistent with the configuration used in the emergency diesel generator loading calculations.

(7) The calculation for the required inventory in the auxiliary feedwater storage tank did not properly account for the cooling water to AFW pump G-10S bearings which drains to a sump.

(8) A jumper wire was discovered in the control circuit for a refueling water pump which would have prevented the pump from starting during some design basis scenarios.

(9) A single failure scenario was discovered involving the containment fire spray header which could reduce the effectiveness of the containment heat removal function.

(10) The Technical Specifications concerning axial offset and core monitoring were inadequate to assure that the plant would operate within its design basis.

(11) The reactor trip inputs intended to provide backup protection from a reactor coolant pump sheared shaft or locked rotor event, would not have functioned as required.

(12) The Safeguard Load Sequencers may prevent automatic breaker closure and loading of one train during a SIS/LOP.

The increased focus and awareness of the new engineering design organization has been successful in identifying these problems. Most were detected as a result of new design work initiated during the current SONGS 1 Cycle 10 refueling outage. It is likely that similar problems will be uncovered in the future due to continued study of SONGS 1 design. These design studies include the Design Bases Document effort, revalidation of the 1976 NUS performed Single Failure Analysis, ongoing design changes, and reviews that result from IE Bulletins, INPO SOER's and applying current regulatory criteria to SONGS 1 (e.g., HELBA). In order to determine the potential impact of similar issues which may remain to be discovered, the safety significance of the twelve known issues was examined. Each of these issues involves a nonconformance with some aspect of plant design or design criteria. However, alternative indications, diverse or redundant equipment, likely operator actions, or the low probability of the accident scenario provides reassurance that

the safety significance is small. Because of this, accelerated corrective action is not necessary and current SCE plans to continue with our program to develop design basis documentation and upgrade technical capabilities is acceptable as is, or as supplemented by "Follow-up Actions" associated with the twelve issues discussed in this report. Each Follow-up Action has a sequential number assigned to it as it appears in the text. Section VII of the report provides a summary listing of all the follow-up actions.

The following are the results of the evaluation of each of the twelve issues.

1. POTENTIAL OVERLOAD OF 480V SWITCHGEAR MAIN BREAKERS

ISSUE: The peak loading on 480V Switchgear 1 and 2 could exceed the continuous current rating of their main breakers following a safety injection actuation under the worst postulated combination of non-essential and safety related loads starting and operating.

Calculation results indicate that, following a Safety Injection Signal (SIS) actuation with the worst postulated combination of non-essential and safety related loads starting and operating, the peak loads on 480V Switchgear 1 and 2 would exceed the continuous current rating of their main breakers (52-1102 and 52-1202). The subject breakers (Westinghouse Model DB-50) are rated at 1600 amps continuous and the load currents for the two breakers are conservatively calculated to be 1896 and 1640 amps (at approximately 460V), respectively. This condition would result in breaker heatup which eventually could result in breaker degradation and potential loss of power to both trains of the 480V buses. This problem does not occur following a SIS actuation with a concurrent Loss of Offsite Power (SISLOP) event because the non-essential loads are automatically shed and locked out, thus eliminating the overload condition.

REFERENCES: NCR S01-P-7009, January 30, 1989
LTR SCE to NRC, February 21, 1989
LER - None required

DISCOVERY: To support implementation of Cycle 10 design changes, electrical calculations were being revised to evaluate the effect of adding additional post-SIS loads onto the electrical distribution system. Using the latest design basis information and the present worst case post-SIS bus loads, the calculations revealed that the pre-modification worst case loading conditions exceeded the continuous duty name-plate breaker rating. This was reported to the NRC on January 30, 1989 via a 4-hr phone notification and follow-up letter.

ROOT CAUSE: SCE has not been able to definitely determine the root cause for this error. However, SCE is aware of possible generic calculation deficiencies. This issue appears to be related to an inexperienced design staff. As discussed in our October 3, 1988 letter, SCE has already initiated actions to correct this problem.

CORRECTIVE ACTION: In order to determine whether the breakers had sufficient design margin above the 1600 amp continuous rating to handle the worst postulated post-SIS load profile (1896 amps), a test was performed on an equivalent DB-50 breaker. The test was performed to determine the effects of heating on the breakers during the postulated overload conditions. The test guidelines were based on ANSI C37.50, "Test Procedures for Low-Voltage AC Power Circuit Breakers Used In Enclosures." The test results were used to predict temperatures of critical breaker components (contacts, insulation and bus connections) for the worst postulated current profile based on graphical and analytical techniques. The predicted temperatures were plotted against time (Attachment G) and then compared to ANSI maximum recommended values. It was found that, under worst case conditions, some of the ANSI recommended temperatures would be exceeded. However, the additional temperature rise allowed by ANSI for four-hour breaker emergency overload conditions would not be exceeded. For the purpose of this evaluation, an ambient temperature of 40 degrees Centigrade (conservative) and a switchyard voltage of 230KV (most probable) were assumed. The test breaker was inspected following the test and neither the insulation nor contacts were degraded and the breaker performed acceptably throughout the test.

In addition to the main breaker overload issue, an analysis was performed to determine whether the remainder of the auxiliary electric system was capable of handling postulated worst peak loading. The analysis concluded that acceptable performance of the auxiliary electric system would be maintained, although the station service transformer rating and power cable ampacities would be exceeded. Based on the four-hour limits prescribed in ANSI C57.92, the transformer overload condition (133% of 1400 KVA OA rating at 65°C rise) would result in a negligible loss of transformer life, even without crediting the transformer forced air fans. The main power cables feeding 480V Switchgear #1 are routed through a 34 inch fire barrier and are also randomly laid in a section of covered cable tray. This condition would require that the cables be further derated due to the thermal effects of the fire barrier and the random lay of the cables. The resulting ampacity of the cables is below the postulated worst case load current. Although these cables could have exceeded allowable design temperature limits, they would have operated satisfactorily based on their tested capability to operate in high temperature LOCA environments (these are EQ cables located in a mild temperature environment).

Based on the breaker test and analysis, the main 480V breakers will continue to be used for one refueling cycle. The corrective actions to be completed prior to returning to service from the Cycle 10 outage are as follows:

1. Perform preventative maintenance on main 480V breakers and their spares per station maintenance procedures to ensure that the installed breakers are in the same condition as the tested breaker.

2. Revise operating procedures to require operator surveillance of Station Service Transformer loading within four hours after a safety injection actuation and make necessary adjustment of 480V switchgear loading if required to achieve acceptable continuous levels.

3. Rework the fire barrier to the required designed depth of 10 inches to ensure that adequate current carrying capability exists on the main power cables for 480V Switchgear #1.

4. Modify cable tray covers to improve cable ampacity.

In addition, the following options will be investigated for possible long term corrective action for this condition. A viable solution will be selected and implemented prior to restart from the Cycle 11 refueling outage.

1. Rerate breakers to postulated maximum current value.

2. Replace breakers with breakers which are rated to continuously carry the maximum current.

3. Implement design modifications and/or operator and control actions to ensure that the present current rating of the existing breakers will not be exceeded.

SAFETY SIGNIFICANCE: The postulated overload condition would result in peak load currents above the continuous ratings of the breakers, transformers, and cables eventually causing overheating of breaker and transformer components and cables. The heat up of these components is not instantaneous and would be gradual over the course of several hours. Assuming that no action would have been taken by the operators, the temperature reached by the breaker and transformer components and cables, although over ANSI limits, would have resulted in thermal aging of the components rather than complete failure. The test breaker was subjected to sustained (3 hours) temperatures greater than 15°C above ratings and peak temperatures as high as 90°C above ratings with no indication of impending failure. In accordance with ANSI C57-92, the transformers would have remained within allowable overload limits with some loss of life. The cables have a documented capability to survive high temperature LOCA environments in excess of the temperatures that would occur due to the postulated overload condition. Based on these conclusions, failure of the breakers or cable due to the postulated overload condition is not credible and even though SCE prudently reported it initially via a four-hour phone notification and follow-up letter, the condition was determined not to be reportable under 10 CFR 50.72 or 50.73.

2. STEAM GENERATOR WIDE RANGE LEVEL INSTRUMENTATION

ISSUE: SONGS 1 did not have Safety Related and environmentally qualified Steam Generator Wide Range (SGWR) level indication in the Control Room. This instrumentation should have been installed to provide redundant Auxiliary Feedwater (AFW) system flow indication as committed to in a letter submitted to the NRC on January 5, 1981. The letter was in response to the post-TMI Action Plan, Item II.E.1.2.

REFERENCES: LER 1-88-20, dated January 9, 1989
NCR SO1-P-6813, dated January 23, 1989

DISCOVERY: During Cycle 10 refueling design change work, power was turned off to a non-safety related lighting panel which resulted in the loss of power to the SGWR level sigma indicators in the Control Room. This occurrence resulted in a condition that was non-conforming with respect to updated FSAR Section 10.4.7.3.2 which specified that "Each steam generator instrumentation system is powered from a separate 120-V-ac vital bus to maintain its independence". The level transmitters themselves were correctly powered from safety related regulated busses 1, 2 and 3, while the associated Control Room sigma indicators were powered from a non-safety related lighting panel (panel L-5 breaker 30). The referenced NCR was written against this condition and all commitments were reviewed concerning the SGWR level system. The post-TMI Action Plan requirement for SGWR level system was identified during the commitment review. Further evaluation of the as-installed equipment determined that the existing SGWR level system loops were not environmentally qualified which was also contrary to the post-TMI Action Plan requirement.

ROOT CAUSE: The need to implement a plant modification to satisfy the NRC commitment had not been clearly defined in the normal Licensing Commitment List tracking mechanism (LCL). A commitment was identified in the LCL as entry TMI 80-004 which referenced the January 5, 1981 letter. However, the LCL entry simply noted that all TMI equipment required Environmental Qualification (EQ) by June, 1982. The LCL entry was general in nature and did not call out the specific requirements for each piece of affected equipment. The requirement to qualify post-accident TMI equipment was later deferred by the issuance of 10 CFR 50.49 regarding environmental qualification of electrical equipment. As part of this deferment, LCL item TMI-80-004 was closed and the requirement to environmentally qualify post-accident equipment was included with LCL item SEP-80-001.

In accordance with 10 CFR 50.49, SEP-80-001 required qualification of all equipment (including post-accident equipment) to Division of Operating Reactors (DOR) guidelines by March 31, 1985. The LCL entry, SEP 80-001, did not include the January 5, 1981 letter as a reference nor cross-reference the previous LCL entry, TMI-80-004. The specific requirement associated with the SGWR level instrument upgrade was never satisfied by implementation of the necessary plant modifications. This issue is related to commitment management weaknesses. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this problem.

FOLLOW-UP ACTION NO. 1

LCL entries will be reviewed for possible omissions similar to the SGWR level transmitter commitment. The scope of this review will be 10% of all entries between 1979 and 1982 and will be completed within six months after return to service.

CORRECTIVE ACTION: To comply with the NRC commitment, the existing safety related environmentally qualified Steam Generator Narrow Range (SGNR) level instruments will be converted to provide wide range indication prior to SONGS 1 restart from its Cycle 10 outage. AFWS flow and SGWR level instrumentation commitment reviews have been completed and all other open issues are presently carried on the appropriate tracking lists.

It is appropriate to expect that SCE's Design Bases Documentation (DBD) program, described in our letter to the NRC dated January 9, 1989, would identify and resolve a deficiency such as that described above. As a part of our review of SONGS 1 restart, the DBD program plans were reviewed to determine if any modifications are needed to increase our confidence that the program will identify similar discrepancies. One change to an existing checklist was identified.

FOLLOW-UP ACTION NO. 2

A cross check of TMI Action Plan references and the Systematic Evaluation Program (SEP) Integrated Safety Assessment will be added to the DBD preparation checklist. This change provides two separate DBD reference document search paths for those requirements related to these programs.

SAFETY SIGNIFICANCE: The SGWR level indication has no safety system actuation function, and serves only as an alternate indicator of AFWS flow initiation/operation (the AFWS flow instruments being the primary devices). For the most limiting events which require AFWS operation (such as feedwater line break events), the applicable transient analyses show that the steam generators reach dry out conditions and remain at essentially zero level indication for several hours, even with maximum AFWS flow. Therefore the value of SGWR level instrumentation is not significant during these most limiting events.

The unavailability of SGWR level indication does not preclude the ability of the operators to implement the response strategy of Emergency Operating Instructions (EOI's). The SONGS 1 EOI's provide both event and symptom-based guidance that has as its basis the continued operational mode of six critical safety functions which ensure the continued integrity of designed barriers against any radioactive release. One of the six safety functions is that of "heat sink", and it is the one directly impacted by the lack of SGWR level indication. Specifically, within the loss of heat sink EOI, level indication is used as: (a) a criterion in determining the need to initiate RCS bleed and feed during a loss of secondary heat sink situation and (b) an indicator of steam generator dryout. In the first case, available alternate instrumentation that is utilized includes RCS pressure, T-hot Resistance Temperature Detectors (RTD's), Core Exit Thermocouples (CET's) and Pressure Operated Relief Valve (PORV) position indication. In the second case, AFW flow and RCS delta-T (T-hot and T-cold RTD's) are used as alternate instrumentation. All of these parameters are monitored by safety related, environmentally qualified instrumentation with the exception of the CET's. Therefore, there was low safety impact by failing to have the SGWR level instrumentation appropriately powered or environmentally qualified.

3. CHARGING PUMP MOTOR G-8B REWIND QUALIFICATION

ISSUE: The SONGS 1 South Charging Pump Motor (G-8B) was found to have been rewound in 1972. This pump motor is required to be environmentally qualified (EQ) in accordance with 10CFR50.49. The EQ Data Package (EQDP) was based on the original winding material, not the rewind material.

REFERENCE:
Memo For File, July 21, 1972
Letters - SCE to NRC dated December 29, 1988 and February 2, 1989; Subject: Recertification of Charging Pump Motor Rating SONGS 1.
NCR S01-P-6764, dated October 23, 1988
LER - None required

DISCOVERY: On July 22, 1988, following a discovery that the charging pump motors would have operated beyond a 1.15 service factor during the initial safety injection and recirculation phases, the NRC imposed Operating License Condition 3.L(6) on SONGS 1. This Operating License Condition required that the pump motors be recertified or rewound to a higher rated service factor which enveloped their accident operation or be replaced with motors having an appropriately higher service factor. A thorough review of the pump motor's maintenance history was conducted to develop data necessary for motor recertification by Westinghouse. During this review, an SCE Memo for File was identified which indicated that G-8B was rewound in 1972 following a pump seizure. Confirmatory documentation was then located at Westinghouse's Compton Repair Facility where the pump motor rewind was accomplished.

ROOT CAUSE: The primary root cause lies in the failure of personnel who developed the EQDP to have thoroughly researched all possible records to determine the actual configuration of the pump motor. A contributing factor is the less stringent equipment configuration assurance procedures which were in effect early in the life of SONGS 1. The pump motor rewind met all specifications in place at the time. These specifications only required that the pump motor meet Class B insulation criteria and did not require that the rewind material be identified or documented. When the EQDP was prepared, there were no obvious indications (e.g., a rewind label on the pump motor or entry in the maintenance history records) that a rewind had taken place. Previous EQ reviews by other

organizations (Bechtel and Wyle Labs) also failed to identify this rewind. This issue is related to changing standards for design basis documentation. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this type of problem.

CORRECTIVE ACTION: A review of the SONGS 1 Operating Logs and NCR's has been completed to determine if any other pump or fan motors requiring EQ have been rewound or repaired. The Operating Logs and NCR's were selected as they are considered to be the most complete, accessible and reliable source of information. The Operating Logs are quite detailed, noting time and reason when important equipment is taken off line or put back on line. Although the level of detail regarding Operating Log entries varies as a result of different personnel making the entries, there is no significant variance in detail between periods of plant operation and outages. Whether in an outage mode or at power, the Operating Log entries clearly identify when equipment is taken off line or removed from the plant for repair, and typically provide details relative to any associated problems. Each day a summary equipment status is also provided at the mid-night entry which lists all out-of-service equipment and usually indicates if it has been removed from the plant as well.

The Operator Log review disclosed entries dated April 30, 1972 regarding the Charging Pump Motor G-8B failure and the need to take it out of service for repair. In addition, the May 10 & 12 entries indicated that the pump was reinstalled and the clearances lifted. It is noted that none of these log entries stated that the motor was rewound. Entries were also found in 1983 which identified that one of the refueling water pumps required removal and rework. Further investigation of this entry determined that the pump motor was sent to an offsite facility to dry its windings. This activity had no impact on the pump motor's EQ status. Another log entry stated that an auxiliary feedwater pump motor was rewound. Further investigation revealed that the repair was properly documented in the appropriate EQDP. No other entries were found concerning EQML pump or fan motors which might affect their EQ status.

The computerized NCR listing was reviewed for key words "rewind", "winding", and "rewound". No EQML pump or fan motors' rewind efforts were identified in this review.

Only EQML pump and fan motors were considered within the scope of the Operating Log and NCR review since it would have been standard practice (due to cost and schedule impact) to simply replace all other failed EQ equipment (such as cables, transmitters, or solenoid valves). These "replacement" equipment items have previously been walked down in the plant and verified to match their EQDP entries. The only exception to the walkdown method of verification was valve motor operators. However, configuration assurance relative to this equipment was thoroughly established in 1986-87 as the result of the MOVATS program and SCE's response to NRC concerns on the Limitorque actuator EQ status.

Additional actions to be implemented by return-to-service from the next refueling outage may be either of the following:

1. Rewind the pump motor to the higher rated service factor in accordance with existing qualification requirements,

2. Replace the pump motor with a qualified motor with the higher rated service factor.

SAFETY SIGNIFICANCE: Although most documentation related to the charging pump motor rewind had been routinely purged by Westinghouse, an extensive investigation found enough evidence (e.g., standard rewind procedures in place at the time and recollections from involved personnel) to prepare and submit a Justification For Continued Operation (JCO) in accordance with the requirements of 10CFR50.49. Based on data and test results from different sources, the JCO conclusion was that the material used in the rewind operation is qualified for operation in its post-accident environment and the motor would perform as required in the existing configuration. Therefore, there is low safety significance as a result of the charging pump motor rewind.

4. RESIDUAL HEAT REMOVAL PIPING WALL THICKNESS

ISSUE: The SONGS 1 Residual Heat Removal (RHR) suction piping (Line RCS-5002-8"-2501) was found to have a wall thickness corresponding to schedule 120 pipe, whereas the SCE design documents for this line specifies schedule 160 pipe.

REFERENCE: NCR S01-P-6896, dated January 12, 1989
LER - None required

DISCOVERY: In determining what calibration blocks (CB) were going to be used for the SONGS 1 Refueling In-Service Inspection (ISI), it was noted that the CB required for the weld examination (RHR Weld 5002-7) could not be located. On January 4, 1989, a Westinghouse NDT Technician performed an ultrasonic test (UT) thickness check on the pipe in question to justify the use of a substitute CB. This inspection identified a potential discrepancy between the actual wall thickness and the thickness specified in the SCE documents. The piping discrepancy was verified by an SCE NDE Level III examination and reported to Station Technical on January 12, 1989. A Nonconformance Report (NCR) was issued at that time. The RHR return line (RCS/RHR-3001-6") was UT inspected and determined to be schedule 160 pipe.

ROOT CAUSE: Although the SCE Line List identifies the suction line as 8 inch schedule 160 pipe, revision 4 to the Westinghouse Piping Specifications for SONGS 1 identifies the subject line as being 8 inch schedule 120 piping. In 1984, stress calculations were performed for these lines as part of the SONGS 1 seismic upgrade analysis for Long Term Service (LTS). Impell, in performing the stress calculations, utilized SCE's piping material specifications (Line List) which indicated that the RHR suction piping was schedule 160. Although previous events can not be reconstructed, it is possible that SCE's piping material specification is based on an earlier revision to the Westinghouse Piping Specifications which may have specified the RHR suction line as being schedule 160 sometime prior to Revision 4 of the line list. Due to the difficulty in recovering data from the time period prior to Revision 4, it is presently impossible to conclusively establish the root cause for the discrepancy. A document search is being performed at the Bechtel Power Corporate Retention Center in order to obtain information regarding the original suction line installation. This information, if located, may be helpful in understanding this record

discrepancy. This issue is related to changing standards for design bases documentation. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this type of problem.

CORRECTIVE ACTION: All affected documents, including the stress calculation, for the RHR suction line were revised to reflect the change to schedule 120 pipe. An analysis indicated acceptable stress levels using schedule 120 pipe.

For those lines in which the ISI Program (M-documents) obtained a wall thickness value, comparisons of thickness values with design requirements is being conducted.

FOLLOW-UP ACTION NO. 3

A review of all ISI data sheets completed during this second 10-year interval (1978 to present) is in progress. The purpose of this review is to compare wall thickness measurements for large bore Class 1 and 2 pipe included in the ISI program with SCE design documents for any additional piping schedule discrepancies. This review will be completed by May 31, 1989. The review of piping inside containment will be completed before SONGS 1 restart.

SAFETY SIGNIFICANCE: The stress calculation for the subject piping (Impell Calc. RC-107) was reviewed with respect to the as-found condition of the piping (i.e., schedule 120 vs. schedule 160). It was determined that the as-installed piping meets all applicable code requirements. Since the present piping would have fulfilled the design function, there is low safety significance to the discrepancy.

5. CCW FLOW TO RHR HEAT EXCHANGER TEMPERATURE CONTROL VALVE SINGLE FAILURE

ISSUE: SONGS 1 has two parallel Residual Heat Removal System Heat Exchangers (RHR HX's), both of which are served by the Component Cooling Water (CCW) system. CCW also serves other safety related systems (Attachment D) required to mitigate the consequences of a Design Basis Event (DBE) such as a Loss Of Coolant Accident (LOCA). CCW flow through each RHR HX is controlled by an air operated, fail open valve (TCV-601A and TCV-601B) in each heat exchanger return line to the CCW pumps. Both RHR HX control valves are provided air from the same non-safety related header. During a design basis accident, failure of the non-safety related air system would cause both valves to fail to the open position. A concurrent single active failure within the CCW system or electrical train would also have to be assumed. As a result, the remaining CCW pump would try to serve both RHR HX's, potentially resulting in CCW pump runout. This situation could result in cavitation and air-binding of the single operational pump and loss of all CCW flow.

REFERENCES: LER 1-89-03 dated February 27, 1989
NCR S01-P-7005, dated January 28, 1989

DISCOVERY: The NRC issued Generic Letter 88-14, "Instrument Air System Problems Affecting Safety Related Equipment" on August 8, 1988, which requested that licensees perform a variety of verification activities related to the Instrument Air System and the equipment served by the system. A multi-discipline task force was set up within SCE to develop a response to the Generic Letter and thoroughly review the SONGS 1 Instrument Air System. During this review, the failure state of the valves (open) and their potential impact on system performance during post-accident conditions were recognized.

ROOT CAUSE: A contractor performed a Single Failure Analysis (SFA) for SONGS 1 Emergency Core Cooling System (ECCS) in 1976. The failure mode of the CCW RHR HX isolation valves was not addressed in this study. Further, no hydraulic calculation related to the original CCW system design could be located which addressed the single failure condition. A previous study of the air system failure consequences, performed in 1983, addressed the consequences of TCV-601A/B failure only on their normal RHR function but not the post-accident condition, due to the narrow focus of the study.

The root cause of these discrepancies can not be positively established at this time. However, the root cause appears to be related to the excessive use of contractors not familiar with the plant design, a lack of qualified personnel to properly oversee the contractor's efforts, a lack of a readily accessible Design Bases Document and failure to have individuals trained on the integrated system design. As discussed in our October 3, 1988 letter, SCE has already initiated actions to correct these problems.

CORRECTIVE ACTION: As an interim corrective action, prior to restart from the current Cycle 10 refueling outage, one valve will be isolated in Modes 1 through 3 by closing a manual block valve. Both valves will have a mechanical stop installed on their stem to limit the degree to which they can open. Analyses have established acceptable flow rates for both normal and post-accident conditions in Modes 1 through 3, assuming a single failure of one safety injection/electrical train. Further tests have been conducted to confirm the adequacy of the modification. In Modes 4 and 5, both block valves will be opened. Analyses have established acceptable flow rates for both normal and post-accident conditions in Modes 4 and 5, assuming a single failure of one RHR train. (In accordance with the Technical Specifications, operation of both safety injection/electrical trains is assumed in Mode 4 without single failure.) Long term corrective action is under evaluation and includes the possibility of separating the power supplies to the valves, changing the valve failure mode, etc.

FOLLOW-UP ACTION NO. 4

A reanalysis of the 1976 ECCS and supporting systems Single Failure Analysis will be completed within nine months of plant restart.

FOLLOW-UP ACTION NO. 5

The design basis document review will be conducted for the CCW systems at all three Units on a best effort basis utilizing qualified SCE resources. As a result, the CCW systems for SONGS 2 and 3 will be performed in 1989 and SONGS 1 in 1990.

SAFETY SIGNIFICANCE: It has been determined that the most limiting events for impact of the TCV failures are LOCAs during Mode 1. (An overall assessment of the TCV failure impact on FSAR events is provided in Attachment B2.) A total loss of CCW flow concurrent with a design basis LOCA results in loss of containment heat removal by the recirculation heat exchanger during the post-LOCA recirculation mode. The recirculation heat exchanger removes heat from the containment sump water which is recirculated to the core and to the containment sprays. Without the recirculation heat exchanger, spray effectiveness would be decreased and containment heat removal would be provided only by condensing heat transfer to passive heat sinks and to the containment sphere inside wall. Containment pressure and temperature would increase during the recirculation mode with potential effect on pump NPSH and EQ profile unless operator action is taken to restore CCW flow or provide other means of heat removal. These effects are discussed in the evaluations provided below.

The safety significance of a total loss of CCW flow was assessed by consideration of three cases.

Case 1: LOCA occurs and TCV-601A/B fail open. No single failure is assumed. One CCW pump is running and the standby CCW pump starts on a safety injection signal. CCW pumps do not cavitate. Design CCW flow (1000 gpm) is available to the recirculation heat exchanger at the initiation of the recirculation mode (design basis case).

Case 2: LOCA occurs and TCV-601A/B fail open. Single failure of the standby CCW pump is assumed. The running CCW pump cavitates resulting in loss of CCW flow. At two hours the operator restarts a CCW pump, throttles CCW flow to prevent cavitation, and restores partial CCW flow (435 gpm) to the recirculation heat exchanger.

Case 3: LOCA occurs and TCV-601A/B fail open. Single failure of the standby CCW pump is assumed. The running CCW pump cavitates resulting in loss of CCW flow. At two hours the operator closes the block valves downstream

of the TCVs thus isolating CCW flow to the RHR heat exchangers and restarts a CCW pump which restores full design CCW flow to the recirculation heat exchanger.

In evaluating the above cases, it is necessary to establish some basic parameters and assumptions as follows:

A. LENGTH OF TIME TO RECOVER CCW ASSUMING SINGLE FAILURE OF A CCW PUMP:

Based upon the fact that a loss of CCW flow would be indicated and alarmed in the control room, that the Shift Technical Advisor (STA) is available in the control room within 10 minutes of the operating crew declaring an emergency, and that the Technical Support Center (TSC) would be manned to support the diagnosis, it was assumed that the problem causing loss of CCW flow would be diagnosed and full or partial flow re-established within 2 hours. This assumption was validated by the STAs. Dose rate calculated at the CCW pumps or RHR heat exchanger block valves using appropriately conservative assumptions was 4 R/hr with 1% failed fuel which supports these recovery operations (throttling the discharge valve, venting and then restarting the CCW pump, or closing RHR heat exchanger block valves and restarting the CCW pump).

B. REQUIRED POST-ACCIDENT LOADS FOLLOWING LOSS OF INSTRUMENT AIR:

The loss of instrument air will also isolate other CCW system loads (either CCW side or primary process side) including: letdown flow to the RHR heat exchangers, excess letdown flow to the excess letdown heat exchanger, RCP seal water flow to the seal water heat exchanger, and CCW flow to the RCP thermal barrier coils (see Attachment D). Due to the trip of the RCPs on SIS/SISLOP, the RCP motor heat load would also be removed from the CCW system. The remaining heat loads would be the spent fuel pit heat exchanger, the recirculation heat exchanger, the charging pump lube oil coolers, reactor shield cooling coils, and miscellaneous sample cooler and radwaste system heat loads. Of these, only the spent fuel pit heat exchanger, recirculation heat exchanger and charging pump lube oil cooler

would have a safety related function impacted by the interruption and restoration of reduced CCW flow post-accident. (The shield cooling coils are required only to prevent long-term damage to the reactor cavity concrete resulting from power operation.) These loads are addressed further below:

(1) Previous evaluations of the spent fuel pit have shown that cooling can be interrupted up to several hours without unacceptable heatup or loss of inventory above the spent fuel assemblies. Additionally, a thermal-hydraulic calculation has been performed which shows that over 40% of the initial CCW flow would be available following pump restart/throttling, which would have provided acceptable heat removal for the actual spent fuel pit heat loads which have been present.

(2) The charging pumps each have in addition to the CCW cooled lube oil cooler a fan cooled lube oil radiator. However, since the fans only start on a Safety Injection Signal (SIS) concurrent with a Loss of Offsite Power (SISLOP combination), credit cannot be taken for their automatic operation. A preliminary analysis has been conducted which determined that convection and radiation heat transfer would be sufficient to maintain lube oil temperature within the acceptable range for post-LOCA charging pump operation for 45 minutes. It is likely that the pump would continue to operate considerably longer if more realistic assumptions for bearing performance are made. Additionally, based on discussions with the STAs, it is reasonable to assume that operators would take action to install local jumpers which would start the fans within 30 minutes, therefore maintaining lube oil cooling to support charging pump operation. This action is supported by appropriately conservative dose projections for the applicable areas post-LOCA (i.e., less than 4 R/hr) with 1% failed fuel.

FOLLOW-UP ACTION NO. 6

The preliminary analysis will be completed before Mode 4 entry to confirm the acceptability of charging pump operation without CCW flow.

(3) The recirculation heat exchanger provides long-term containment heat removal following a LOCA, and for MSLB or FWLB in containment assuming a loss of RHR capability. A loss or reduction of recirculation heat removal would affect containment pressure and temperature, the containment sump temperature at the recirculation pumps, and the recirculated fluid temperature. The LOCA is bounding because recirculation conditions are reached the soonest, maximizing system heat loads, and the recirculated fluid is provided to the charging pumps for core cooling as well as to the refueling water pumps for containment spray. An evaluation of the containment pressure and temperature (P/T) effects will be addressed as part of the three cases to be evaluated.

The results of the evaluation/analysis of the three cases described above are discussed below.

CASE 1:

Assuming no single failure of a CCW pump, two CCW pumps provide close to design flow to the recirculation heat exchanger assuming both TCV-601A/B failed open. Adequate flow margin to runout has been demonstrated analytically and by test to prevent cavitation of the CCW pumps.

In this likely scenario, essentially normal heat removal capability exists from the recirculation heat exchanger and the containment response is that of the design basis case already analyzed. The detailed containment pressure and temperature response for the design basis LOCA is shown in Attachment H. The peak containment pressure which occurs during the blowdown phase was calculated to be 48.2 psig. This value was calculated using an updated version of the code originally used to calculate the FSAR peak containment pressure of 49.4 psig. A secondary containment pressure peak of 38.5 psig occurs during the recirculation mode.

CASE 2:

Single failure of a CCW pump is assumed resulting in cavitation of the other CCW pump with TCV-601A/B failed open. The operator restores partial CCW flow to the

recirculation heat exchanger at two hours by throttling CCW flow at the CCW pump discharge and restarting one CCW pump. The containment pressure and temperature response for this case was analyzed using the design basis methodology described in Attachment H and compared to the design basis case results. Only the recirculation mode pressure and temperature response is affected. The recirculation containment pressure peak increases from 38.5 psig to 46.7 psig but remains below the blowdown peak of 48.2 psig. The recirculation containment temperature peak increases from 262 degrees F to 273 degrees F. but remains below the blowdown peak of 289 degrees F. Containment pressure is reduced to below 50% of the peak value within a few days so that containment integrity is maintained and the previously calculated 2 hour and 30 day dose consequences remain bounding.

The pressure and temperature changes also affect the Net Positive Suction Head (NPSH) available to the various pumps operating during the recirculation phase. However, only a minor increase in sump temperature would occur, so that the only significant concern would be the effect on fluid downstream of the recirculation heat exchanger where cooling would be interrupted. Since saturated sump conditions were assumed, the principal effect of the increased temperature would be a decrease in the fluid density within the system. The density change from the assumed 200 degrees F to 260 degrees F heat exchanger outlet temperature (i.e., from 60.1 to 58.6 lbm/ft^3) would affect the static head and head losses for the piping from the heat exchanger to the charging and refueling water (containment spray) pumps. Evaluation of the applicable head loss and static head terms at the revised density values indicates that the available NPSH for the charging pump would be decreased by about 2 ft (vs. NPSH margin of 15 ft), and for the refueling water pumps by less than 1 ft (vs. NPSH margin of 13 ft). Thus, adequate NPSH exists for the recirculation, charging and refueling water pumps in the event of CCW interruption during post-accident recirculation.

The elevated pressure/temperature profile during recirculation also differs from that used to environmentally qualify (EQ) equipment inside containment. However, the duration of any significant difference is relatively short compared to the overall

accident duration assumed for EQ, and did not affect the qualification status of the EQ packages reviewed. This result is expected to be representative of the EQ impact for other equipment in the EQ program.

CASE 3:

A single failure of a CCW pump is assumed resulting in cavitation of the other CCW pump with TCV-601A/B failed open. The operator restores full design CCW flow to the recirculation heat exchanger at two hours by closing the block valves downstream of TCV-601A/B and restarting a CCW pump. This case was not specifically analyzed but is bounded by Case 2 results since full CCW flow is restored. Containment pressure and temperature response would be identical to Case 2 for the first 2 hours and then trend toward the base case profile.

SUMMARY

In the unlikely event all CCW flow were to be lost, adequate post accident cooling would be restored either by throttling and restart of the available CCW pump or closure of manual block valves and restart of the operable CCW pump. That one of these actions would be taken within two hours is highly likely since this would provide sufficient time for onsite and offsite emergency support facilities to be manned and operating.

Although these actions would undoubtedly have mitigated the consequences of the failure of TCV601 A and B, the accident sequence would have been considerably more complex (i.e., required operator actions within certain time constraints) than it otherwise need have been. A probabilistic study was performed to evaluate the risk of significant core damage from this issue (see Attachment B1). The study concludes that this issue represented a small contribution to the overall core melt frequency.[1] Consequently, the failure of TCV-601 A and B is considered to have low safety significance. However, due to the unnecessary complexity of this sequence, SCE recognizes the importance of correcting this configuration and identifying any other potential similar issues. Therefore, the SONGS 1 Single Failure Analysis conducted in 1976 will be reanalyzed within 9 months following restart from the Cycle 10 refueling outage.

[1] Estimated to be 3.1 E-4/year.

6. ELECTRICAL OVERLOAD DUE TO SWING BUS ALIGNMENT

ISSUE: Unacceptable diesel generator loading (beyond Operating License maximum) could occur on Train A if Swing 480V Bus 3 remains in its normal Train A alignment during emergency loading. Swing Bus 3 could remain in its normal alignment as a result of a single failure affecting Train B automatic controls.

REFERENCES: LER 1-88-019, dated January 12, 1989
NCR S01-P-6834, dated December 16, 1988

DISCOVERY: During a review of a proposed Technical Specification change relating to the swing bus, the engineer who had previously prepared the Single Failure Analysis (SFA) for the bus reviewed the system elementaries for the current configuration. It was found in this review that the configuration of the bus feeder breaker controls had been incorrectly evaluated in the safety evaluations for the previous modifications. Further review determined that the electrical system impact of this previously unrecognized single failure was not bounded by the existing electrical system analysis.

ROOT CAUSE: The primary root cause for this condition was a lack of familiarity within the appropriate engineering disciplines with respect to integrated system design and operation. In this particular instance, the responsible engineers failed to recognize an inconsistency between the single failure analysis (SFA) results and the electrical system configuration. The SFA results correctly identified the bus configuration which would result from the single failure, but the electrical system calculations did not address nor support this condition. A contributing factor to the failure to identify this inconsistency during the recent SFA effort was the time constraint and competing workload of the personnel involved in the SFA effort, which impacted their ability to cross check results with the respective discipline calculations. This issue is related to an inexperienced design staff. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this problem.

CORRECTIVE ACTION: Prior to restart from the current Cycle 10 refueling outage, a design change will be implemented that automatically sheds the swing bus from Train A for events requiring safety injection initiation. The SFA has been revised to accurately

reflect the consequences of all swing bus configurations. Within nine months of restart from the Cycle 10 outage the 1976 SFA will be reviewed in detail to ensure that all entries are correct and reflect the existing plant configuration.

As a result of the switchgear 3 single failure issue, an evaluation was initiated to identify other electrical bus arrangements in SONGS 1 which have a similar swing bus configuration. The only other automatic swing bus arrangement is the 120VAC Vital Buses 1, 2, 3, and 4. The Vital Buses power the four regulated buses and safety related instrumentation. The Vital Buses are each powered from the 125VDC Bus No. 1 through the inverters while the alternate supply is from 37.5 KVA and 7.5 KVA transformers fed from MCC #2 (a Train B source).

In the unlikely event of a failure of DC Bus No. 1 or the inverters, automatic transfer switches would transfer power for the Vital Buses to the alternate source from MCC #2. Although loading conditions in these circumstances are acceptable, previous electrical analyses for fuse/breaker coordination did not evaluate this scenario and instead credited the current limiting feature of each inverter for proper coordination.

Therefore, an additional electrical fuse/breaker coordination analysis was performed assuming the Vital Buses would be powered from the alternate supply. The results of this analysis showed that there is proper fuse/breaker coordination when powered from the alternate source and crediting the cable impedance of the loads to establish the maximum available fault current for fuse/breaker coordination.

SAFETY SIGNIFICANCE: The SONGS 1 diesel generators are rated at 6000kW by the manufacturers. However, in deference to NRC concerns regarding piston skirt design, the diesels were recently restricted by the Technical Specifications to a 5250kW (+ or - 5%) rating prior to the start of the Cycle 10 refueling outage. Following certain design modifications to the diesels (e.g., a slow start package for routine surveillance tests and installing approved piston skirts) the original diesel generator rating will be recognized by the Technical Specifications as 6000kW. Had the postulated single failure occurred, the diesels would have had a loading of approximately 5900kW. Although this load exceeds the existing technical specification load limit, it is within the rated capacity of the DG set.

It is SCE's judgment that operation of the diesel generators at 5900 kW for short periods is not expected to impact the ability of the diesel generators to perform their intended safety function. Thus, this issue is considered to have low safety significance.

Had this postulated single failure occurred in conjunction with a Main Steam Line Break (MSLB) outside containment causing Motor Control Center #3 (MCC 3) to malfunction, Train A bus voltage would have been degraded by spurious operation of MCC 3 loads during the safeguards loading sequence. MCC 3 is a swing bus load which is not environmentally qualified. Although it is expected that only the time response of the Train A emergency loads would have been affected, a specific bus voltage calculation to support this conclusion has not been performed. Thus, it has been conservatively assumed that the worst result of this voltage degradation would be that Train A loads would not have automatically started, although they would still be available for manual starting by operator action from the Control Room. The Emergency Operating Instructions (EOIs) specify the operator actions to be taken in the event the automatic systems fail to start, including shedding of the swing bus. Based on a best estimate analysis performed by Westinghouse for Cycle 9, operation of one charging pump ten minutes after a MSLB concurrent with a complete loss of safety injection will provide sufficient shutdown margin to prevent a return to power. Therefore, since this meets the acceptance criteria for this event, the bus loading degradation scenario is considered to be of low safety significance.

7. AFW TANK VOLUME REQUIREMENT

ISSUE: The existing calculation which determined the minimum amount of water to be retained in the Auxiliary Feedwater Storage Tank (AFWST) to support safety system operation did not take into account losses due to pump bearing cooling water flow.

REFERENCES: LER 1-88-017, dated January 5, 1989
NCR 1R-0074, dated December 9, 1988

DISCOVERY: During the Cycle 10 refueling outage, design modifications were implemented on the Auxiliary Feedwater System (AFWS) which require an additional water volume during post-accident conditions. The AFWST minimum volume calculation thus required change to reflect the additional water volume needed to support the design modifications. During this review it was determined that the previous calculation had failed to consider the water loss to pump bearing cooling.

ROOT CAUSE: The engineers responsible for performing and reviewing the calculation did not adequately review the plant's configuration, and thus did not recognize the need to account for water lost from the AFWST to supply pump bearing cooling water in the calculation. Contributing to this condition was the lack of a flow process drawing which would have readily identified all flow paths for water contained in the AFWST. In addition, the calculation process in effect at the time did not impose adequate inter-disciplinary reviews. Had other engineering disciplines reviewed the calculation the error may have been found and corrected. This issue is related to an inexperienced design staff. As indicated in our October 3, 1988 letter, SCE has already initiated corrective action to correct this problem.

CORRECTIVE ACTION: The calculation is being formally revised to reflect the actual AFWST volumetric requirements. The type of inter-disciplinary review required for calculations, has also been improved in SCE procedures and practices.

The cooling water flow to the bearing was measured and found to be 10.5 gpm. As a conservative measure the flow subsequently has been throttled-back to 5 gpm, the nominal value recommended by the pump vendor. The system flow calculation was reviewed to

determine if any other unaccounted flows exist. None were identified. A proposed Tech Technical Specification change has been submitted to the NRC associated with the third AFW pump and AFW system redesign which revises the minimum required volume of AFW from 150,000 gallons to 190,000 gallons. The proposed volume of AFW includes allowances for AFW pump bearing cooling for the motor-driven AFW pump (G10S) and for spillage of AFW during the feedline break event prior to operator action to isolate AFW to the faulted line.

SAFETY SIGNIFICANCE: In order to assess the safety significance, the original calculation was reevaluated with adjustments for actual plant conditions. Taking credit for reduced power operation (less than 92%) and the reduced RCS average temperature program and assuming the measured boaring cooling water flow (10.5 gpm), it was determined that the originally calculated volume of 150,000 gallons would have been adequate. In addition, the AFWST low level alarm was set at 165,000 gallons to alert the control room Operations personnel to take corrective action and rapidly restore the tank above 165,000 gallons. Therefore, there has always been an acceptable volume of water maintained in the AFWST and there was no safety significance as a result of this calculational error.

8. REFUELING WATER PUMP (RWP) G27S JUMPER

ISSUE: An unwarranted jumper was found in the control circuit of Refueling Water Pump (RWP) G-27S. In the unlikely event of a Loss of Off-site Power (LOP), the jumper would have prevented the automatic start of the South Refueling Water Pump (RWP) G27S upon receipt of a Containment Spray Actuation Signal (CSAS) if the CSAS were generated between 11.5 seconds after the LOP and 34 seconds after reenergization of the bus. In this sequence, the RWP can only be started manually from the control room.

REFERENCE: LER 1-88-016, dated December 30, 1988
NCR SO1-P-6774, dated December 19, 1988

DISCOVERY: The jumper wire was found on November 2, 1988 during a functional test of the pump control circuit following routine maintenance.

ROOT CAUSE: Investigation into the cause of the wiring discrepancy revealed that the subject wire should have been removed in 1976/1977 during RWP circuit modifications associated with the CSAS signal. The internal wiring diagram used by the electricians performing the wiring work in the field had incorrectly reflected the CSAS modifications to the RWP's control circuit, in that the diagram failed to show the removal of the subject wire. A visual verification of the circuitry compared with an elementary diagram which correctly showed the removal of the wire, also failed to identify the discrepancy at that time. In addition, the post-modification functional tests performed on the pump apparently did not completely test the circuit logic, since it should have also identified the discrepant condition.

Due to the number of years that have elapsed since the 1976/1977 CSAS modifications, it is not possible to definitively ascertain the root causes for the wiring discrepancy and inadequate post-modification testing. SCE believes, however, that the root causes for this occurrence are bounded by the findings of SCE's investigation of the adequacy of engineering and technical support for San Onofre which were identified in an October 3, 1988 submittal to the NRC.

CORRECTIVE ACTION: The jumper wire was removed from the breaker circuit and RWP G27S was satisfactorily tested for proper operability. The redundant RWP, G27N, was inspected and tested for similar wiring discrepancies and none were found.

SAFETY SIGNIFICANCE: The presence of the subject wire, which bypassed a contact in the undervoltage (UV) protection portion of the containment spray actuation circuitry, would have prevented the automatic start of RWP G27S in certain accident sequences. Because of the time delays built into the UV protective relay, the timing and duration of events is critical to the capability of the pump to start automatically. In all cases, if power to the pump were available the operator would have the capability to manually start the pump from the control room as directed by control room emergency operating procedures.

The UV protective relay circuit is designed to be bypassed when the RWP performs as a containment spray pump thus allowing the pump to automatically start given a CSAS. With the subject jumper wire in the circuitry, the UV relay would have continued to serve its normal protective function even in the containment spray mode.

The UV relay is designed to actuate and trip the pump if an undervoltage condition exists on the power bus. The relay actuates on a continuous voltage-time curve. For example; if the voltage degrades and remains at 89% rated voltage for 200 seconds, the relay will actuate or if the voltage should degrade and remain at 0% rated voltage, the relay will actuate after only 11.5 seconds. The relay resets after proper voltage has been restored for 27-34 seconds. With the jumper wire in place and the relay actuated, any auto-start signal (CSAS) received has no effect. In the case where the UV relay does not reset until after a CSAS has been generated, the operator must manually start the pump or reset and reinitiate CSAS to start the RWP.

For example, if a CSAS was generated during the course of an accident without a Loss of Offsite Power (LOP), the pump would auto-start and the existence of the jumper would not hamper the pump operation. If the CSAS was generated during an accident involving a LOP and at least 34 seconds after the power was restored, the pump would auto-start and the existence of the jumper would not hamper the pump operation. If the CSAS was generated after the bus lost power for more than 11.5 seconds (relay actuated) and before

the Diesel Generator had restored power to the bus continuously for more than 34 seconds, then the pump would not auto-start. Under these conditions, the pump would have to be manually started by the Operators in the control room as directed by the Emergency Operating Instructions.

Because the redundant RWP did not have a similar jumper wire left in its circuitry, it would have been expected to auto-start upon receipt of a CSAS.

A Probabilistic Risk Assessment was performed for the "as-found" condition based on the following sequence (refer to Attachment I):

> In the event of a Loss of Offsite Power (LOP), an undervoltage condition would have been seen by the UV relay. If a SIS (due to a Small or Large LOCA) had been generated 10.5 seconds or more following the LOP, the running Diesel Generators would have loaded on to their buses one second later (11.5 seconds). Since an undervoltage condition would have existed for 11.5 seconds, the UV relay would have actuated. A CSAS permissive is generated by the SIS/LOP sequencer 21 seconds following the SIS (31.5 seconds following the initial LOP). Since continuous voltage would not have been restored for the 34 seconds (45.5 seconds following the initial LOP) required to reset the UV relay, the CSAS signal to auto-start RWP G-27S would not be acknowledged and the pump would have to be started manually.
>
> If the redundant RWP had failed to start due to random causes, RWP G-27S would have been started from the control room. Station procedure SO1-1.0-10, "Reactor Trip or Safety Injection," clearly instructs the operator to ensure that both refueling water pumps are running.[2]

The PRA analysis shows that the probability that containment spray would be required coupled with the probability that the operator would fail to manually start RWP G-27S coupled with the probability that the redundant RWP would not have been available due to maintenance or various failure modes is low.[3] In light of the low likelihood that the redundant RWP would not have been available to automatically respond, the risk contribution of this design deficiency is concluded to be low.

---

[2] The step in Station Procedure SO1-1.0-10 which requires the operator to ensure that both refueling water pumps are running is the last of the twelve steps that all SONGS 1 operators are required to know and memorize.

[3] Estimated to be 1.7E-9/year.

Events which would have resulted in a Safety Injection Signal (SIS) concurrent with or prior to a LOP (SISLOP), would not have prevented the automatic starting of RWP G-27S.

9. CONTAINMENT SPRAY FLOW DIVERSION

ISSUE: Spurious actuation of the Control Room handswitch for the sphere fire loop spray valve CV-92 during a Loss of Coolant Accident (LOCA), Main Steam Line Break (MSLB) or Feedwater Line Break (FWLB), could cause CV-92 to open, diverting flow from the containment spray header (in the top of the sphere) to the sphere fire loop (inside the secondary shield). This problem was not addressed by either the 1976 ECCS single failure analysis (SFA) nor a system hydraulic calculation (MC734-012) which was issued in 1986 to support recirculation pump replacement in the Cycle 9 refueling outage.

REFERENCES: NCR S01-P-7067, dated March 15, 1989
LER 1-89-008, due April 3, 1989

DISCOVERY: As part of the evaluation of CCW valves TCV-601A and TCV-601B (refer to issue 5) it was recognized that the CCW system TCV failure scenario could apply to other SONGS 1 safety systems with a train-common header arrangement. It was further recognized that the only other such systems which had not been recently reviewed as part of the engineered safety features single failure analyses were the Salt Water Cooling System (SWCS), and the containment spray portion of the Containment Recirculation and Spray (CRS) system. The SWCS configuration is sufficiently simple that such a failure scenario could not occur. The CRS is far more complicated than the SWCS, with several more operating modes and flow paths. Personnel familiar with the system recognized that there were two similar potential valve failures in the containment spray portion of the CRS which had not been addressed in the revised hydraulic calculations: Spray limiter valves CV-517/CV-518, and sphere fire loop spray valve CV-92. Non-Conformance Reports (NCRs) were then written against each of these potential failures to document these calculation assessment deficiencies.

ROOT CAUSE: An investigation to determine the root cause has not been completed at this time. However, as the affected valve was omitted from the 1976 ECCS SFA, similar to CCW valves TCV-601A and TCV-601B, a common underlying cause is anticipated. Due to the length of time which has passed since the completion of the 1976 SFA, it is questionable if an accurate determination of the exact root cause of these oversights can be established. The failure of the 1986 calculation to identify this potential single failure

reflects the narrow focus of issues being reviewed in the calculation. This issue is related to excessive reliance on contractor work. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this problem.

CORRECTIVE ACTION: To prevent a spurious actuation from causing CV-92 to open, power to its pilot solenoid valve (SV-116) will be isolated by redundant devices (eg. a second control switch wired in series with the existing switch) prior to restart from the current Cycle 10 outage. Based on the evaluation which identified this issue, it is considered unlikely that other single failure susceptibilities of this type remain in the plant. However, a formal reanalysis of the SONGS 1 ECCS for single failures utilizing experienced SCE resources will be completed within 9 months of plant restart from the Cycle 10 refueling outage.

SAFETY SIGNIFICANCE: A preliminary assessment of the failure impact of either CV-517 or CV-518, based on existing cases in the CRS system hydraulic calculation, estimated that the consequences would be acceptable due to the safety margin that exists with respect to both flow and NPSH limits. A hydraulic calculation for the sphere fire loop portion of the system could not be located. Consequently, a revision of the CRS system hydraulic calculation was initiated to assess the impact of the postulated CV-92 failure. The preliminary results of this assessment are that:

1. The flow rate to the containment spray header, with two operating refueling water pumps, would be about the same as the assumed single pump flow rate (1080 gpm) during the injection mode. NPSH for all pumps would remain acceptable with considerable margin.

2. The total flow rate to the containment spray header and sphere fire loop nozzles would be about 660 gpm during the recirculation mode. However, because the fire loop nozzles spray onto equipment rather than falling through a substantial elevation and fraction of containment volume, this portion of the total flow would be ineffective for containment pressure/temperature control. The remaining flow of approximately 300 gpm to the containment spray header is less than that assumed in the safety transient analyses (500 gpm) and insufficient to atomize the flow from the spray nozzles, resulting in a significant degradation of the containment heat removal

capability. In an analysis (conservatively assuming no spray flow) the containment pressure would diverge from the expected response at approximately 21 minutes post accident and would exceed design basis peak pressure (49.4 psig) at approximately 103 minutes.

Thus, the injection mode containment pressure/temperature transient would have remained bounded by existing analyses, but the recirculation mode heat removal rate from the containment vapor phase would have been significantly reduced.

CV-92 is normally shut and does not receive an automatic actuation signal. Thus, it would only be open due to a passive failure or spurious operation. The position of CV-92 is indicated in the Control Room and operator action could have been expected to close the valve (by removing control power) prior to exceeding design pressure at 103 minutes. However, the CV-92 pilot solenoid valve is not environmentally qualified and may not open or shut while exposed to a LOCA environment.

A probabilistic study was performed to evaluate the risk of significant core damage attributable to this design issue (see Attachment A). This analysis identified the sequence of concern to be 1) a loss of coolant accident large enough to require recirculation from the containment sump, 2) the failure of valve CV-92 to remain closed, and 3) the failure of the control room staff to recognize and reclose CV-92 in time.

The PRA analysis shows that the annual probability of this sequence represents a low contribution to the overall plant risk.[4]

[4] Estimated to be 4.4 E-8/year.

10. CORE MONITORING TECHNICAL SPECIFICATIONS

ISSUE: Technical Specifications 3.10 (In-Core Instrumentation) and 3.11 (Continuous Power Distribution Monitoring) are applicable only at reactor power levels above 90% of 1347 Mwt. It has been concluded that application of these Technical Specification requirements only at power levels above 90% power could result in SONGS 1 operation in an unanalyzed condition.

REFERENCE: NCR SO1-P-7078 dated February 22, 1989.
Westinghouse Letter 89SC*-G-0010, dated February 20, 1989.
Informational LER 1-89-010 (not yet issued)

DISCOVERY: As part of preparing the Cycle 10 Reload Safety Evaluation, a concern was raised about the basis of certain 90% power limitations associated with Technical Specifications 3.10 and 3.11. Because of the additional steam generator tubes that were plugged during the Cycle 10 refueling outage, the axial offset equations in Technical Specification 3.11 were changed. The review of this change indicated that the applicability of Technical Specifications 3.10 and 3.11 for only Mode 1 above 90% power could no longer be supported.

ROOT CAUSE: Technical Specifications 3.10 and 3.11 were approved by the AEC in November 1973. The original basis for these technical specifications was concern about the power peaking factors associated with fuel densification. Because of these fuel densification concerns, the AEC required that Edison institute continuous power distribution monitoring. A 10% reduction in power was judged by the AEC to be sufficient to accommodate the uncertainties associated with fuel densification and therefore the technical specifications were only applicable for operations above the 90% power level. Since that time no significant changes to limits or requirements related to continuous power distribution monitoring were made and no detail reviews were made of the range of the associated technical specification applicability. As part of the Cycle 10 Reload Safety Evaluation reanalysis to reflect an equivalent 20% steam generator tube plugging in any steam generator while on the reduced Tavg program, changes were made to axial offset monitoring equations that appear in Technical Specification 3.11. In the process of changing this technical specification, a detailed review indicated that while limiting the applicability of Technical Specifications 3.10 and 3.11 to power levels above 90% provided

protection for fuel densification, there was the possibility of SONGS 1 potentially operating in an unanalyzed condition (i.e., core power distribution could have exceeded safety analysis limits). In order to protect against such operation, these Technical Specifications are being revised as described below under Corrective Action. This issue is related to excessive reliance on contractor work. As discussed in our October 3, 1988 letter, SCE has already initiated action to correct this problem.

CORRECTIVE ACTION: As part of the Cycle 10 Reload Safety Evaluation, Technical Specification 3.10 is being revised as follows:

1. The applicability is changed from "Mode 1 above 90% Rated Thermal Power" to "Mode 1".

2. Action B has been changed from being less than 90% rated thermal power in 1 hour to "be in Mode 2 within 6 hours".

3. The basis has been changed from being less than 90% rated thermal power in 1 hour to "be in Mode 2 within 6 hours".

As part of the Cycle 10 Reload Safety Evaluation, Technical Specification 3.11 is being revised as follows:

1. The applicability is changed from "Mode 1 above 90% Rated Thermal Power" to "Mode 1".

2. The reference to "less than 90% rated thermal power" has been deleted from Action A.

3. Action C has been changed from being "less than 90% rated thermal power in 1 hour" to "be in Mode 2 within 6 hours".

SAFETY SIGNIFICANCE: In the past it has been SCE's practice to perform the calibration required by Technical Specification 3.10 and the axial offset measurements required by Technical Specification 3.11 at all power levels. It has never been necessary to reduce SONGS 1 reactor power below 90% because of exceeding the axial offset limits.

However, on one occasion during Cycle 8 the power was reduced to less than 90% for a short time due to an inability to perform the incore-excore calibration required in Technical Specification 3.10 in a timely manner. The plant operated stably during this

period. When the incore-excore instrumentation was subsequently calibrated and the axial offset measurements performed, there was no indication that adverse changes had occurred in core power distribution. Thus the plant has never achieved a core power distribution that was not considered in the safety analyses and, therefore, this issue represents no safety significance.

11. RCP SHEARED SHAFT AND LOCKED ROTOR REACTOR TRIP

ISSUE: Reanalysis of the Reactor Coolant Pump (RCP) sheared shaft event for the Cycle 10 Reload Safety Evaluation indicated that the variable low pressure trip (assuming single failure of the RCP low flow trip) would not provide a reactor trip over the entire operating range (i.e. reduced T-avg program, reduced power level, negative Moderator Temperature Coefficient [MTC]). Review of the RCP motor overcurrent trip for the RCP locked rotor event (assuming single failure of the RCP low flow trip) indicated that the trip setpoint was non-conservative and would not have provided protection for the event.

REFERENCE: LER 1-89-007 due March 29, 1989
NCR-SO1-P-7089 dated February 27, 1989

DISCOVERY: The RCP locked rotor and RCP sheared shaft events were not part of the original SONGS 1 plant design basis. These events were first analyzed in 1983 in response to SEP Topic XV-7 and the results showed the acceptance criteria were met with reactor trip initiated by the RCP low flow trip. Subsequently in 1987, a Single Failure Analysis (SFA) of the Reactor Protection System (RPS) was performed. The SFA identified a single failure susceptibility with the RCP low flow trip for these events. For these single loop events, a single failure of the low flow trip in the affected loop would have prevented a reactor trip (1 channel per loop, 1 out of 3 loops trip).

As a result, the RCP motor overcurrent trip was credited for the locked rotor event, and the sheared shaft event was reanalyzed with the Variable Low Pressure (VLP) trip. The analysis results at the time showed that the consequences were acceptable.

During reanalysis of the sheared shaft event to reflect revised conditions for the Cycle 10 Reload Safety Evaluation, Westinghouse discovered that with the plant operating on the reduced T-avg program, a reactor trip would not occur during a sheared shaft event. Previously, the sheared shaft event had only been analyzed for nominal T-avg plant operation which was incorrectly assumed to be bounding. The sheared shaft event was subsequently reanalyzed with a more restrictive VLP setpoint with acceptable consequences and plans were made to implement the more restrictive setpoint.

During review of the Cycle 10 Reload Safety Evaluation, SCE questioned whether the more restrictive VLP trip would be effective over the entire operating range (e.g. reduced power level, negative MTC, rod control in auto). Westinghouse performed confirmatory analysis which indicated that a single VLP trip setpoint would not provide protection over the entire operating space. An RCP motor undercurrent trip was proposed to provide protection for the sheared shaft event. During engineering of the RCP motor undercurrent trip, it was discovered that the RCP overcurrent trip setpoint was non-conservative. A 4-hour phone report was made to the NRC.

ROOT CAUSE: Following the RPS SFA, in March 1987, Westinghouse reanalyzed shaft breaks with VLP for nominal T-avg initial conditions only. Westinghouse assumed that the nominal T-avg initial condition was the worst case and would bound the reduced T-avg initial condition, which is the case for other non-LOCA transients. Westinghouse failed to recognize that for an event relying on the VLP trip, the reduced T-avg initial conditions could become limiting since initially the plant is farther from the trip setpoint. In July 1988, Westinghouse identified the problem with reduced T-avg condition and reanalyzed the shaft break for the reduced T-avg condition.

SCE committed to implementing the new VLP setpoint equation during the Cycle 10 refueling outage. During review of the reduced T-avg sheared shaft analysis and VLP setpoint, SCE questioned whether the VLP trip would provide protection at reduced power level. Westinghouse subsequently confirmed that VLP would not provide reactor trip over the entire operating range. Westinghouse failed to recognize other plant initial states (other than reduced T-avg) which could lead to more limiting results.

During design engineering of a proposed RCP motor undercurrent trip to provide sheared shaft protection, it was discovered that the overcurrent trip was non-conservative and would not have provided protection for the locked rotor event.

Westinghouse failed to provide a conservative sheared shaft analysis is related to the uniqueness of SONGS 1 design, in this case the Reactor Protection System and the lack of Westinghouse personnel sufficiently familiar with the unique design of SONGS 1 are the

root causes of these errors. The previous failure to recognize this error resulted from over-reliance on vendor analysis by SCE and insufficient overall plant knowledge of personnel reviewing the Westinghouse analysis.

The existence of a non-conservative overcurrent setpoint credited for the locked rotor event is related to a lack of readily available documentation of the details of the RCP overcurrent trip (design basis documentation) when credit was taken for the overcurrent trip in lieu of the low flow trip, the incorrect assumed familiarity of Westinghouse with the SONGS 1 RPS design and inadequate interdisciplinary review by SCE engineers of the updated SFA crediting the overcurrent trip. Since no change to the plant was required (only credit for an existing trip), it was assumed without critical review that the pump circuit breaker trip, actuated by motor overcurrent, would occur in sufficient time to accommodate the locked rotor event. This would have resulted in equivalent response time to the low flow trip.

CORRECTIVE ACTION: Because an automatic reactor trip on variable low pressure may not occur for the locked rotor/sheared shaft events for reduced power operation or more negative MTC, credit is not taken for this trip. The existing reactor protection system provides a reactor trip on RCP breaker opening due to overcurrent to the RCP motor. For the locked rotor event, the breaker has been modified to ensure RCP breaker opening will occur. Analysis indicates that acceptable consequences result if reactor trip occurs within 6 seconds (initiation of rod motion). An additional overcurrent trip relay will be installed prior to return to service to provide a reactor trip within the required time. For the sheared shaft event, an undercurrent trip will be implemented so that a RCP breaker trip will also occur in a no load current condition to the RCP motor.

SAFETY SIGNIFICANCE: The low flow reactor trip is the primary means of protection for this event. There are other trips available that may provide redundant protection for these events, but they were not credited due to the conservative assumptions in the analysis. The existing variable low pressure trip provides protection for the locked rotor/sheared shaft events with the plant on the nominal T-avg program at 100% power. With plant operation on the reduced T-avg program, no automatic reactor trip would have occurred at 100% power. However, event analysis shows that no DNB would have occurred for power levels less than 94%. This power level bounds that at which the plant has been operating (except for a short period in 1984 for a warranty run) since the installation of SG

sleeves in 1981. For both the locked rotor and sheared shaft events, multiple indications and alarms are available to the operator which would precipitate a manual reactor trip. Therefore, the overall safety significance is low.

12. DIESEL GENERATOR LOAD SEQUENCING LOGIC

ISSUE: Upon a Safety Injection Signal (SIS) with a LOP present (i.e., SISLOP), the diesel generator load sequencing logic is designed to close the DG output breaker to independent, safety-related buses associated with each of the two DG's (DG-1 and DG-2). However, when the load sequencers initiate on a SISLOP, although the LOP signal latches, it is reset by the opposite train DG bus. This prevents the unconnected DG from automatically closing its breaker and sequencing its loads (i.e., the output breaker closes). Consequently, if one DG starts and energizes its emergency bus in a shorter period of time than the alternate DG, the LOP signal will clear and the output breaker for the lagging DG will not close. Based upon the data associated with the actuation time of the bus undervoltage relays, it is necessary for the output breaker of the lagging DG to close within approximately 0.8 seconds of the leading DG. If this does not occur during a postulated SISLOP scenario, the automatic response capability of one of the two trains of safety-related components may be lost. This is contrary to the design requirements.

REFERENCES: NCR S01-P-7093, dated March 2, 1989
LER 1-89-004, due April 3, 1989

DISCOVERY: This deficiency was discovered as a result of performing a special SISLOP test on DG-2 on February 2, 1989, during the refueling outage. The test consisted of utilizing test pushbutton switches to simulate a SIS and simultaneous LOP. The SIS and LOP switches were simultaneously depressed, resulting in the expected SISLOP response. The switches were released after evidence of the proper SISLOP response (i.e., after a few seconds). However, after the DG accelerated to operating speed, the output breaker did not close as expected. During the subsequent investigation, it was discovered that release of the LOP switch removed the LOP signal (i.e., the switch did not "seal in"), thus preventing the closure of the output breaker. Additional review of the sequencer logic diagrams revealed that failure of the LOP signal to "seal in" was not restricted to use of the test switches. The sequencer circuit is designed such that the LOP clears if either of the two emergency buses is energized.

ROOT CAUSE: The root cause of the deficiency in the sequencer circuit is currently being investigated. Preliminary indications are that the cause is related to weaknesses within post

modification testing programs. SCE believes that this cause is bounded by the findings of SCE's investigation of the adequacy of engineering and technical support for San Onofre which were identified in our October 3, 1988 submittal to the NRC.

CORRECTIVE ACTION: Install time delay relays prior to return to service in the circuits of the 4160V undervoltage inputs to the sequencer for monitoring LOP conditions. The time delay relay will be continuously energized during normal voltage conditions. The relay will drop out instantaneously upon receipt of an undervoltage signal and will pick up 12 seconds after restoration of bus voltage. The 12 second time delay will ensure that both DG breakers close before reset of the opposite train undervoltage signal to each sequencer occurs.

SAFETY SIGNIFICANCE: For a SISLOP event, at least one train of safeguards is required to place the plant in a safe shutdown condition. The deficiency described in this report could have resulted in one of the two trains of safeguards being unavailable for automatic actuation. This deficiency is safety significant only in the event that a safety related component associated with the leading DG fails. In the event of a single failure of the Safety Injection train which receives power from the loaded diesel, neither train of safety injection would have been automatically actuated as assumed in the transient analyses. Since the lagging DG would have received a start signal and would therefore be running, upon recognition of the deficiency, manual operator action could be taken to close its output breaker, thereby re-energizing the bus and respective components.

During a LOCA and a concurrent Loss of Offsite Power, the SLSS generates a SISLOP sequencer signal. The SISLOP signal initially sends start signals to both DG 1 and 2. Both DG's should start, run, and load to their respective 4KV buses simultaneously. However, during testing, it was discovered that loading of the DGs is not simultaneous and that the loading of one DG will remove the undervoltage condition on the sequencer input and will prevent the loading of the other DG.

A probabilistic study was performed to evaluate the risk of core damage attributable to this design issue (see Attachment J). This analysis identified the sequence of concern to be 1) a loss of coolant accident, 2) a conditional loss of offsite power resulting from the unit trip, 3) the successful starting and loading of diesel generator A, 4) the failure of safety

injection train A, 5) the successful starting of diesel generator B but its failure to load on to its bus, and 6) the failure of the control room operators to load diesel generator B on to its bus in time. The PRA analysis shows that the annual probability of this sequence represents a low contribution to the overall plant risk.[5]

[5] Estimated to be 2.9 E-7/year.

IV. ADEQUACY OF CORRECTIVE ACTIONS CURRENTLY UNDERWAY

In this section the problems evaluated in Section III are assessed as a group to determine if corrective actions presently underway as a result of recommendations made by SCE's Task Force which performed an Independent Assessment of the Engineering and Technical Support to SONGS remain appropriate. Specific Task Force recommendations generally encompass the issues evaluated in this report. However, evaluation of these twelve issues has provided insight to supplement some of the existing corrective actions and to reestablish priorities for others.

Although the Task Force had many specific recommendations several are pertinent to the issues noted in this report. These are as follows:

- Add senior knowledgeable design staff.
- Perform all upper tier design in-house.
- Reduce reliance on outside contractors.
- Evaluate and refine the Configuration Management Program.
- Develop a Design Bases Documentation Program.
- Develop an improved Licensing commitment management process.

As a result of the twelve issues evaluated in this report, we have identified the following five common causes:

- Excessive reliance on contractors
- Inexperienced design staff
- Changing documentation standards
- Commitment Management weaknesses
- Post-modification testing weaknesses

As discussed below, the first four of these five common causes are directly related to and are being addressed by the corrective actions already underway as a result of recommendations made by SCE's Task Force.

EXCESSIVE RELIANCE ON CONTRACTOR WORK

Four issues all resulted from a contractor scope of work which was insufficiently challenged by SCE and ultimately was determined to be significantly flawed. Issues (5), CCW Isolation Valves Single Failure, and (9), CV-92 Failure Mode, were both related to the 1976 NUS single failure analysis. This analysis was not sufficiently challenged by SCE reviewers to ensure an adequate product was received before it was utilized as a design basis for the plant. In addition, issues (10), Core Monitoring Technical Specifications, and (11), RCP Sheared Shaft and Locked Rotor Reactor Trip, were a consequence of accepting representations from Westinghouse without ensuring the accuracy of the assumptions and analysis methodology utilized. In these four issues we see the intersection of two of the already recognized weaknesses. First, over reliance on contractors, and second lack of knowledgeable senior design staff capable of insightfully challenging contractors work.

In assessing the acceptability of our improvement programs two specific items must be addressed, namely our efforts to correct past weaknesses and our ability to detect embedded flaws in previously completed tasks.

The corrective actions to improve future work are underway as indicated in our October 3, 1988 letter and we anticipate continued improvement as the new organization matures. Reliance on contractors is being reduced, and more experienced personnel are being infused into the design process both through internal transfers and by outside hiring. These more experienced personnel will also have the effect of improving contractor work because of the added ability to review and challenge contractor work.

FOLLOW-UP ACTION NO. 7

A program to better monitor Westinghouse and CE analytical work will be developed and implemented within 9 months after restart from the Cycle 10 refueling outage.

The efforts to detect embedded existing flaws is being addressed by the DBD program. As a result of this report, the scope of the planned DBD for accident analyses will be reviewed to ensure all technical specifications related to reactor core neutronics and thermal hydraulic parameters are incorporated.

FOLLOW-UP ACTION NO. 8

A DBD section will be structured to validate the accident analyses and technical specification requirements related to reactor core neutronics and thermal hydraulics. This section will be developed as one of the high priority sections. (This work will be initiated approximately 6 months after restart from the Cycle 10 refueling outage.)

INEXPERIENCED DESIGN STAFF

Several issues are the direct result of an insufficiently knowledgeable design staff. Specifically issues discussed in items (1) 480VAC Breaker Overload, (6) 480VAC Loading Configurations following single failure inconsistent with DG loading calculation, and (7) Auxiliary Feedwater Storage Tank Volume Calculation, all resulted from errors in the assumptions made in the Design Basis for the analysis. These errors were less a result of the difficulty in determining the design basis then they were a result of the poor level of overall plant knowledge which was available to the design staff. Present efforts to improve the experience and knowledge level of the staff is considered sufficient. In addition problems of this nature should be effectively identified by the DBD program.

FOLLOW-UP ACTION NO. 9

Given the number of electrical issues noted in this report, the DBD program schedule will be revised to increase the priority of SONGS 1 electrical systems.

SYSTEM	CURRENT SCHEDULE	REVISED SCHEDULE
125 VDC	1991	1991
480 VAC	1992	1990
120 VAC	1995	1992
4160 VAC	1995	1990

CHANGING DOCUMENTATION STANDARDS

Issue #3, Plant maintenance records did not document that charging pump G8B was rewound, and issue (4), RHR piping not constructed of the same schedule as shown in the SCE line list; are seemingly a consequence of the documentation standards which were common in the industry in the later 1960's and early 1970's. Because these standards were significantly less rigorous then those in place today one must be particularly careful when performing work on SONGS 1 to carefully consider the accuracy of design information prior to completing an analysis.

FOLLOW-UP ACTION NO. 10

Both the design engineers and those participating in the DBD program will be trained in the various methods of validating SONGS 1 design information.

COMMITMENT MANAGEMENT WEAKNESSES

Issue (2), Steam Generator Wide Range Level Instrumentation Not Upgraded to Comply With TMI Commitments, resulted from omission of a key reference on the Licensing Commitment Lists (LCL's) during the transition of files. In addition, the LCL item did not include appropriate cross-references. The LCL was designed to track overall commitments. Each LCL item included a list of references which provided the basis for the LCL and additional information regarding specific commitments. Thus, the references included on LCL's provided the only mechanism to track the SGWR level transmitter qualification commitment. There is presently an effort underway to upgrade our licensing commitment management system. As part of the upgrade of the licensing commitment management system, procedure revisions will be implemented to require entry of all appropriate references and cross-references to other associated LCL's. Progress in the area is not sufficiently complete yet to gauge the effectiveness of the new program. Notwithstanding implementation of a more comprehensive tracking program, existing flaws caused by errors of omission of references would not be corrected by this program. Identification of these types of errors are within the scope of the DBD program.

FOLLOW-UP ACTION NO. 11

Both the DBD program and the new commitment management program will be a focus of oversight organization reviews to ensure their future effectiveness.

POST MODIFICATION TESTING WEAKNESSES

Issue (8), Jumper Cable Left In Control Circuit After Modification and (12) Diesel Generator Load Sequencing Logic, represent a failure of the post modification testing program to adequately identify and resolve complex time-dependent problems. In recent times post modification testing programs have significantly improved however, past problems have been noted with this function. For example, problems with backup Nitrogen systems at SONGS 1 were associated with weaknesses in our post-modification testing system.

FOLLOW-UP ACTION NO. 12

A root cause analysis of recently identified prior post modification testing deficiencies which have been recently identified will be performed and corrective action initiated as appropriate.

V. OVERALL SAFETY SIGNIFICANCE

The twelve issues discussed in this report, individually and collectively, do not represent a significant hazard to the continued safe operation of SONGS 1. This assessment is based on evaluations which have shown that each issue has a low safety significance based on one or more of the following:

(1) A demonstration that the system or component would have completed its safety function without modifications,
(2) Likely operator action that would have been taken to mitigate postulated accidents,
(3) Modifications completed before returning the unit to service ensure completion of required safety functions,
(4) The availability of alternate or diverse equipment to perform the required safety functions, or
(5) The results of PRAs indicate an insignificant contribution to the overall plant risk.

The majority of the twelve issues included in this report surfaced as a direct result of the recent reorganization of SCE's design and engineering organizations which focused SCE's design-related activities and stressed the performance of work in a more thorough and comprehensive manner. In order to determine the overall perspective of the total scope of issues, individual safety significance evaluations were performed for each issue. The evaluation results can be grouped and summarized. Issues 1, 2, 3, 4, 6 and 7 are considered to be of low safety significance and adequate in the "as found" condition (accept as is). Issues 8, 9, 10, 11 and 12 are considered to be of low safety significance due to the extremely low probability of occurrence. Only the issue regarding CCW flow to the RHR Heat Exchanger Temperature Control Valve Single Failure (Issue 5) is considered to be more significant than the other issues. However, it is also of low safety significance. The safety significance is low because of the relatively long time (more than 2 hours) available to respond to the problem, the operator action that would likely be taken to mitigate the consequence of the event, and the low probability of the accident sequence.

In addition, the identified issues were, in general, due to subtle aspects related to the unique design of SONGS 1. The root causes of the issues indicate that a greater attention to detail is required when completing engineering tasks on SONGS 1 but no fundamental problem exists with the design of the plant or with the manner in which SCE operates or maintains SONGS 1.

Due to the continued emphasis SCE will place on engineering evaluations of the SONGS 1 design, technical issues will, in all likelihood, arise in the future. SCE considers that these issues will also have low safety significance because of the in-depth evaluations that have already been completed on SONGS 1. Detailed analyses were completed in 1987 and again in 1989 using the 1976 Single Failure Analysis as a starting point. These analyses identified single failure susceptibilities of increasing complexity but with decreasing probability. Identification of these single failures can be attributed to increased understanding of how single failure analyses must be completed on SONGS 1 as well as increased experience of SCE design personnel. As previously mentioned, these past issues have been shown to have low safety significance and there is no reason to believe that future issues, which may involve yet more subtle aspects of the SONGS 1 design, should not have even lower safety significance.

Accordingly, SCE considers that there is reasonable assurance that operation of SONGS 1 should continue without undue risk to the health and safety of the public.

VI. CONCLUSIONS

The twelve issues identified and assessed in this report have been resolved or are being resolved through root cause corrective actions at the present time. The safety significance evaluation for each of the twelve issues revealed that the issue was of low safety significance or that alternate measures were available to mitigate the consequence of the deficiency during an accident scenario and that these scenarios have a low probability of occurrence.

Our letter of October 3, 1988 previously informed you that SCE's Task Force which performed an Independent Assessment of Engineering and Technical Support for San Onofre Nuclear Generating Station concluded that programmatic deficiencies in engineering technical support were primarily caused by (1) the complexity of the then existing organization, (2) heavy reliance on engineering contractors combined with inadequate allocation of SCE engineering resources, and (3) the lack of readily accessible design basis documentation. Consistent with the findings and corresponding recommendations to correct these deficiencies, SCE (1) reorganized the focus design related engineering activities, (2) is reducing reliance on contractors, (3) is increasing staffing and (4) is undertaking a design basis documentation program. As part of the reorganization and focusing of design-related engineering activities, SCE has emphasized that work be performed in a questioning and inquisitive manner. SCE firmly believes that the twelve issues discussed in this report are the result of proper implementation of the Task Force recommendations.

SCE has reviewed the Task Force conclusions in light of the design deficiencies detailed in Section III of this report to assess the adequacy of actions being taken to correct the underlying root causes. Appropriate corrective action was identified for the root causes of each deficiency. These actions were then compared with the Task Force recommendations.

It has been determined that the conclusions and recommendations of the Task Force remain valid. For example, the root causes for some of these events relate to the lack of readily accessible design basis documentation, a lack of integrated system knowledge on the part of the design engineer, and/or excessive reliance on engineering contractors, all of which were detailed in the Task Force evaluation of engineering deficiencies. However, this comparison has pointed out some subtle aspects that need to be addressed

regarding the Task Force and some recommendations, priorities and schedules will be revised. Section VII of this report tabulates "Follow-up" actions identified during the evaluation of the twelve issues and many of these actions involve minor redirection or changes in schedule of Task Force recommendations.

The twelve issues evaluated in this report did not present a significant safety hazard. As the new design organization matures, it is very likely that we will continue to find other similar issues. We will continue to foster a more questioning attitude in the performance of work. In addition, the design bases program, revalidation of the 1976 NUS Single Failure Analysis, and ongoing design change activities will facilitate identification of similar issues. However, because of the unique design of SONGS 1, the defense in depth approach to plant design and operation, the existence of diverse and redundant equipment, detailed procedures, and a high level of operator training, SCE considers that future issues will also have a low safety significance and will not impact safe plant operation.

The issues addressed in this report have all had adequate corrective action implemented. Programs to aggressively pursue identification and resolution of any additional problems in the plant are in place and being expanded. Based on the expected limited safety significance of these twelve issues and our belief that future issues will have a similar low safety significance, it is our judgment that return-to-service of SONGS 1 is acceptable and does not represent an undue risk to the health and safety of the public.

VII. FOLLOW-UP ACTIONS

This is a summary list of the following actions identified elsewhere in this report.

(1) LCL entries will be reviewed for possible omissions similar to the SGWR level transmitter commitment. The scope of this review will be 10% of the entries between 1979 and 1982 and will be completed within six months after restart from Cycle 10 refueling outage. [See pg 16]

(2) A cross check of TMI Action Plan references and the Systematic Evaluation Program (SEP) Integrated Safety Assessment will be added to the DBD preparation checklist. This change provides two separate DBD reference document search paths for those requirements related to these programs. [See pg 16]

(3) A review of all ISI data sheets completed during this second 10-year interval (1978 to present) is in progress. The purpose of this review is to compare wall thickness measurements for large bore Class 1 and 2 pipe included in the ISI program with SCE design documents for any additional piping schedule discrepancies. This review will be completed by May 31, 1989. The review of piping inside containment will be completed before SONGS 1 restart. [See pg 22]

(4) A reanalysis of the 1976 ECCS and supporting systems Single Failure Analysis will be completed within nine months of plant restart. [See pg 24]

(5) The design basis document review will be conducted for the CCW systems at all three Units on a best effort basis utilizing qualified SCE resources. As a result, the CCW systems for Units 2 and 3 will be performed in 1989 and SONGS 1 in 1990. [See pg 24]

(6) The preliminary analysis will be completed before Mode 4 entry to confirm the acceptability of charging pump operation without CCW flow. [See pg 27]

(7) A program to better monitor Westinghouse and CE analytical work will be developed and implemented within 9 months after restart from the Cycle 10 refueling outage. [See pg 53]

(8) A DBD section will be structured to validate the accident analyses and technical specification requirements related to reactor core neutronics and thermal hydraulics. This section will be developed as one of the high priority sections. (This work will be initiated approximately 6 months after restart from the Cycle 10 refueling outage.) [See pg 54]

(9) Given the number of electrical issues noted in this report, the DBD program schedule will be revised to increase the priority of SONGS 1 electrical systems. [See pg 54]

(10) Both the design Engineers and those participating in the DBD program will be trained in the various methods of validating SONGS 1 design information. [See pg 55]

(11) Both the DBD program and the new commitment management program will be a focus of oversight organization reviews to ensure their future effectiveness. [See pg 56]

(12) A root cause analysis of recently identified prior post modification testing deficiencies which have been recently identified will be performed and corrective action initiated as appropriate. [See pg 56]

VIII. ATTACHMENTS

A. Probabilistic Risk Assessment of Failure of Containment Sphere Fire Loop Spray Valve CV-92

B1. Probabilistic Risk Assessment of Failure of CCW Isolation Values to the RHR Heat Exchanger

B2. Overall Assessment of Events Impacted by TCV-601 A/B Failure

C. Safety Injection System Diagram

D. SONGS 1 CCW System Diagram

E. Auxiliary Feedwater System Diagram

F. SONGS 2/3 CCW System Diagram

G. 480V Bus Overload Test Results

H. Containment Pressure Response to TCV-601 A/B Failure

I. PRA of Failure of RWP G27S

J. PRA of Diesel Generator Loading Failure on SIS/LOP

ATTACHMENT A PRA of Failure of Containment Sphere Fire Loop Spray Valve CV-92

THE IMPACT OF POST-LOCA FAILURE OF CONTAINMENT SPHERE FIRE LOOP SPRAY VALVE CV-92 ON CORE MELT FREQUENCY FOR UNIT 1

1.0 PURPOSE

The purpose of this analysis is to assess the impact on core melt frequency of the failure of the Containment Sphere Fire Loop Spray Valve CV-92 due to a LOCA.

2.0 BACKGROUND

Containment Sphere Fire Loop Spray Valve CV-92 is a fail closed valve which is designed to close and isolate the containment sphere fire loop spray header from the containment spray header. Failure of the valve to remain closed would require an electrical short in valve control power. A failure of the control room hand switch for valve CV-92 (due to an electrical short or operator mis-operation) may cause the valve to open during a Loss of Coolant Accident (LOCA) and divert containment spray flow to the containment sphere fire loop header resulting in degraded containment spray heat removal capability. (Main Steam Line Breaks were judged to be non-contributors to the probability of core melt). Operator recovery of full containment spray capacity requires the operator to recognize the event and open the appropriate breaker (closing valve CV-92).

3.0 ANALYSIS

The failure of CV-92 contributes to the probability of core melt only through the following failure sequence:

1) A LOCA of sufficient size as to eventually require recirculation from the containment sump.

2) Failure of valve CV-92 to remain closed.

3) Failure of the operating staff to identify and correct the CV-92 failure.

Assumptions:

- Loss of containment heat removal leads to core melt.
- LOCA requiring recirculation occurs at t = 0.

- Failure of CV-92 to remain closed prior to recirculation (during recirculation, flow limiting valves CV-517 and CV-518 are closed) does not affect containment spray capacity.

- Failure of CV-92 to remain closed during recirculation impairs the containment spray capacity and leads to core melt (regardless of any operating containment spray pumps).

- Failure of CV-92 prior to LOCA ($t < 0$) is not modeled since failure to remain closed would be indicated by decreasing RWST level indication.

- The earliest that the operator would be able to diagnose and respond to a failure of CV-92 is when containment pressure increases above 40 psig during recirculation ($t = 40$ minutes). This is based on preliminary containment analysis results (see Attachment H on Containment Pressure Response). The operator is assumed to have an additional 60 minutes ($t = 100$ minutes) to close CV-92. The probability of the operator failing to close CV-92 in time is assumed to be 0.1.[6] The time period during which CV-92 could open and require a prompt (less than 60 minutes) operator response is assumed to be 2 days.

- During the later stages of recirculation (after 2 days), decay heat production is reduced. The time required for the operator to respond and correct a failure of CV-92 during this period is much longer than the 60 minutes stated in the previous assumption. For simplicity, the probability of the operator failing to close CV-92 in time given a valve failure between 3 and 30 days post-LOCA is judged to be 0.01.[7]

---

[6] The operator failure probabilities assumed in this analysis are conservative with respect to NUREG/CR-1278, Table 20-1.

[7] NUREG/CR-1278, Table 20-1.

Calculation :

[Core Melt Freq] = [Freq. of LOCA requiring recirc.[8]] *
{ [Pr of Failure of CV-92 during 2 days[9]] *
[Oper. fails to close CV-92 within 60 min] +
[Pr of Failure of CV-92 during 28 days] *
[Oper. Fails to close CV-92 in time (t>60m)]}
= [3.8E-3/yr] *
{ [(1.0E-6/hr)(2 days)(24 hr/day)] * [0.1] +
[(1.0E-6/hr)(28 days)(24 hr/day)] * [0.01] }

= **4.4E-8/yr**

4.0 CONCLUSION

The estimated frequency of core melt for this sequence is 4.4E-8/yr which represents a small percentage of the overall core melt frequency for Unit 1.

---

[8] Frequency of LOCAs with diameter > .75" is 3.8E-3/yr (based on WASH-1400, Reactor Safety Study, U.S.N.R.C., October 1975).

[9] IEEE-500, Section 8.22, "Switches - all modes of failure = 1.0E-6/hr"

ATTACHMENT B-1 PRA of Failure of CCW Isolation Valves to RHR Heat Exchanger

AN ASSESSMENT OF THE CORE MELT IMPACTS OF FAILURES OF THE COMPONENT COOLING WATER RHR HEAT EXCHANGER ISOLATION VALVES AT SONGS-1

1.0 PURPOSE

The purpose of this analysis is to estimate the amount of increased risk to which the plant was exposed prior to the time that this failure mode was recognized as significant.

2.0 BACKGROUND

CCW failure could occur during a Loss of Coolant Accident (LOCA) as a result of the unexpected opening of the CCW isolation valves (TCV-601A and TCV-601B) to the RHR heat exchangers. It has been shown through analysis that in spite of CCW diversion to the RHR heat exchangers, enough CCW would pass through the Recirculation Heat Exchanger to cool the core and maintain containment pressure within previous analyses. However, it is believed that these diversion paths would have exposed the operating CCW pump to failure from runout and/or gas binding. Engineering evaluation also determined that CCW pump failure would not occur when these valves open if either:

- At least two CCW pumps are running (both the A and B pumps receive a start signal on a SIS signal); or
- One CCW pump is running and the operator can throttle the pump discharge using local manual valves.

2.0 ANALYSIS

A simplified fault tree model of the risk of core melt during the post-LOCA recirculation phase was constructed. Two basic cases were analyzed. Case 1 represents the current plant with the identified CCW failure mode. Case 2 represents the plant design and response if the failure mode had never existed. The risk of the failure mode can be determined by examining the difference between the results of the two cases. It should be noted that because this is a comparative risk assessment, simplified models were able to be constructed for those plant features that remain identical between the two cases.

Comparative analysis using risk models is well recognized as the best application for such models. While the uncertainty in the exact value of core damage frequency may be large, it is possible to construct a comparison in such a way that the mean, median, upper, and lower bounds can be compared with similar results. This is true of the results quoted below.

Appendix A presents the fault tree used to evaluate the post-LOCA core melt risk. The fault tree model consists of the CCW model (with its support systems: Saltwater Cooling, AC and DC Power, and SIS and LOP signals) obtained directly from the SONGS-1 PRA and a new "Core Melt due to post-LOCA Recirculation Failure" developed specifically for this analysis.

The post-LOCA recirculation failure fault tree contains simplified models of the recirculation system and charging system. These simplified models consider only the dominant failure modes of the components. Items not included in the tree include failures of Class-1E electric power systems and actuation signals, recovery actions, and unavailabilities due to maintenance and testing. The specific assumptions concerning the development of this model include the following:

- o A LOCA occurs of sufficient size to require recirculation from the containment sump.
- o Failure of recirculation injection requires failure of both the charging pumps or both the refueling water pumps.
- o Recirculation injection must occur successfully through at least two of the three RCS injection lines.
- o It is assumed that charging pump G-8B is the normally running pump and pump G-8A is locked out. For conservatism, it is assumed that the running pump lacks an operable air cooler. Therefore pump G-8B is dependent upon CCW to provide pump cooling.
- o Charging pump G-8A will probably run for two hours without CCW cooling. It is likely that operator training and procedures would have led operating staff to locally start fan cooler E-908 within this time.
- o Both CCW valves to the RHR heat exchanger fail open.
- o The running CCW pump continues to run for a short time while the standby CCW pump receives a "SIS" start signal.
- o The third CCW pump would not auto-start but would have to be manually started.
- o Neither core melt nor excessive containment pressure would occur within two hours of the LOCA with or without CCW pumps (due to heat capacity of the water in the sump).
- o Without operator action to throttle its discharge valve, a single CCW pump would fail due to runout or gas binding.
- o Without operator action, two operating CCW pumps would not fail due to runout or gas binding.
- o The radiation dose rate at the CCW pump discharge valves would be sufficiently low to permit local operator action.
- o Failure of CCW would lead to core melt.

The CCW fault tree was modified to split the tree into two segments, one reflecting all the non-CCW pump failures (see pages 1 and 2 of the CCW fault tree), and the other

resenting failures of the three CCW pumps (sheets 3 through 5 of the CCW fault tree). e top gate of the pump failure fault tree requires failures of all three CCW pumps to result in complete CCW failure. To represent those cases in which failure of two of the three pumps results in CCW failure, a new top gate was created which features a 2-of-3 logic.

For the cases in which CCW failure due to failure of TCV-601A/B is assumed to have never existed, gate Y-05-02 is set to FALSE to eliminate all CCW failures resulting from loss of only 2 CCW pumps.

Based on the Case 2 model (no failure of TCV-601A and TCV-601B), the probability of core melt due to LOCAs requiring recirculation is estimated to be 3.0976E-4 per year.

Based on the Case 1 model (failure of TCV-601A and TCV-601B), the probability of core melt due to LOCAs requiring recirculation is estimated to be 3.1006E-4 per year. This value has uncertainty associated with it. The large number of significant figures is provided as the cutsets which are affected by the values in question are small contributors which would otherwise be omitted for comparison.

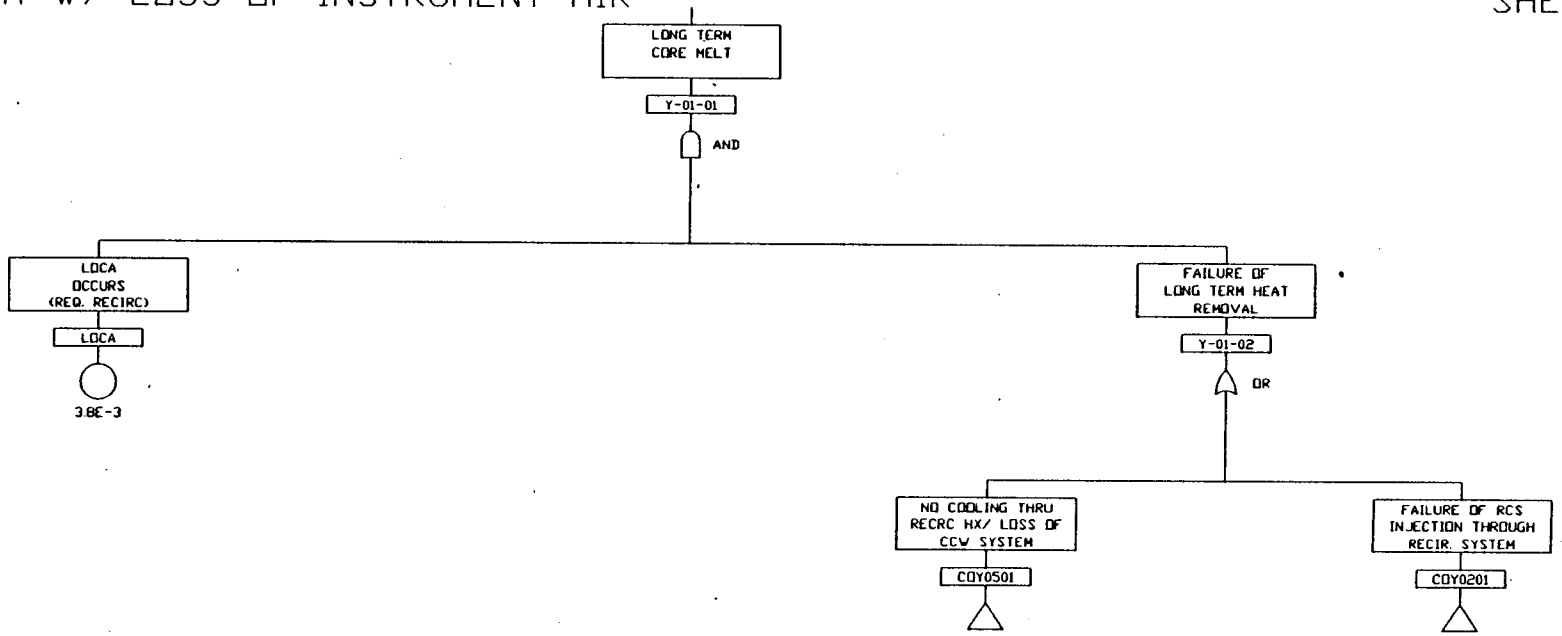
Variations were performed on Case 1 (failure of TCV-6O1A and TCV-601B) to assess the sensitivity of core melt frequency to operator responsiveness in recovering a failed CCW pump (by venting the casing and throttling the discharge valve) and starting fan cooler E908.

4.0 CONCLUSION

The best estimate of the probability of core melt during the time this design deficiency existed is 3.1006E-4 per year. Thus, this design deficiency represents a best estimate increase in the probability of core melt of 3.0E-7 per year (or 0.1%). While this value has uncertainty associated with it, it is clear that the deficiency is a relatively small contribution.

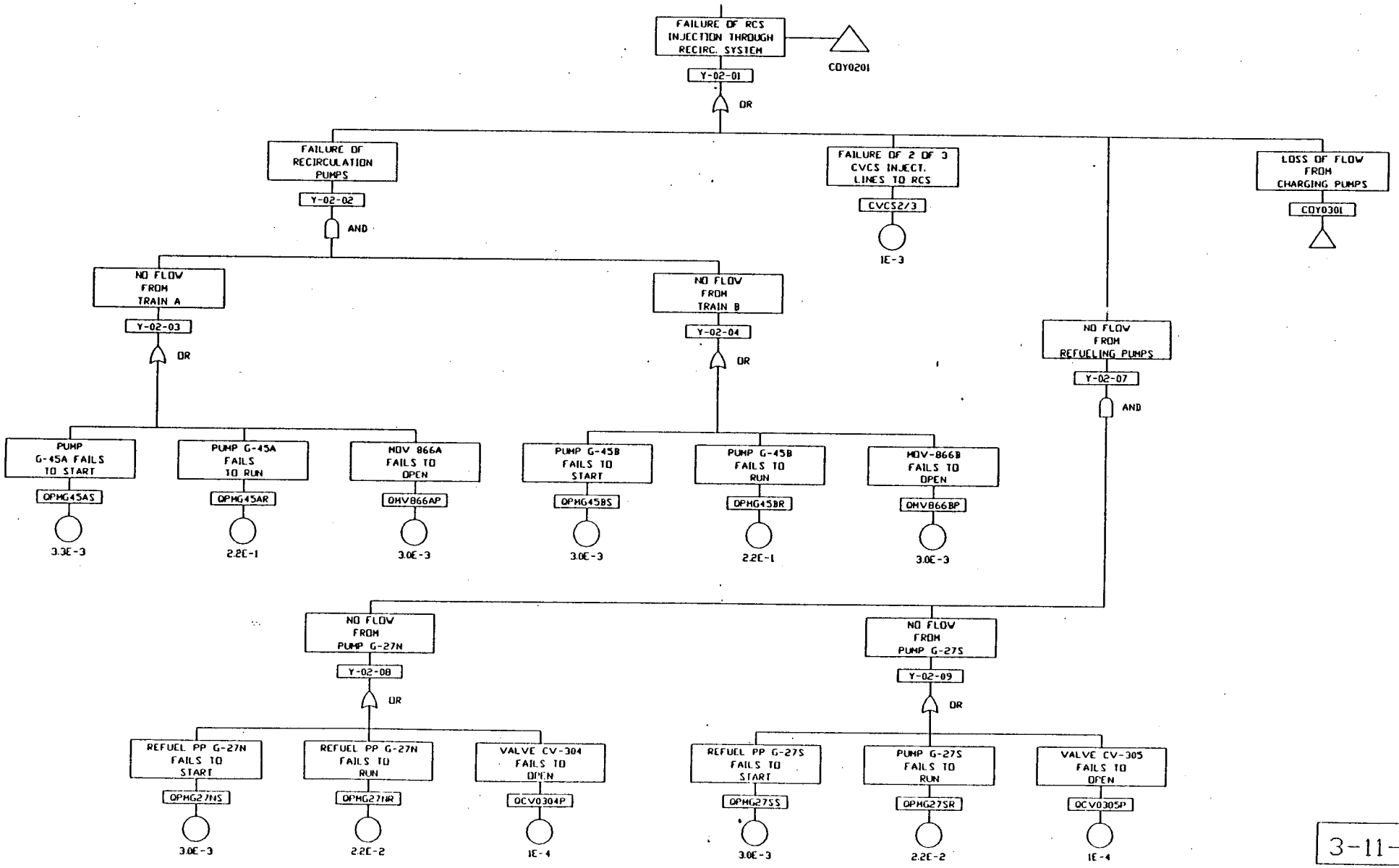
SONGS 1: LOCA W/ LOSS OF INSTRUMENT AIR

SHEET 1



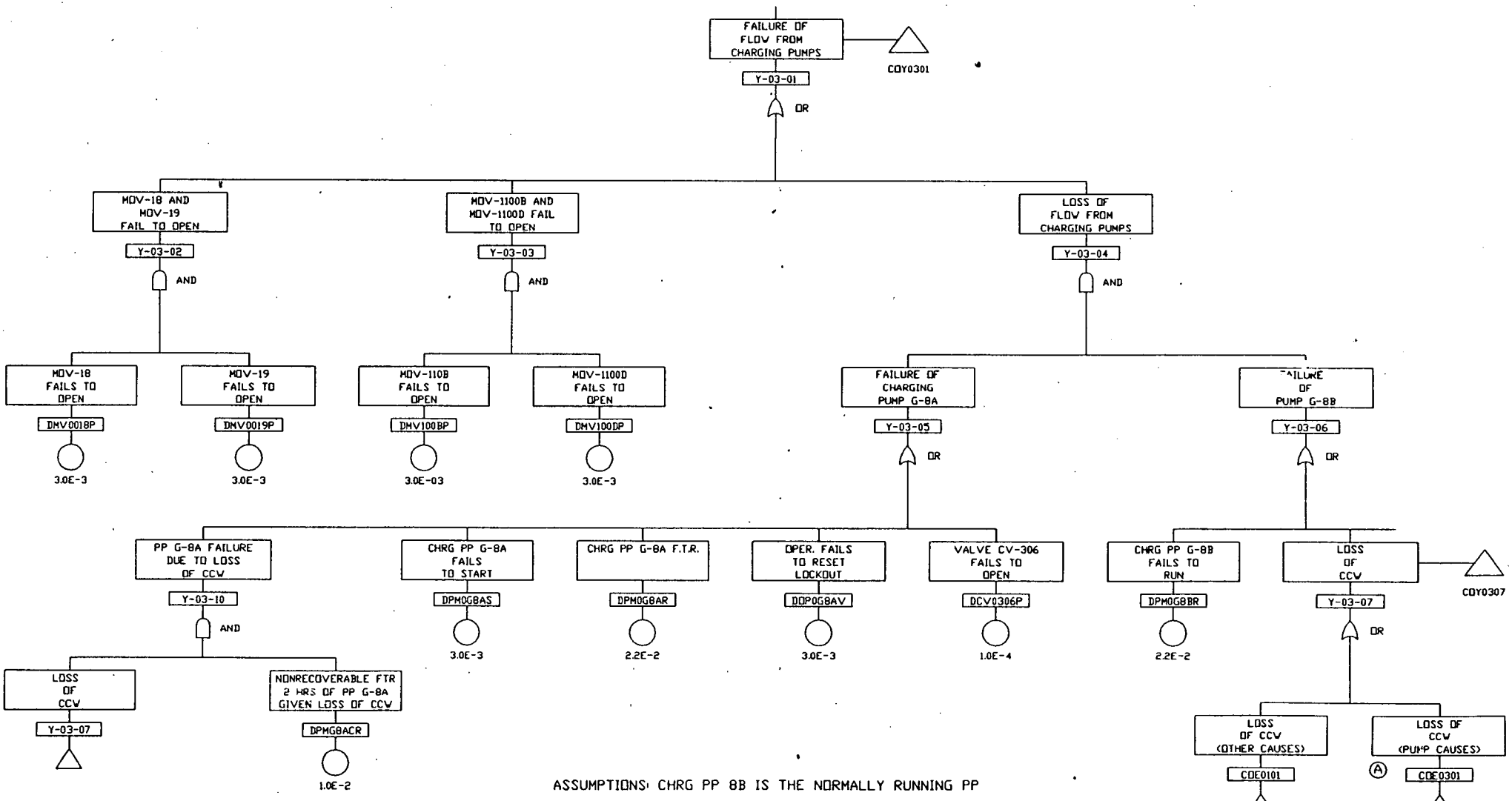
3/10/89

SONGS 1: LOCA W/ LOSS OF INSTRUMENT AIR



3-11-89

SONGS 1: LOCA W/ LOSS OF INSTRUMENT AIR



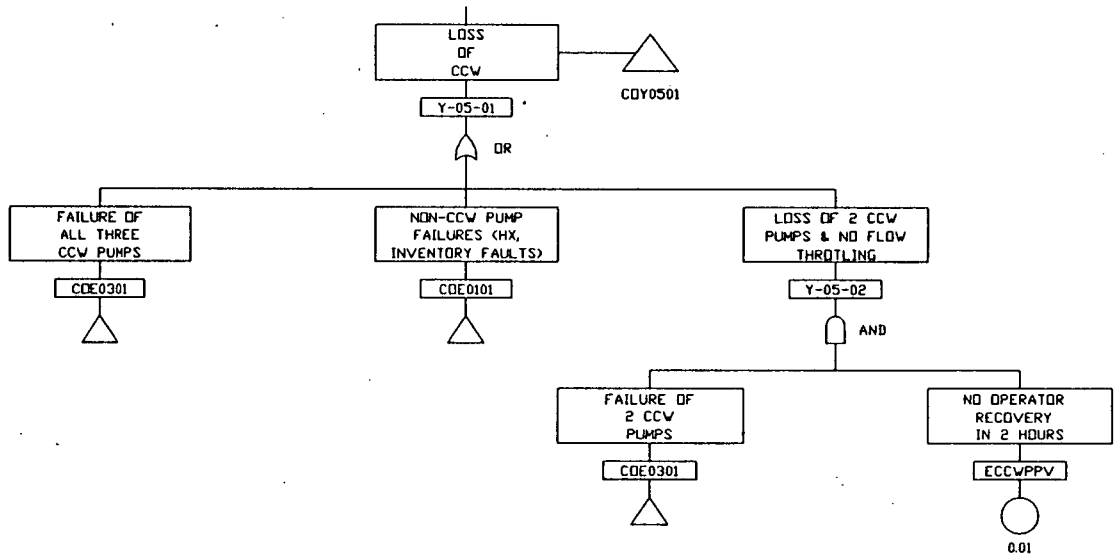
ASSUMPTIONS: CHRG PP 8B IS THE NORMALLY RUNNING PP

PP G-8A IS LOCKED OUT

PP G-8B LACKS OPERABLE FAN COOLER

Ⓐ FOR CASE 1 CHANGE CONNECTOR TO COE0301A

3/16/89



A) OPERATIONAL RECOVERY INCLUDES:

1) RECOGNITION OF LOSS OF CCW PUMPS

2) VENTING AIR BOUND CCW PUMPS

3) THROTTLING OF CCW PUMP DISCHARGE VALVE OR CLOSING CCW/RHR ISO VALVES

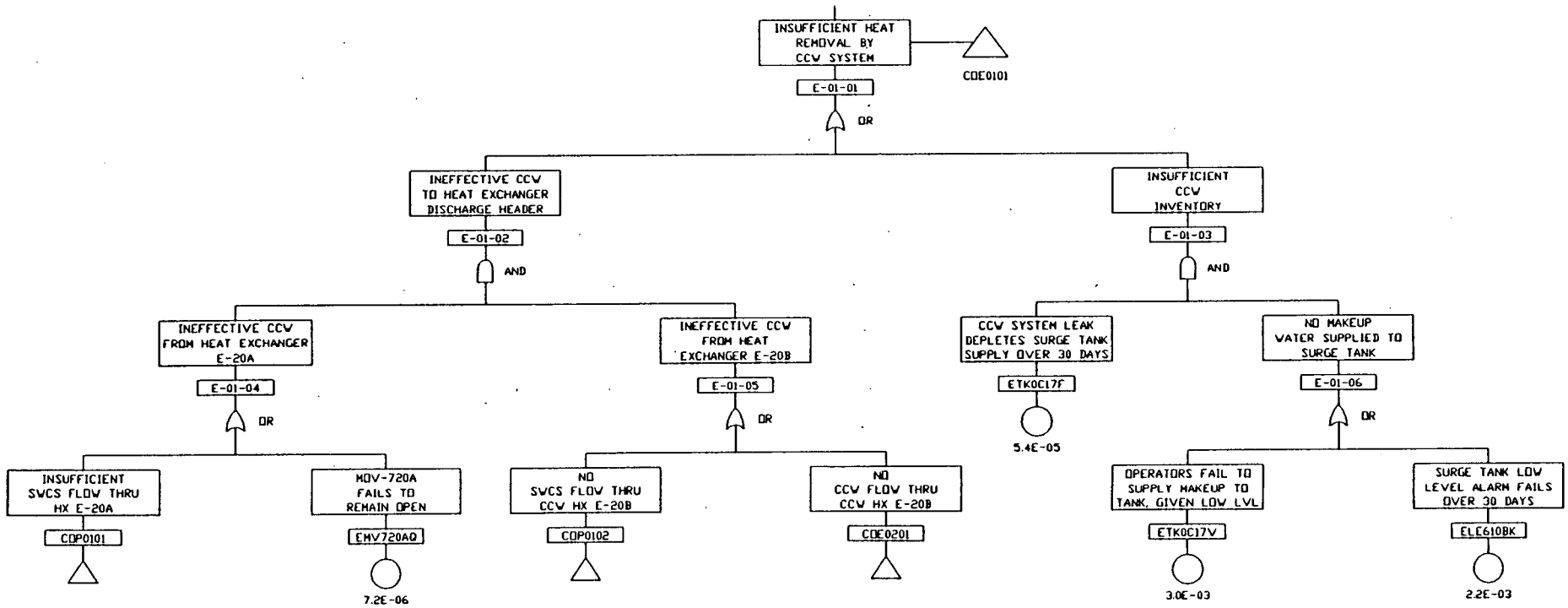
4) RESTARTING CCW PUMPS

3/10/89

FIGURE E: COMPONENT COOLING WATER FAULT TREE

UNIT 1

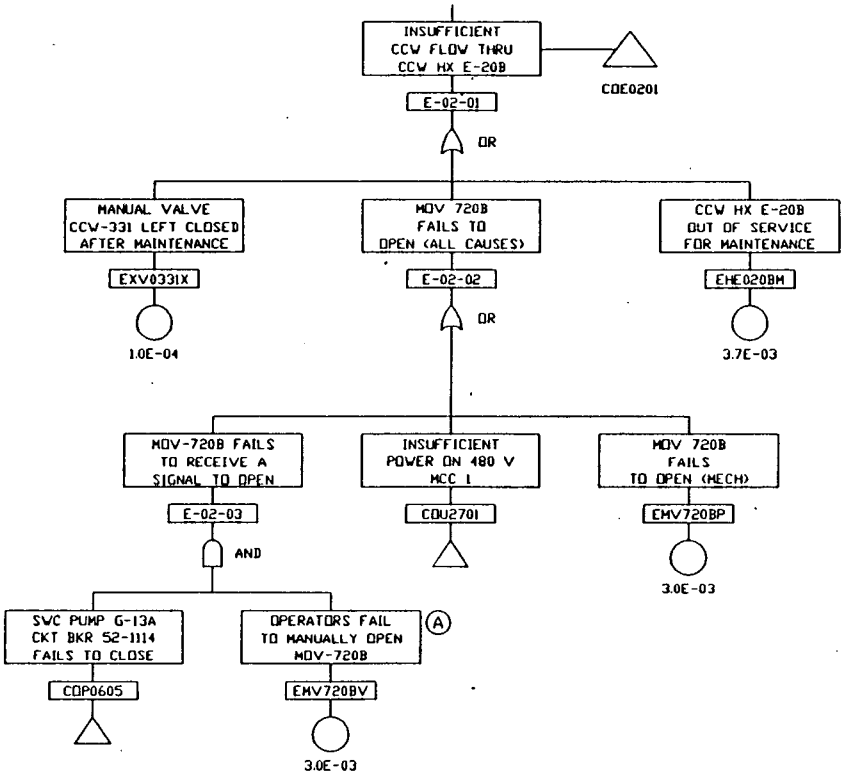
(ASSUME CCW PUMP G-15A AND HEAT EXCHANGER E-20A ARE NORMALLY IN SERVICE)



3/10/89

FIGURE E, SHEET 2

UNIT 1

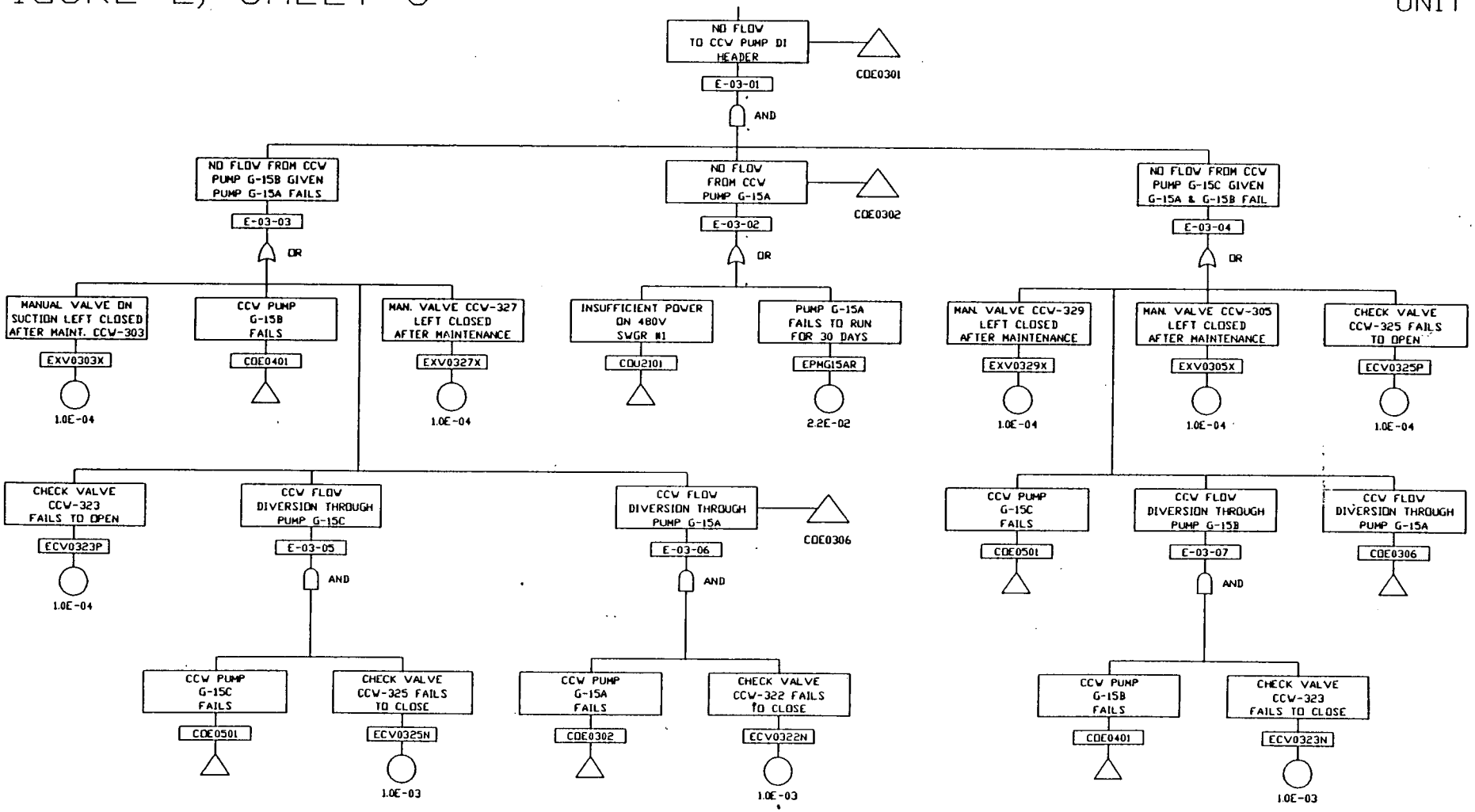


(A) OI SO1-2.4-1, "LOSS OF SALTWATER COOLING SYSTEM," STEP 4.1
OI SO1-2.1-10, "LOSS OF COMPONENT COOLING WATER SYSTEM"

3/10/89

FIGURE E, SHEET 3

UNIT 1

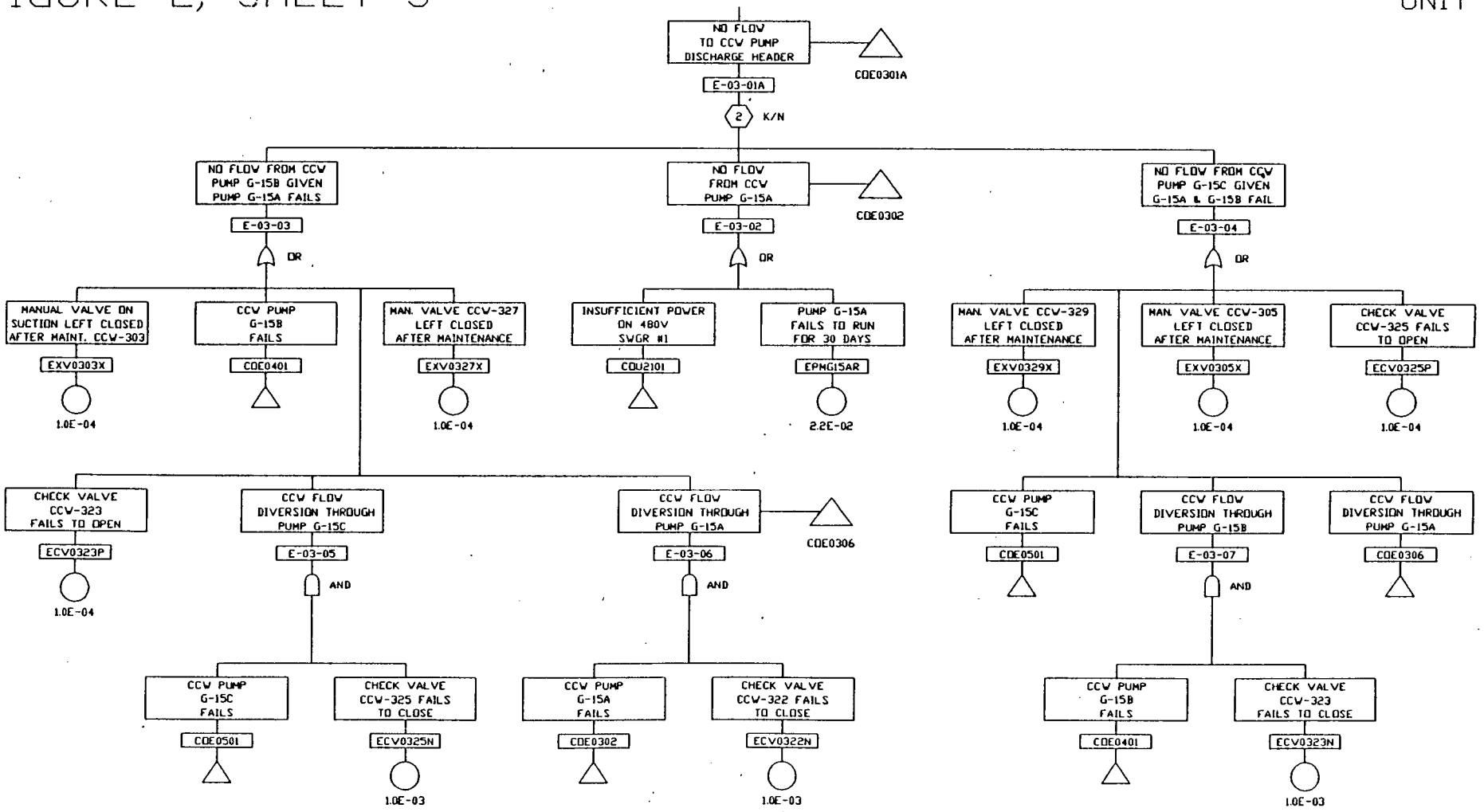


3/10/89

SPECIAL STUDY: CCW 2 OF 3 PUMPS NEEDED FOR OPERATION

FIGURE E, SHEET 3

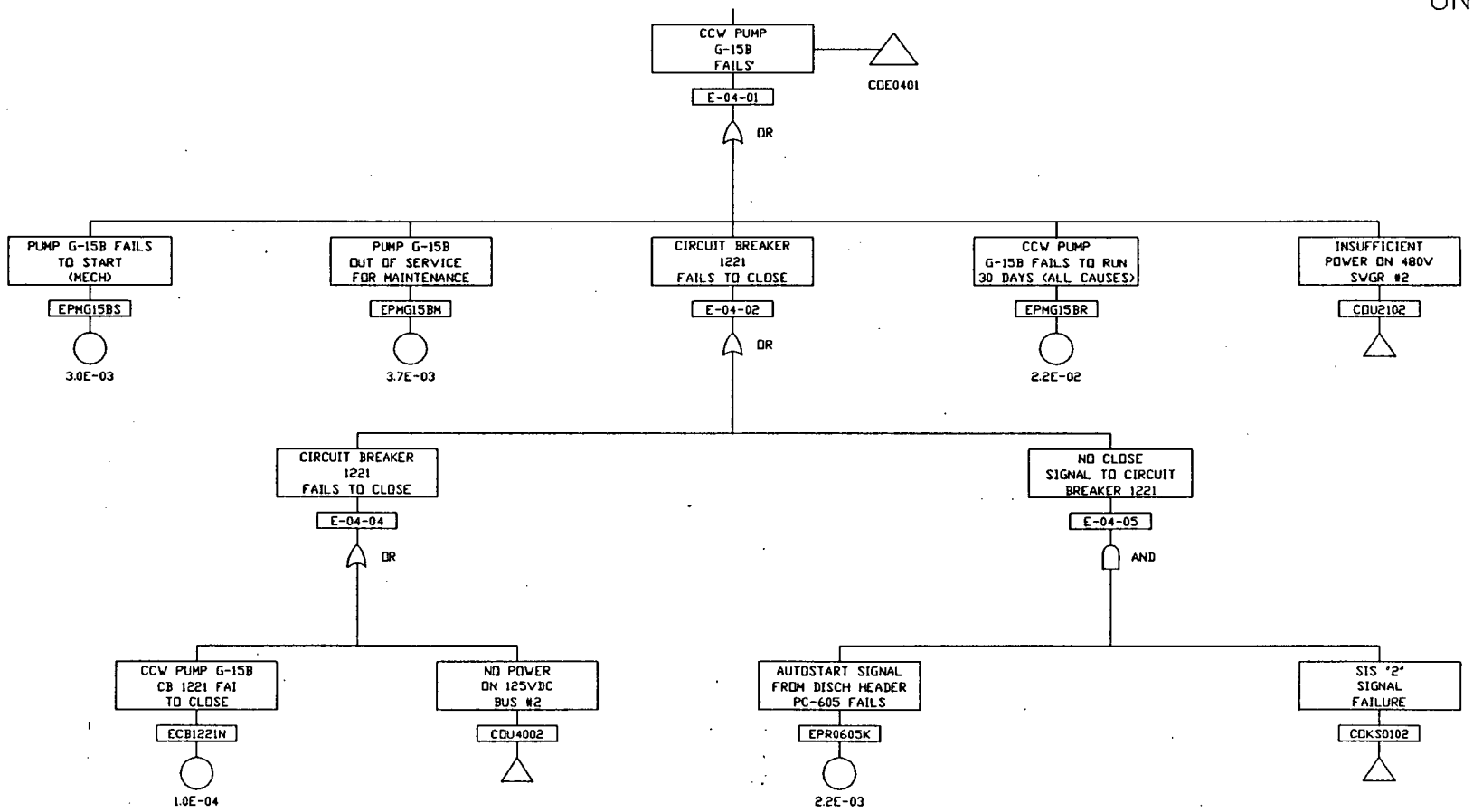
UNIT 1



2/3/89

FIGURE E, SHEET 4

UNIT 1

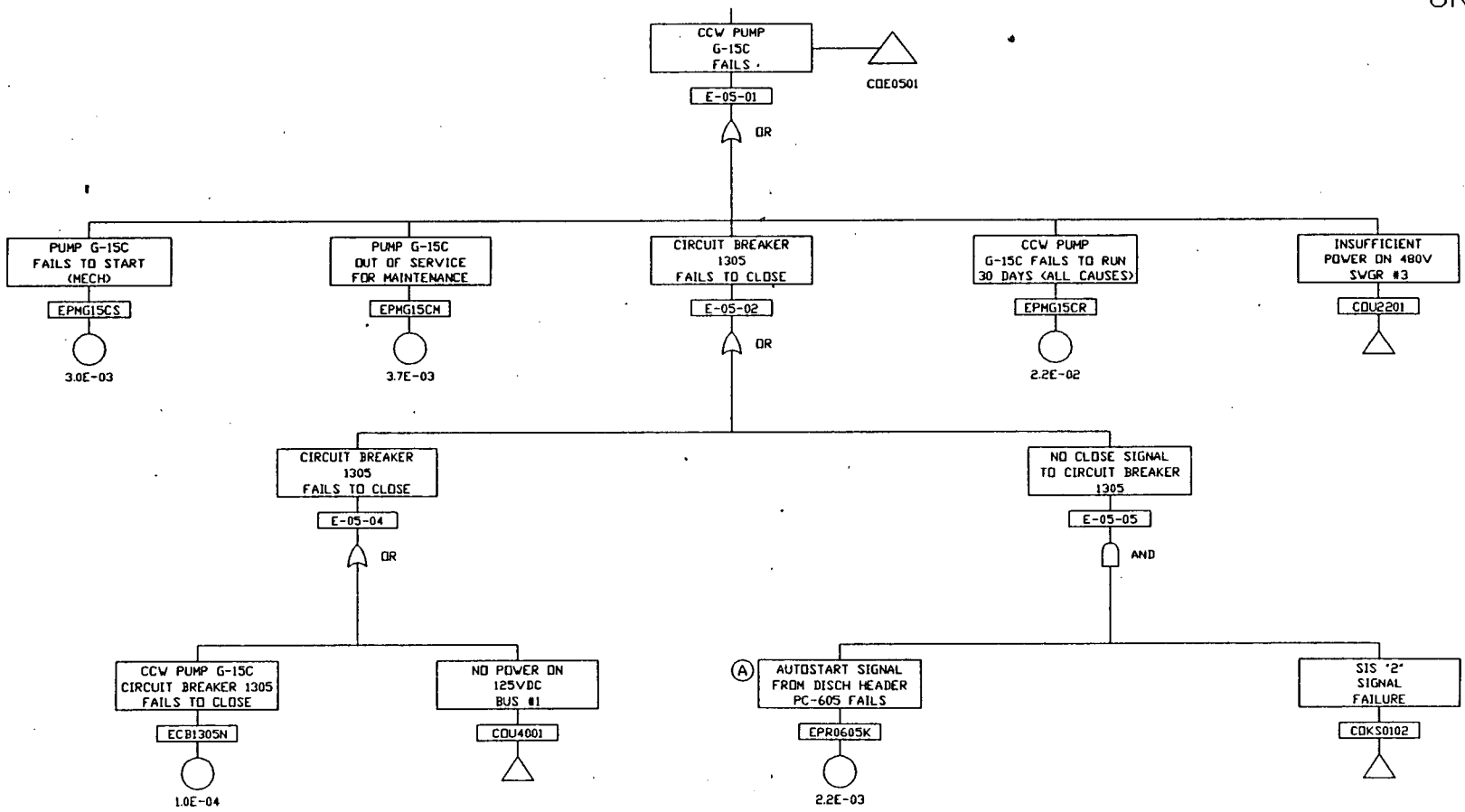


Ⓐ OI SO1-2.1-10, "LOSS OF COMPONENT COOLING WATER SYSTEM"

3/16/89

FIGURE E, SHEET 5

UNIT 1



(A) DI SO1-2.1-10, "LOSS COMPONENT COOLING WATER SYSTEM"

10/10/88

ATTACHMENT B-2 Overall Assessment of Events Impacted by TCV-601A/B Failure

GENERAL: In the historical case (i.e., prior to rebalancing the CCW system with reduced flow to the spent fuel pit heat exchanger), failure to the open position of either TCV-601A or TCV-601B with the balance of the system in its normal operating configuration, would have resulted in a total system demand in excess of the capacity of one CCW pump. However, failure to the open position of both TCV-601A and TCV-601B (for example, due to instrument air failure) would not have exceeded the capacity of two running pumps even with the recirculation heat exchanger aligned. Thus, only under concurrent single failure conditions, in which only one of the two Technical Specification required CCW pumps would have been available, would cavitation and air-binding of the running pump and interruption of CCW flow have occurred. As described in more detail in Issue #5, this interruption would have been limited to 2 hours or less, and would not affect the capability of the charging pumps via their lube oil cooling. The pertinent effects would be a loss of forced reactor coolant flow (following the loss of RCP motor cooling), loss of residual heat removal system capability, and loss of recirculation system cooling capability.

DISCUSSION: The above identified effects are addressed further below:

Increased/Decreased Secondary Heat Removal:

A natural circulation cooldown to RHR entry conditions could be required, but is already assumed for the bounding non-pipe break events. If the single failure affecting CCW were to occur after RHR entry, a return to steaming conditions could occur. However, based on the existing procedures, steam generator level could be reasonably expected to have been recovered into the normal range prior to RHR entry, and additional condensate aligned prior to exhausting the AFW tank, to support this system response.

For secondary pipe break events assuming RHR is unavailable in the worst case event, long-term cooling for SONGS 1 utilizes either secondary recirculation (breaks in containment) or continued steaming (breaks outside containment). Secondary recirculation does not occur until at least 4 hours post-accident, after restoration of CCW can be assumed, and continued steaming does not require CCW. In either case, the dose consequences reported in the FSAR (0-2 hour at exclusion area boundary) would have remained bounding.

Reactivity/Distribution Events:

Same effects as the non-pipe break secondary heat removal events.

Loss of Forced Reactor Coolant Flow:

Same effects as the non-pipe break secondary heat removal events. TCV failure could also have initiated this event.

Increase in RCS Inventory:

Same effects as the non-pipe break secondary heat removal events.

Decrease in RCS Inventory:

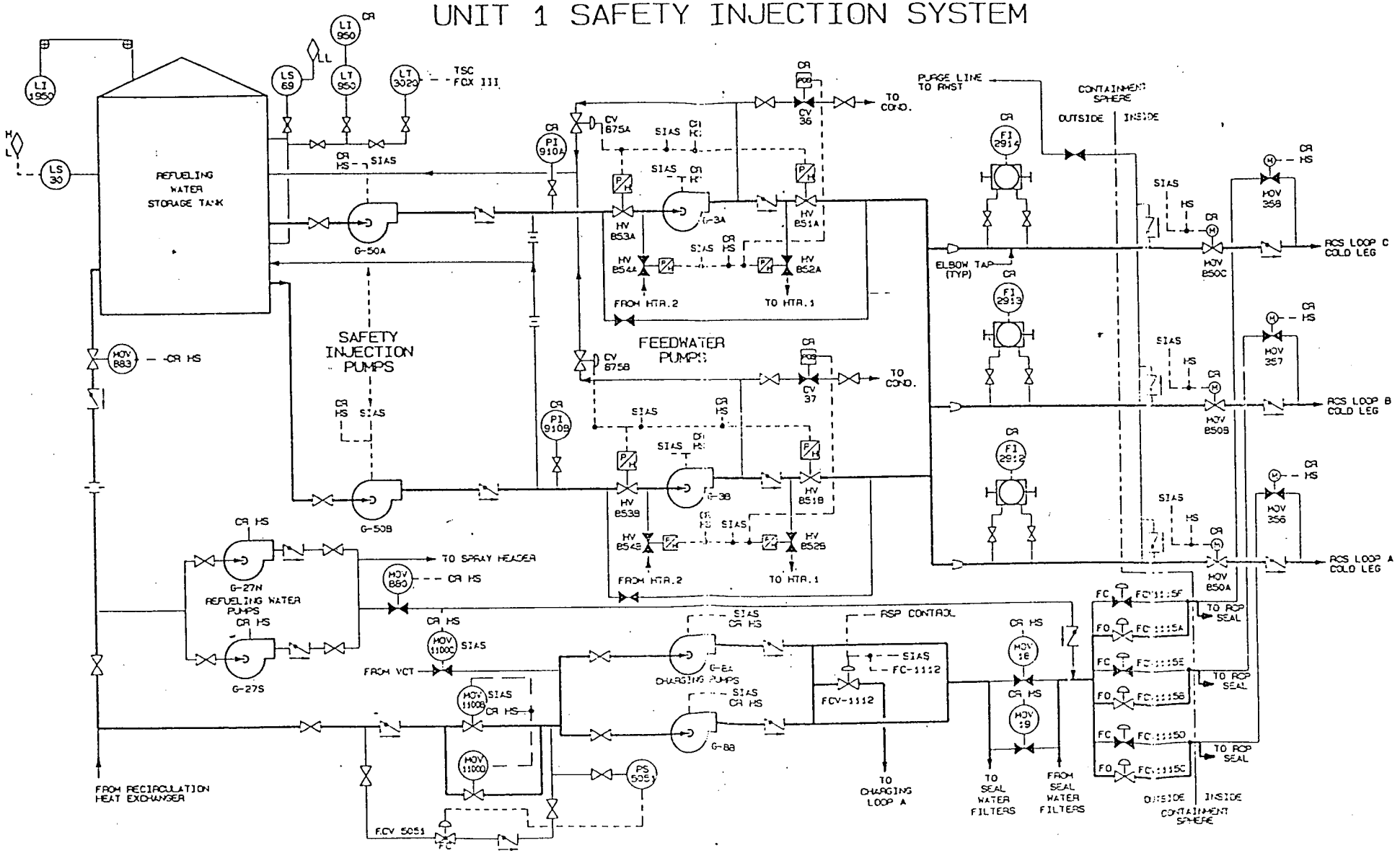
For the control system malfunction events, the loss of non-regenerative letdown cooling following CCW failure could result in the diversion of letdown flow to radwaste in lieu of return to the volume control tank. However, this remains bounded by the analyzed events which do not assume makeup to the VCT. The impact on long-term cooling via RHR would be the same as the non-pipe break secondary heat removal events discussed above.

For Steam Generator Tube Rupture (SGTR) events, the interruption of CCW flow could have resulted in up to 2 additional hours of steaming. However, the dose consequences reported in the FSAR (0-2 hour at exclusion area boundary) would have remained bounding.

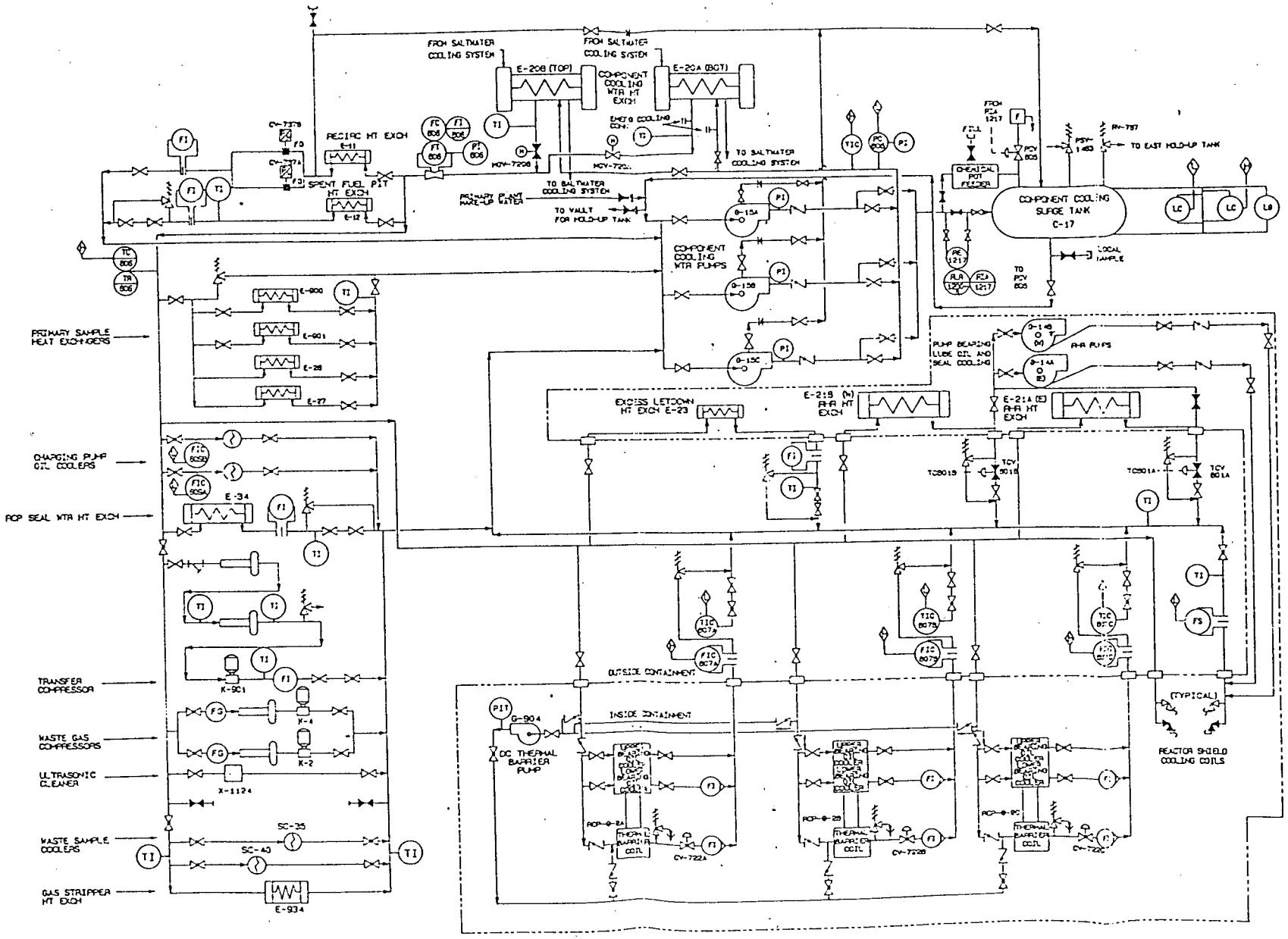
For large break Loss of Coolant Accidents (LOCAs), recirculation conditions can be reached in as little as 10 minutes. An interruption of CCW to the recirculation heat exchangers of up to 2 hours would increase the temperature of the recirculated fluid to the charging and refueling water (containment spray) pumps, reduce containment spray effectiveness and result in degraded containment heat removal. Small break LOCAs would require longer to reach recirculation conditions, and so would be less limiting.

CONCLUSION: The limiting event in terms of CCW interruption resulting from TCV-6001A/B failure is the large break LOCA.

UNIT 1 SAFETY INJECTION SYSTEM

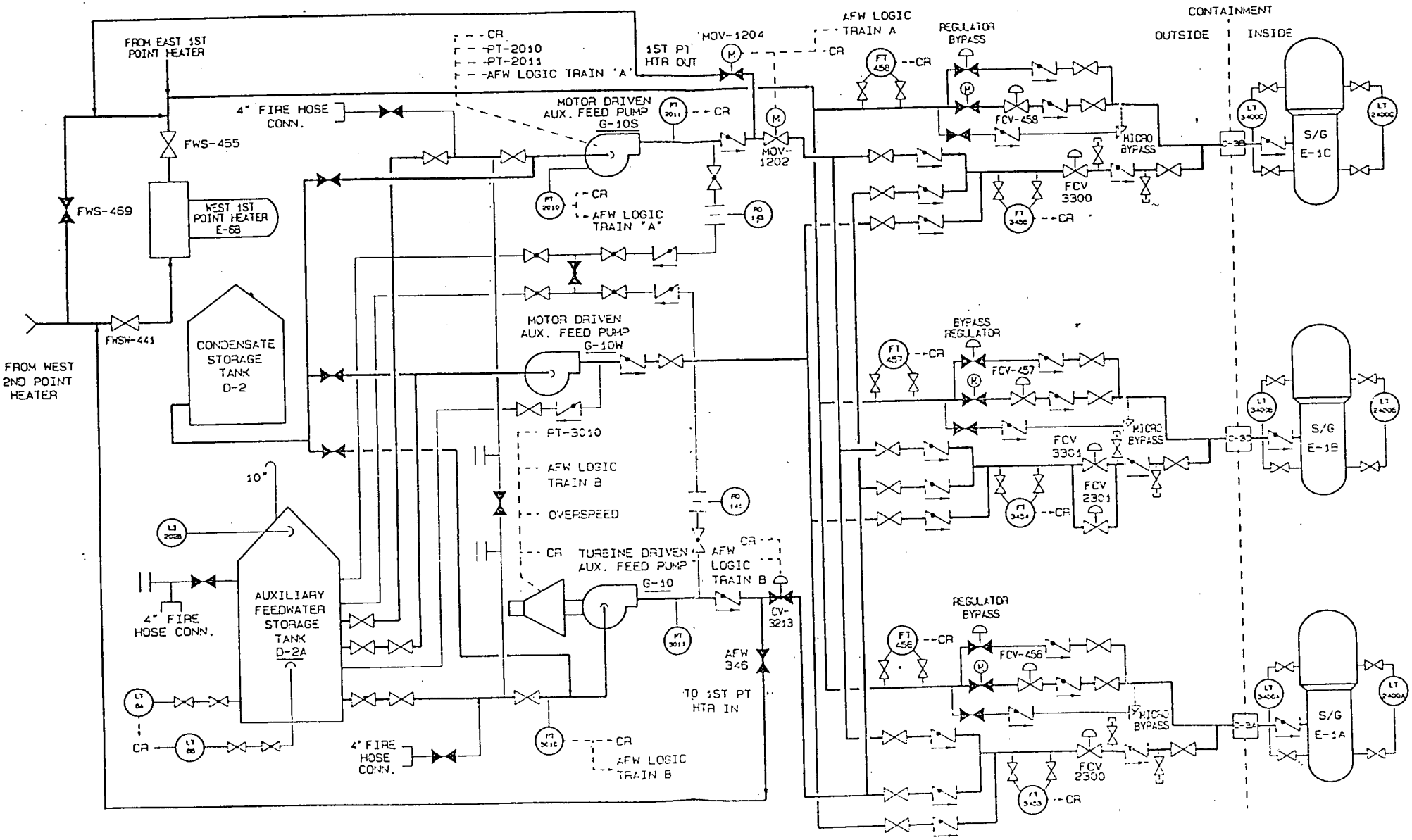


COMPONENT COOLING WATER SYSTEM

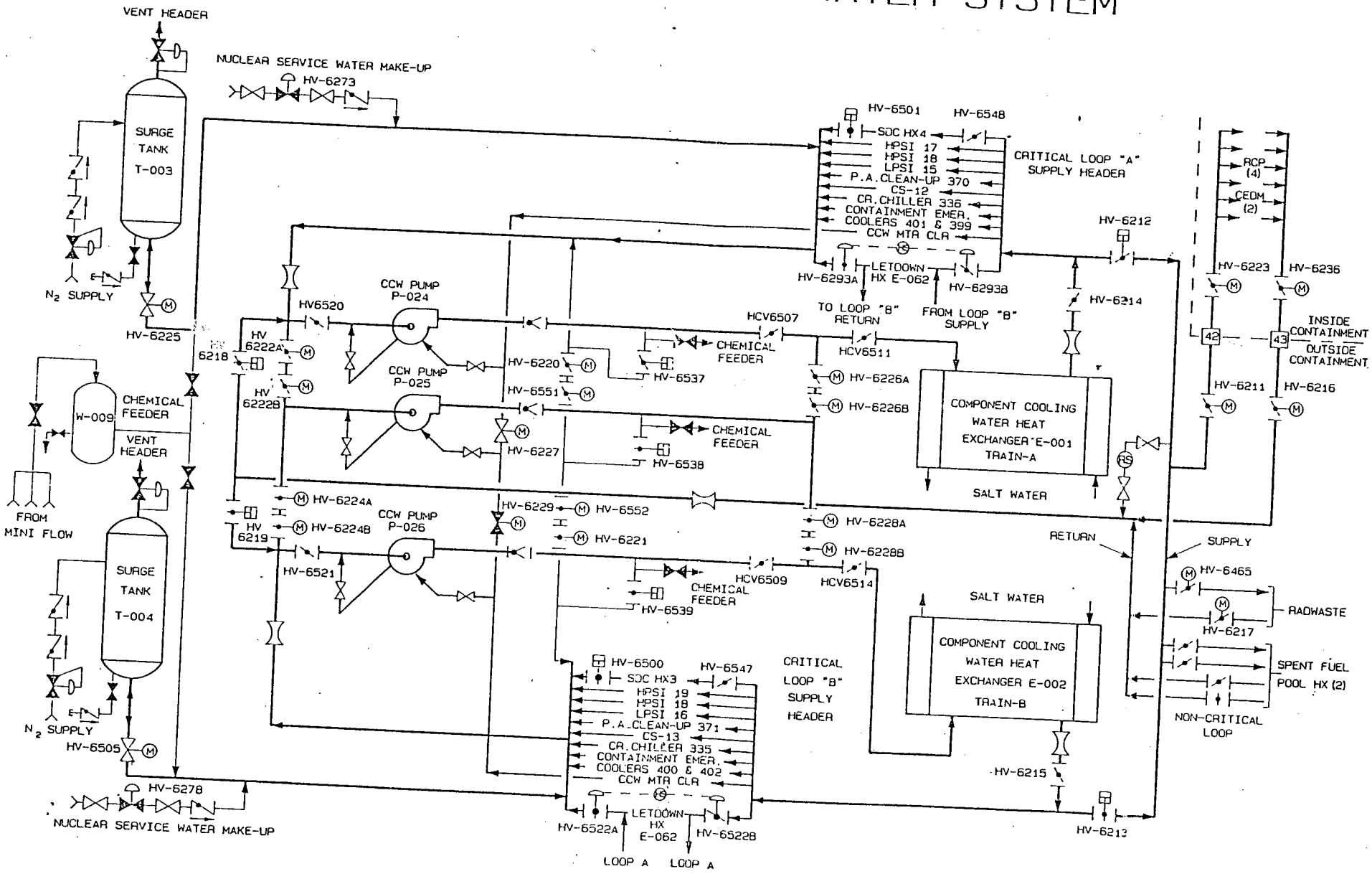


ATTACHMENT E

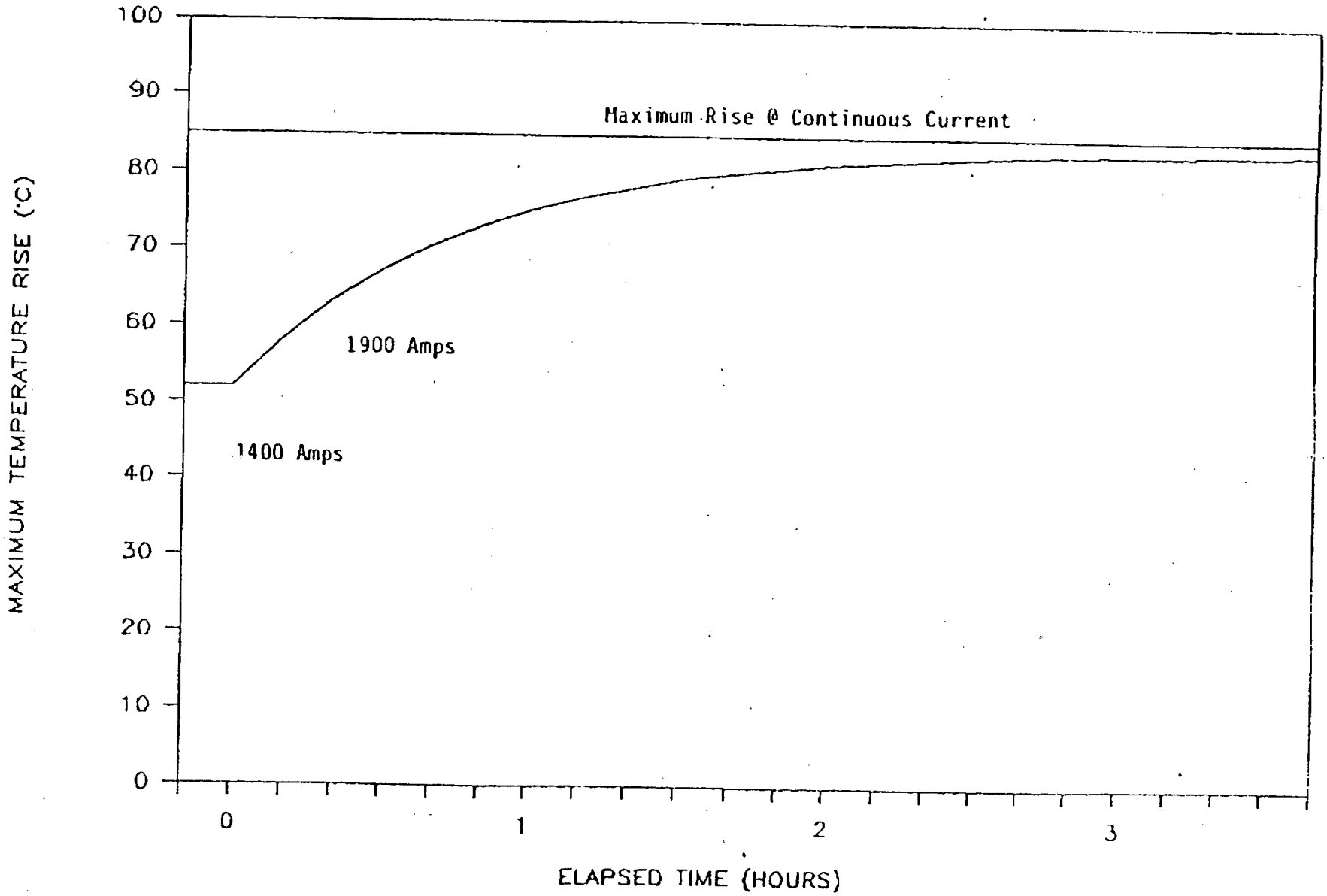
AUXILIARY FEEDWATER SYSTEM



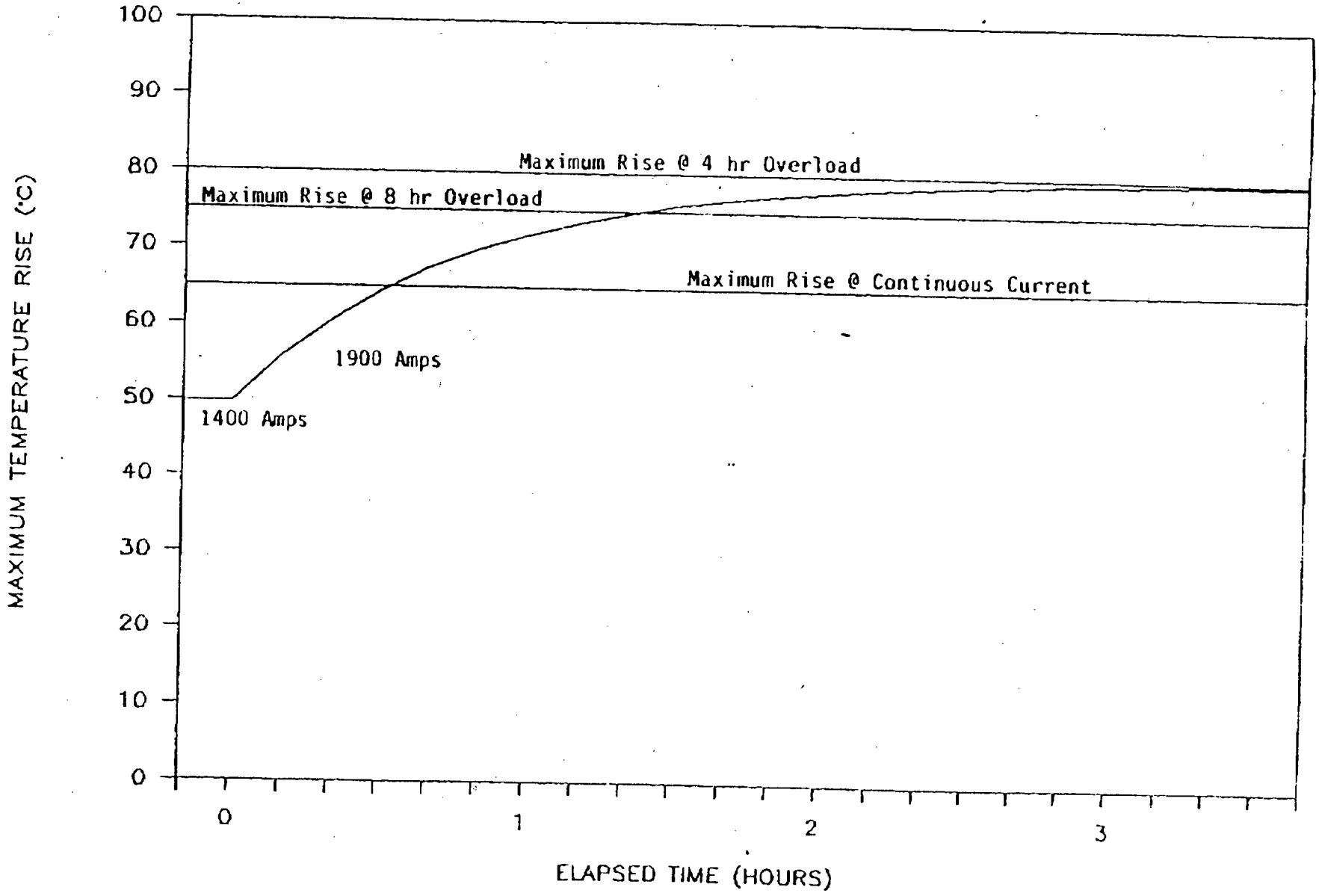
COMPONENT COOLING WATER SYSTEM



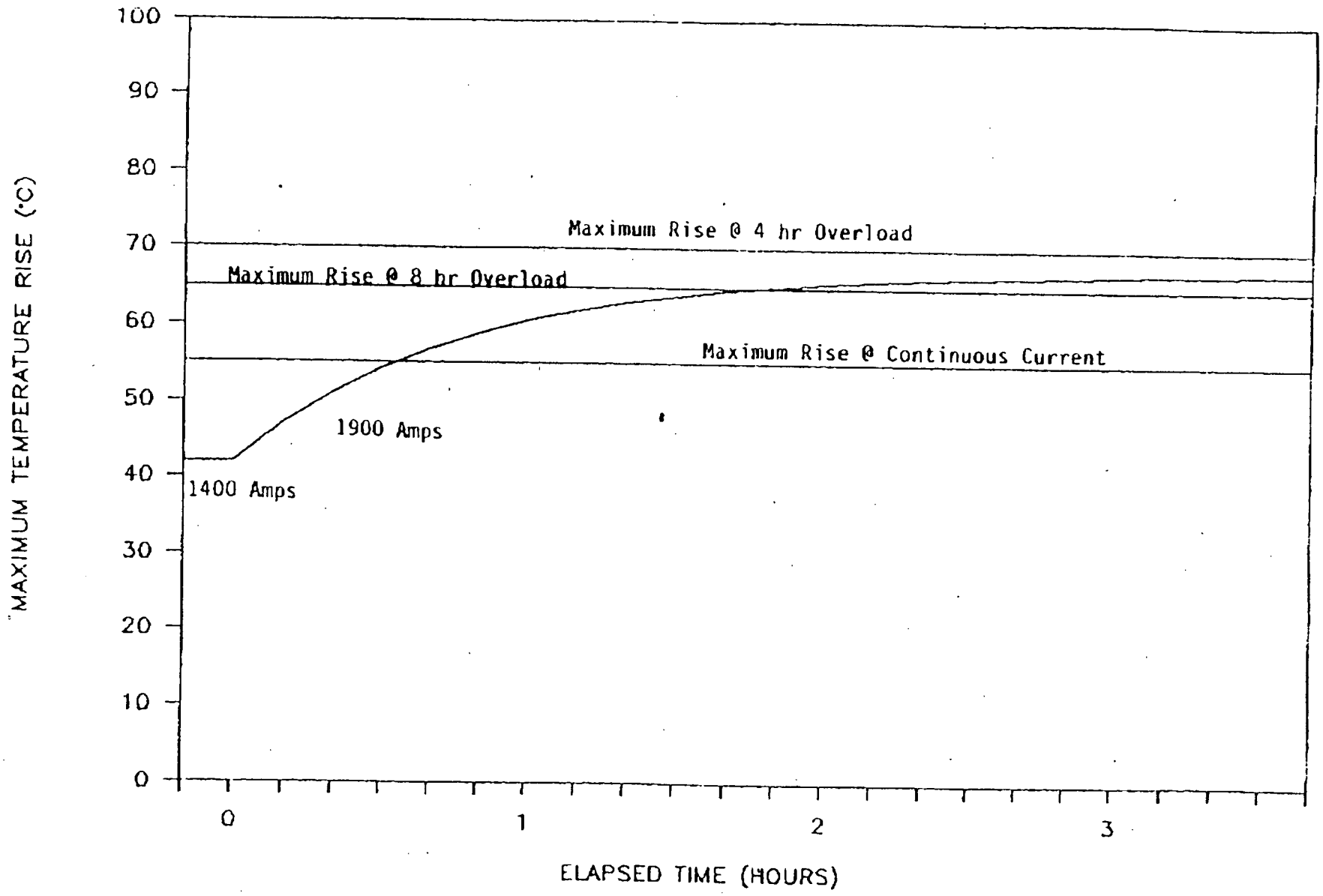
DB-50 MAIN CONTACT THERMAL RESPONSE



DB-50 INSULATION THERMAL RESPONSE



DB-50 BUS CONNECTION THERMAL RESPONSE



CONTAINMENT PRESSURE/TEMPERATURE EVALUATION (LOSS OF RECIRCULATION COOLING)

An analysis was performed to assess the safety significance of a loss of CCW cooling to the recirculation heat exchanger post-LOCA. Loss of CCW results from a postulated failure due to loss of air to TCVs-601A and B that control flow to the RHR heat exchangers and cause the running CCW pump to cavitate assuming single failure of a second CCW pump to auto start. Two cases were analyzed to assess the effect on containment temperature-pressure transient post-LOCA.

CASE 1: Design basis case assuming normal operation of the recirculation heat exchanger (1000 gpm) initiated at the start of the recirculation mode (1250 seconds).

CASE 2: No CCW flow to the recirculation heat exchanger for 2 hours post-LOCA. At 2 hours the operator throttles the CCW pump discharge valves and restarts one CCW pump resulting in partial CCW flow (435 gpm based on hydraulic calculation) to the recirculation heat exchanger.

METHODOLOGY

The containment pressure analyses was performed in accordance with Bechtel's Topical Report "Performance and Sizing of Dry Containments," BN-TOP-3A using the Bechtel COPATTA computer program.

The COPATTA model conservatively predicts both the pressure and temperature within the containment regions and the temperatures in the containment structures. Separate blowdown and core thermal behavior studies were made by Westinghouse to determine mass and/or energy input rates from sources such as: the release of reactor coolant, decay energy and sensible heat release, which may cause heating or boil-off of residual water in the reactor vessel or super-heating of steam as it passes through the steam generator and enters the containment through the postulated point of reactor coolant system rupture.

The COPATTA model treats the containment and the heat transfer surfaces following a LOCA. Included in this model are ESF system parameters and analytical techniques that enable calculation of their effects upon the containment. Several options are incorporated in the model to facilitate use of these features.

COPATTA calculates a pressure-time transient with stepwise iteration between the thermodynamic state points. The iterations are based on the laws of the conservation of mass and energy together with their thermodynamic relationships. Superposition of heat input functions is assumed so that any combination of coolant release, decay heat generation, and sensible heat release can be used with appropriate ESF features to determine the containment pressure-time history associated with a LOCA.

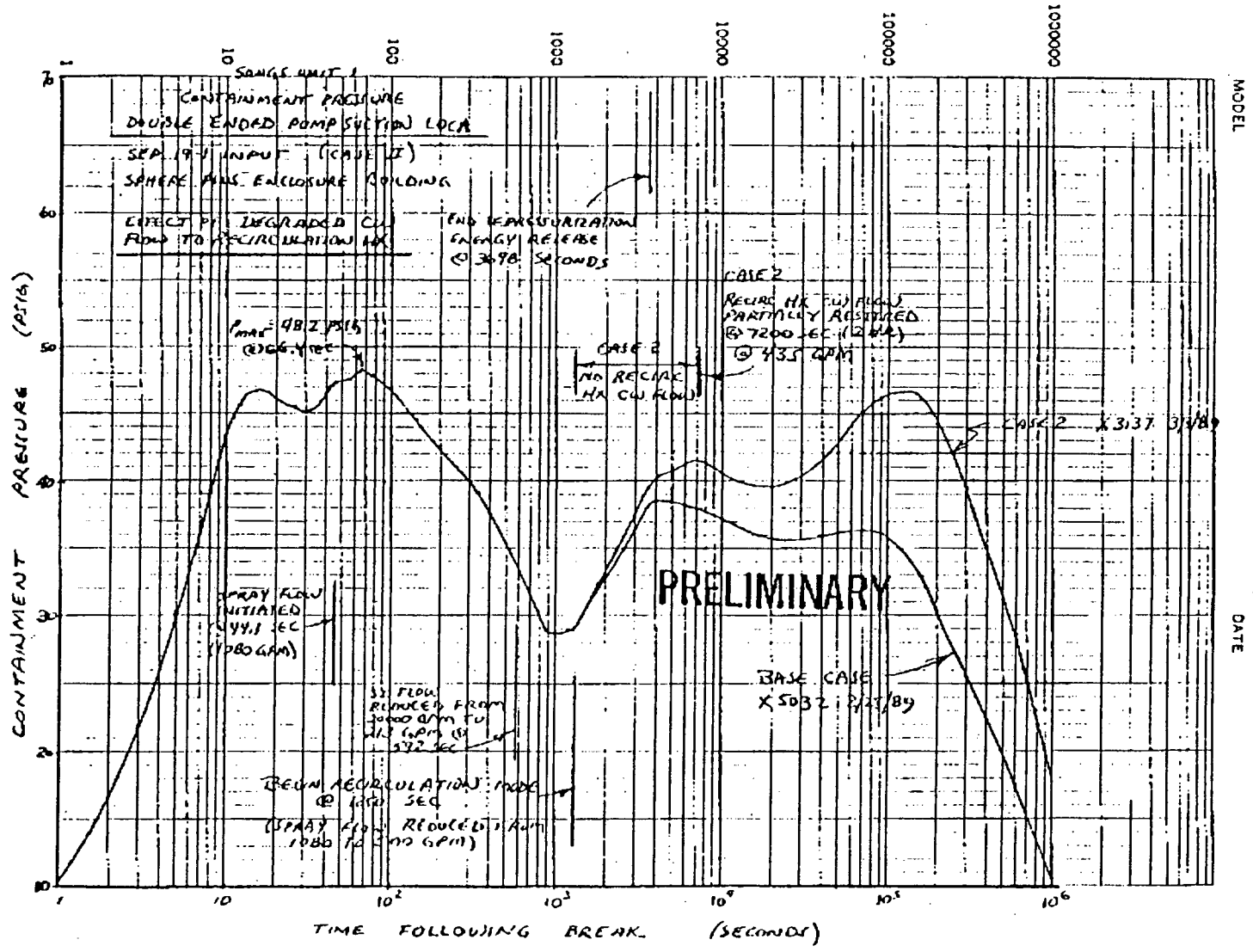
The program uses a three region containment model consisting of: the containment atmosphere (vapor region), the sump (liquid region), and the water contained in the reactor vessel. Mass and energy are transferred between the liquid and vapor regions by boiling, condensation, or liquid dropout. Evaporation is not considered. A convective heat transfer coefficient can be specified between the sump liquid and atmosphere vapor regions. However, since any heat transfer in this mode is small, a conservative coefficient of zero was assumed. Each region is assumed homogeneous, but a temperature difference can exist between regions. Any moisture condensed in the vapor region during a time increment is assumed to fall immediately into the liquid region. Noncondensible gases are included in the vapor region.

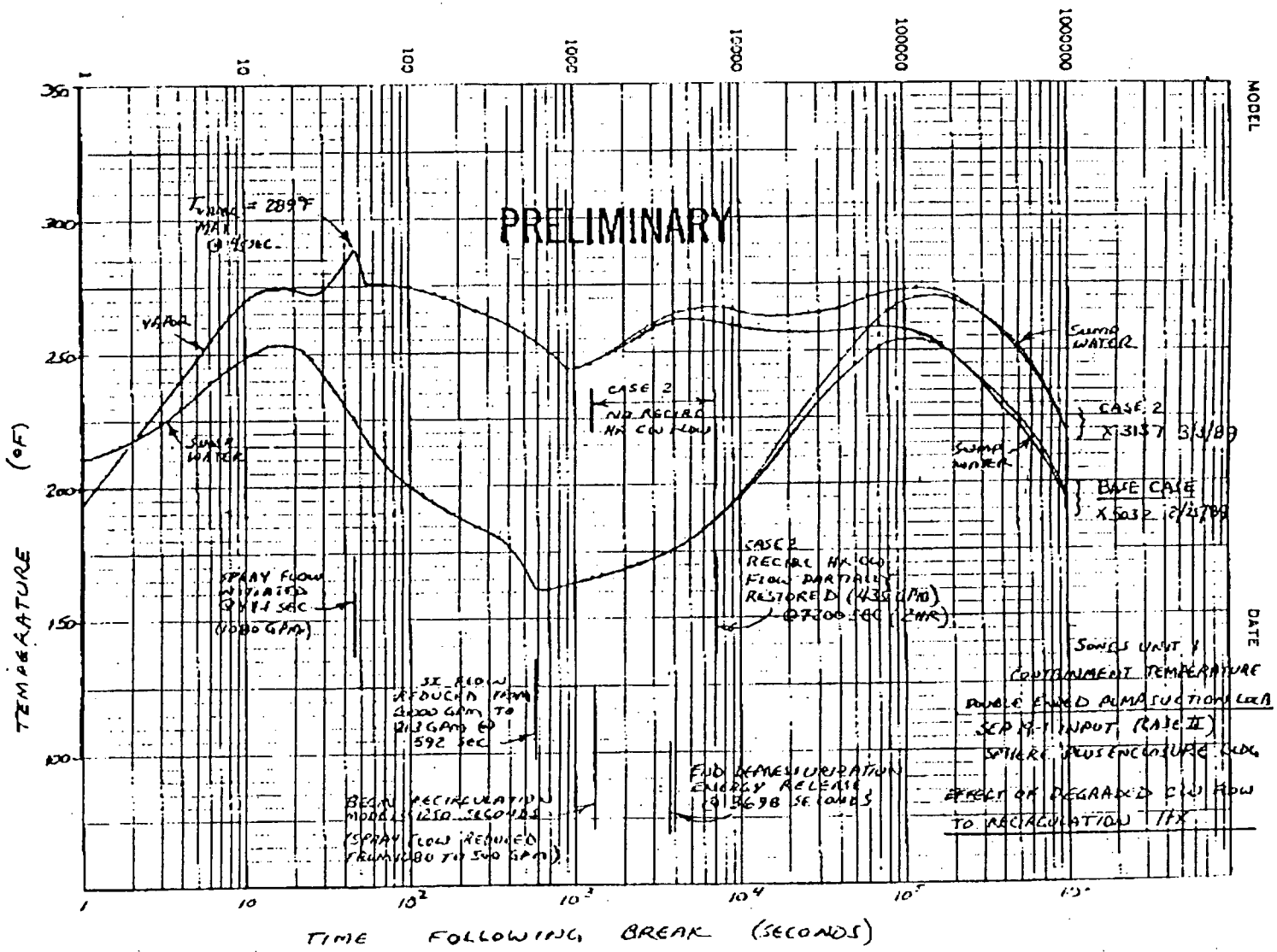
RESULTS

The containment pressure and temperature response and sump water temperature response versus time are shown in Figures 1 and 2. For the base case COPATTA calculated peak pressure is 48.2 psig at 66 seconds and peak temperature is 289 degrees F at 45 seconds. A secondary pressure peak of 38.5 psig occurs at approximately one hour.

For the case where partial CCW flow to the recirculation heat exchanger is initiated at 2 hours, sufficient heat removal is provided to maintain containment pressure within design limits and below the blowdown pressure peak. The secondary pressure peak is 46.7 psig at 1.6 days. Containment temperature is 273 degrees F at 1.6 days which is approximately 11 degrees F increase compared to the design basis case. Heat removal by the recirculation heat exchanger was calculated to be 3.65 E9 BTU/hr at 10.4 days compared to 3.9 E9 BTU for the design basis case.

The results of the case with partial recirculation heat exchanger flow indicate that recovery options are available which mitigate the effect of an initial loss of CCW flow to the recirculation heat exchanger and maintain the plant well within design limits.


SONGS UNIT 1
CONTAINMENT PRESSURE
DOUBLE ENDED PUMP SUCTION LOCA
SEP 19-1 INPUT (CASE II)
SPHERE PLUS ENCLOSURE COOLING
EFFECT OF DEGRADED CW FLOW TO RECIRCULATION HX
END DEPRESSURIZATION ENERGY RELEASE @ 3698 SECONDS
CASE 2
RECIRC HX CW FLOW PARTIALLY RESTORED @ 7200 SEC (2 HR) @ 435 GPM
CASE 2
NO RECIRC HX CW FLOW
P_{max} 48.2 PSIG @ 66.4 SEC
SPRAY FLOW INITIATED @ 44.1 SEC (1080 GPM)
SI FLOW REDUCED FROM 1000 GPM TO 415 GPM @ 372 SEC
BEGIN RECIRCULATION MODE @ 1650 SEC
(SPRAY FLOW REDUCED FROM 1080 TO 300 GPM)
PRELIMINARY
BASE CASE
X 5032 2/27/84
CASE 2 X 3137 3/1/84
CONTAINMENT PRESSURE (PSIG)
TIME FOLLOWING BREAK (SECONDS)
MODEL
DATE


PRELIMINARY
MODEL
DATE
TEMPERATURE (°F)
TIME FOLLOWING BREAK (SECONDS)
1
10
100
1000
10000
100000
1000000
10^2
10^3
10^4
10^5
10^6
350
300
250
200
150
100
T_{max} = 289°F MAX @ 45 sec.
VAPOR
SUMP WATER
CASE 2 NO RECIRC HX CCW FLOW
CASE 2 X 3137 3/3/89
SUMP WATER
BASE CASE X 5032 2/27/89
CASE 2 RECIRC HX CCW FLOW PARTIALLY RESTORED (435 GPM) @ 7200 SEC (2 HR)
SPRAY FLOW INITIATED @ 41.1 SEC (1080 GPM)
SI FLOW REDUCED FROM 4000 GPM TO 1913 GPM @ 592 SEC
BEGIN RECIRCULATION MODEL (1250 SECONDS)
(SPRAY FLOW REQUIRED FROM 1080 TO 540 GPM)
END BLOWDOWN/BEGIN ENERGY RELEASE @ 3698 SECONDS
SONGS UNIT 1
CONTAINMENT TEMPERATURE
DOUBLE ENDED PUMP SUCTION LOCA
SCRAM INPUT (CASE II)
SUMP RECIRCULATION FLOW
EFFECT OF DEGRADED CCW FLOW TO RECIRCULATION HX

ATTACHMENT I PRA of Failure of RWP G27S

THE IMPACT OF A MISPLACED WIRE IN THE REFUELING WATER PUMP OPERATING CIRCUITRY ON CORE MELT FREQUENCY FOR UNIT 1

1.0 PURPOSE

The purpose of this analysis is to assess the impact on core melt frequency of a residual jumper wire in the operating circuitry of Refueling Water Pump (RWP) G-27S.

2.0 BACKGROUND

An unwarranted jumper wire was found in the control circuit of Refueling Water Pump (RWP) G-27S. In the unlikely event of a Loss of Off-site Power (LOP), the jumper would have prevented the automatic start of the South Refueling Water Pump (RWP) G27S upon receipt of a Containment Spray Actuation Signal (CSAS) if the CSAS were generated between 11.5 seconds after the LOP and 34 seconds after re-energization of the bus. In this sequence, the RWP can only be started manually from the control room. The other RWP, G27, was inspected and tested for the presence of a similar jumper and none was found.

Specific details of the circuitry are provided for completeness.

1. The actuation of the Refueling Water Pump (RWP) undervoltage (UV) protective relay concurrent with the Containment Spray Actuation Signal disables the RWP. The pump, however, can be started manually by the operator after the UV relay has been reset.

2. To be able to start RWP G-27S, the undervoltage relay must be reset. The operator can then do either of two recovery actions. He can either 1) reset and reinitiate CSAS or, 2) depress the OVERRIDE and START pushbuttons. Again, both operations must occur after the UV relay resets. Actuation of the UV relay is annunciated by double brilliant light indication. Resetting of the UV relay causes the same lights to reduce illumination to normal brilliance.

3. The RWP UV protective relay actuates if an undervoltage condition exists for 11.5 seconds (assuming a complete loss of bus, i.e. 0 voltage).

   Note: The UV relay actuation delay time is dependent on the voltage on the bus. For example, if the bus voltage is degraded to **89%** rated voltage, the undervoltage condition must continue for **200s** before the UV relay actuates. And at **0%** rated voltage, the UV relay actuates if the condition exists for **11.5s.**

4. Given the UV relay is actuated, the relay needs to see proper voltage (restored power) for 27-34 seconds before the relay resets.

5. If a CSAS occurs after the UV relay resets, RWP G-27S starts automatically.

6. Normal operation of the RWP (w/o extraneous jumper) is automatic given CSAS since the UV protective relay is bypassed.

7. A CSAS permissive immediately follows a SIS but delayed 21 seconds after a SISLOP.

8. The Diesel Generator (DG) takes **10 seconds** to reach proper voltage and frequency and **1 second** to close DG output breaker. Therefore, if a demand for DG power occurred at 10.5 seconds, the DG output breaker would close at 11.5 seconds, at which time the RWP UV relay would actuate.

3.0 ANALYSIS

Sequence of Interest:

LOP ---> SIS [occurring after 10.5s post-LOP]

---> CSAS [occurring before restoration of bus voltage +34 seconds]

The configuration of the containment spray system in the sequence of interest is modeled using a fault tree logic model (Figure 1). The data used to quantify the fault tree model are given below:

PROBABILITIES

	EVENT	FREQUENCY (YR^{-1})	SOURCE
1.	Loss of Offsite Power (LOP)	4.5E-2	NSAC/85, "LOP at Nuclear Power Plants"
2.	Large LOCA	9.3E-4	Oconee PRA
3.	Small LOCA	3.0E-3	Oconee PRA
4.	Operator omits step in procedure	0.001 (0.1 is conservatively used in the analysis.)	NUREG/CR-1278 [Table 20-7, Item (3)]
5.	RWP G-27, G-27S Fails to Auto-Start Given Signal	3.0E-3 (1.0 is conservatively used in the analysis for RWP	NUREG/CR-3511, IREP Study
6.	RWP G-27, G-27S Fails to Run For 30 Days	G-27S. 2.2E-2	NUREG/CR-3511, IREP Study

Additional assumptions used in the fault tree model are:

1. Only small (3/4" - 3" break size) and large (break size > 3") LOCAs would pressurize the containment such that containment spray is required.

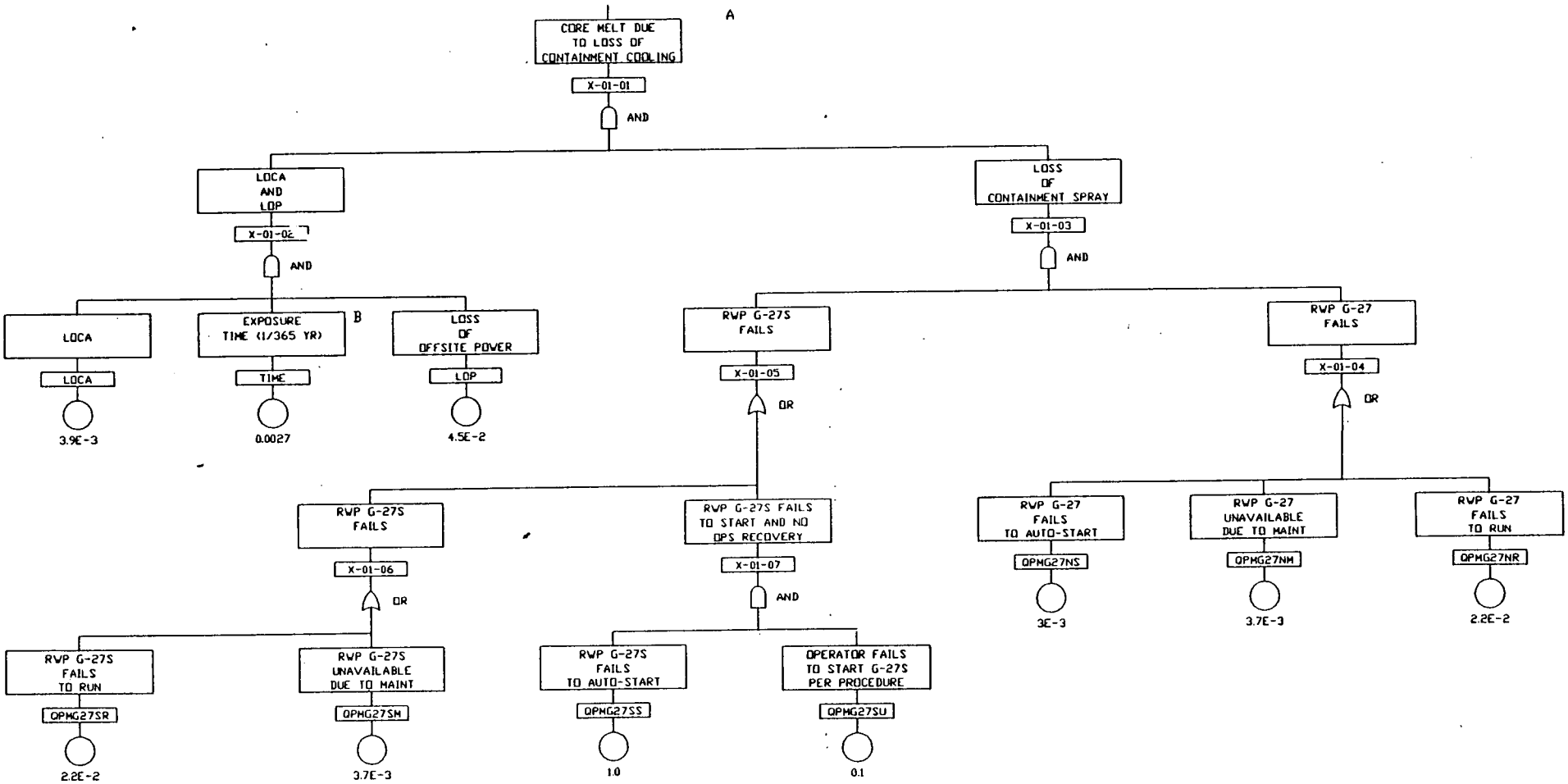
2. It is assumed that s MSLB will not lead to core melt regardless of whether containment sprays operate.

3. The window of exposure after a LOP during which a SIS could challenge the auto-start capability of G-27S is conservatively assumed to be 24 hours.

4. CONCLUSION

The calculated core melt frequency of 1.7E-9/YR is the expected core melt frequency due to a Loss of Offsite Power and a delayed but concurrent Loss of Coolant Accident assuming Loss of Containment Spray leads to core melt.

SONGS1 RWP G-27S WIRE DISCREPANCY



A) ASSUMES LOSS OF COMTAINMENT SPRAY LEADS TO CORE MELT

B) EXPOSURE TIME IS CONSERVATIVELY ASSUMED TO BE 1 DAY

3/10/89

ATTACHMENT J PRA of Diesel Generator Loading Failure on SIS/LOP

THE IMPACT ON CORE MELT FREQUENCY OF A LOSS OF SAFETY INJECTION AT SONGS UNIT 1 GIVEN A SIS/LOP

1. PURPOSE

The purpose of this analysis is to determine the impact on core melt frequency of a single failure of a train of safety injection given a SIS/LOP under the pre-Cycle 10 Safeguard Load Sequencing Systems (SSLS) design.

2. BACKGROUND

During a LOCA and a concurrent Loss of Offsite Power, the SSLS generates a SIS/LOP sequencer signal. The SIS/LOP signal initially sends start signals to both Diesel Generator 1 and Diesel Generator 2. Both DGs should start, run, and load to their respective 4KV buses simultaneously. However, during testing, it was discovered that loading of the DGs is not simultaneous and that the loading of one DG will remove the undervoltage condition on the sequencer input and will prevent the loading of the other DG.

In the event of a single failure of the Safety Injection train which receives power from the loaded DG, both trains of safety injection would be unavailable.

3. ANALYSIS

The sequences of interest are:

1. LOCA (break diameter > 1 inch) & Loss Of Offsite Power & SI Train A Failure & Train B DG failure to load

2. LOCA (break diameter $\leq$ 1 inch) & Loss Of Offsite Power & SI Train A Failure & Train B DG failure to load & No operator recovery of Safety Injection

The SONGS Unit 1 Probabilistic Safety Assessment (PSA) was used to evaluate the subject sequences. In particular, the LOCA sequences from the study were evaluated using the following initiating event frequencies[1]:

A. LOCA (break size > 1 inch) = 2.9E-3/yr

B. LOCA (break size $\leq$ 1 inch) = 5.5E-2/yr

---

[1]Extrapolated from WASH-1400, Reactor Safety Study, U.S.N.R.C., October 1975.

In addition, the following assumptions were used to modify the Safety Injection System model as it would operate during a SIS/LOP condition.

A. DG 1 output breaker closes and supplies power to Safety Injection Train A.

B. DG 2 output breaker remains open leaving SI Train B without a power source.

The results of the PRA indicate the failure probability of an SI train given the above assumptions to be 0.034.

The probability of a concurrent loss of offsite power is assessed to be 0.001.

Evaluating possible operator actions to recognize, diagnose and respond to output breaker failure to close requires the following assumptions:

A. During a LOCA with a break size greater than 1 inch, the operator does not have sufficient time ($t < 20$ minutes) to respond to a loss of safety injection.

B. During a LOCA with a break size smaller than 1 inch, the operator has approximately 20 minutes or more to respond and close the DG output breaker. During these 20 minutes, several events would be occurring simultaneously which would affect the ability of the control room personnel to respond appropriately. Following a LOCA, alarms and annunciators would actuate. Under the increased stress of the event, the control room personnel would:

a) Verify reactor trip. By following Station Procedure SO1-1.0-10, "Reactor Trip or Safety Injection", the operators would have verified that the reactor and turbine have tripped. This should be done rather quickly.

b) Verify electrical buses are energized. In Step 3 of SO1-1.0-10, the operator is asked to verify that 4KV buses 1C and/or 2C are energized. In the process of verification, the operator would become aware that one of the DG output breakers had not closed on the bus since breaker indication is on the adjacent control room panel as 4KV bus power indication. The operator would then, if only one bus is energized, continue as instructed with the procedure. If he does, then he will go on to verify SI valve and pump breaker alignment [skip next item (c) and go to item (d)]. Possibility has been given, based on the "Response Not Obtained" column of Step 3 (SO1-1.0-10), for the operator to transfer or review Station Procedure SO1-1.0-60, "Loss Of All AC Power." If he does, Step 1 asks the operator to verify loss of power from the switchyard. Since by definition a LOP has occurred, the operator would be guided to Step 8.

c) Verify Diesel Generator operation. In Step 8 of SO1-1.0-60, the operator is asked to verify at least one DG is running and if SISLOP has been actuated. If so, then he is to ensure that at least one of the DG output breakers is CLOSED and initiate DG load monitoring. Although both DGs are running, the operator would notice that the one of the DG output breakers have not closed. The operator may not close the open breaker at this point since the procedure only directs the operator to ensure at least one is closed. The operator would then be transferred back to Station Procedure SO1-1.0-10, where in Step 5, he is asked to verify RCP trip.

d) Verify SI valve alignments and SI System pump breaker positions. Verifications are guided by Steps 6 and 7 (SO1-1.0-10). At this point, the operator would get confirmation that power is unavailable on one electrical train since the pump breakers associated with the train are in the open position.

e) Verify adequate SI flow (Step 8). Since Train B Safety Injection is unavailable and assuming a single failure in Train A SI, SI flow indication would display no flow. With no SI flow indication and the knowledge that the DG output breaker aligned with Train B SI is open, the operator would diagnose that Train B Safety Injection is needed and would require the DG output breaker to be closed to provide source power.

   Closure of the DG breaker at this point will result in an unsequenced block load of safety related equipment on to the diesel. However, experience has demonstrated that this will not negatively impact the diesel due to the excess capacity of the diesel and inherent impedance in the electrical system.

Based on NUREG/CR-1278[2], the probability of the team of control room personnel failing to recognize, diagnose and respond appropriately in 20 minutes is 0.1.

---

[2]Item 9 of Table 20-3, NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, A. D. Swain, H. E. Guttman, 1983. Item 9 is appropriate since the control room personnel must diagnose and respond to two abnormal events (i.e. failure of Train A SI and loss of power to Train B SI) within 20 minutes.

The probabilities of the sequences of interest are calculated as follows:

1. [Freq. of Core Melt due to LOCA (diameter > 1")] =

   = [Freq. of LOCA (d > 1")] *
   [Prob. of Conditional Loss of Offsite Power] *
   [Prob. of SI Train A Failure]

   = 2.9E-3/yr * 0.001 * 0.034

   = 9.9E-8/yr

2. [Freq. of Core Melt due to LOCA (diameter $\leq$ 1")] =

   = [Freq. of LOCA (d $\leq$ 1")] *
   [Prob. of Conditional Loss of Offsite Power] *
   [Prob. of SI Train A Failure] *
   [Failure of the operator to load Train B DG]

   = 5.5E-2/yr * 0.001 * 0.034 * 0.1

   = 1.9E-7/yr

3. The combined core melt frequency for the two sequences of interest is:

   9.9E-8/yr + 1.9E-7/yr = 2.9E-7/yr

4. CONCLUSIONS

The two evaluated sequences represent a relatively small risk to Unit 1 in that they constitute less than 1% of the core melt risk from the entire spectrum of LOCAs.