UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

Enclosure

SAFETY EVALUATION
SINGLE FAILURE ANALYSIS FOR RPS AND ESF
SAN ONOFRE, UNIT 1
DOCKET NO. 50-206

1.0 BACKGROUND

The failure of pressure transmitter PT-459 resulted in a fluctuation in the steam flow signals to the Main Feedwater Control System causing a reduction of feedwater flow and automatic initiation of both trains of Auxiliary Feedwater. The subsequent review of this failure and the resulting consequences identified a single failure deficiency in the design of the Steam/Feedwater Flow Mismatch Reactor Trip System. This single failure susceptibility impacted the safety analysis for the loss of the Main Feedwater and the Main Feedline Break transients since credit is taken for this trip in these two events. The licensee provided a revised safety analysis for the Loss of Main Feedwater and Main Feedline Break transients without credit for the mismatch trip. The NRC approved the revised safety analyses in Safety Evaluations dated April 7 and July 16, 1987. In addition, the NRC staff's review of the pressure transmitter failure and resultant inoperability of the mismatch trip concluded that the design of the mismatch trip does not conform with applicable San Onofre Unit 1 design basis in regard to the single failure criterion and control/protection system interaction. As a result of this design deficiency, the NRC, by letter dated September 23, 1986, requested that SCE perform a review of the Reactor Protection System (RPS) and Engineered Safety Features (ESF) for conformance to the applicable design basis.

SCE submitted the RPS Single Failure Analysis by letter dated March 11, 1987. The analysis concluded that the RPS is in compliance with the design bases except for the mismatch trip. The mismatch trip design was found to have additional deficiencies other than the common pressure transmitter PT-459 discussed above. These additional design deficiencies involve the channel-common signal path and power supply configurations of the steam and feedwater flow analog amplifier design and the one channel of input per loop to the RPS for single reactor coolant loop-specific events. SCE committed to resolve the deficiencies along with the Auxiliary Feedwater System upgrade planned for the Cycle 10 refueling outage.

SCE submitted the ESF single failure analysis by letter dated November 6, 1987. The analyses reviewed the existing ESF systems not analyzed in the 1976 Emergency Core Cooling System (ECCS) Single Failure Analyses including modifications to ECCS, and the proposed AFW system configuration. The study concluded the Containment Isolation System (CIS), Overpressure Mitigation System (OMS) and Proposed AFW system configurations meet the applicable single failure criterion.

By Licensee Event Report (LER) No. 87-015, Revision 1, dated May 17, 1988, SCE identified an additional single failure susceptibility. This susceptibility involved the spurious closure of MOV-883 which would result in isolation of the

suction path from the refueling water storage tank to the containment spray system. The licensee implemented immediate measures to assure availability of the suction path to containment spray system and committed to implement a modification to eliminate this single failure susceptibility.

2.0 DISCUSSION

2.1 RPS Single Failure Analysis

The RPS single Failure Analysis was performed to determine conformance of the RPS with the applicable design basis criteria related to the single failure criterion and control/protection system interactions. The analysis was performed in accordance with the applicable definitions and criteria of IEEE Standard 279-1971.

The licensee performed a module-level failure mode and effects analysis of each scram function. This analysis evaluated single failure susceptibility from the input devices through the reactor trip mechanism. Portions common to more than one scram function were also evaluated including power supplies and the scram matrix and breakers. Multiple-failure scenarios for control/protection systems interactions were also analyzed.

In addition, the licensee reviewed the acceptability of spatial (number of channels per RCS loop or steam generator) distribution of inputs to the RPS for loop-specific events not covered by the control/protection system interaction evaluation.

The RPS study concluded that the RPS meets the appropriate design basis except for the Steam/Feedwater Flow Mismatch Trip. This mismatch trip was found to have additional design deficiencies beyond the common pressure transmitter PT-459. The deficiencies result from the steam and feedwater flow analog amplifier design which was found to have single failure susceptibilities due to a channel-common signal path and power supply configurations. The review of the spatial distribution of inputs identified design deficiencies related to single steam generator loss of feedwater flow and certain main feedwater break scenarios. SCE committed to resolve these signal failure susceptibilities of the RPS in conjunction with the AFW system upgrade scheduled for the Cycle 10 refueling outage.

2.2 ESF Single Failures Analysis

The ESF Single Failure Analysis evaluated those systems (or portions of) which are required to mitigate a Loss of Coolant Accident (LOCA) or secondary system failure for single failure susceptibility. A previous single failure analysis of the systems required to mitigate a postulated LOCA with or without offsite power available was submitted by letter dated December 21, 1976. This 1976 analysis evaluated Safety Injection, Containment Spray, Recirculation, Component Cooling Water, Salt Water Cooling and Auxiliary Power systems including Safety

Injection Actuation system. However, this analysis did not evaluate the single failure susceptibility of the containment isolation or main feedwater isolation functions associated with ECCS operations during a LOCA or secondary system failure. Therefore, the recent ESF Single Failure Analysis scope was limited to systems not previously reviewed plus a review of the previous ECCS analysis against resulting plant changes to verify that an acceptable plant configuration has been maintained.

Additionally, as a result of the Main Feedwater Isolation event-specific analysis discussed below, a previously unrecognized potential single failure susceptibility was identified for ECCS ESF functions which rely on the swing 480V Bus No. 3. Therefore, an event-specific, time-dependent (sequence) single failure analysis was performed. This analysis evaluated the SIS and the SISLOP electrical alignment of the 480V Bus No. 3 and the realignment dependency on the 125 V dc system.

The containment isolation ESF function during a LOCA was also evaluated. The module-level failure mode and effects analysis evaluated single failure susceptibility from the input instrumentation through the final actuated devices, including vital and regulated Bus/DC system dependencies. Credit was taken for isolation value configurations which were previously reviewed and found acceptable as part of Systematic Evaluation Program Topic VI-4.

The ESF study included a module-level failure mode and effects analysis of the main feedwater isolation ESF function during a main steam line break. The analysis evaluated single failure susceptibility from the sequencer output through the final actuated devices, including vital and regulated Bus/DC system dependencies, 4kV pump trips, valve position changes and auxiliary power system dependencies. In addition, an event-specific single failure response evaluation of the main feedwater isolation function was performed. This analysis explicitly accounts for the location of an initiating fault, the availability or loss of offsite power, intersystem dependencies and common cause effects, as applicable. The event-specific analyses were prepared based on the module-level failure mode and effects analysis results.

The Overpressure Mitigation System ESF function was also reviewed to determine single failure susceptibility in response to RCS overpressure challenges during reactor shutdown conditions. This module-level failure mode and effects analysis was performed similarly to the module-level analysis for containment isolation as discussed above.

The existing Auxiliary Feedwater System was previously evaluated both in response to the TMI Action plan and the Systematic Evaluation Program (SEP). Several single failure susceptibilities were identified and SCE committed to upgrade the system during the Cycle 10 refueling outage. Therefore, SCE evaluated the proposed upgrade system configuration as part of the current ESF single failure analysis effort. This analysis also accounted for the implementation of the currently proposed Cycle 10 modifications to the steam/feedwater flow mismatch which resolved the previously identified single failure design deficiencies.

The ESF single failure analysis utilized the same criteria as the RPS study. Specifically IEEE Standard 279-1971, 4.2 and 4.7 were applied. The ESF analysis results identified single failure susceptibilities which could result in failure scenarios outside the San Onofre Unit 1 design bases.

The ECCS evaluation confirmed that the single failure susceptibilities identified in the 1976 analysis have been corrected. However, the evaluation identified new susceptibilities associated with the safety injection realignment valves HV-852A or B and with the swing 480V Bus No. 3. The failure susceptibilities associated with the realignment valves are discussed below under the Main Feedwater Isolation discussion (Sectin 3.3.2 of this SE). The 480V Bus No. 3 susceptibilities involve single failure of either DC train, or of Train A (AC power), concurrent with SIS or SISLOP. The failure scenarios could result in concurrent loss of the 480V Bus No. 3 and redundant Train A or Train B loads. Dependent upon the failure timing and charging system alignment, the failure could cause failure of the charging suction valves, the charging pumps or recirculation discharge valves resulting in loss of recirculation flow.

The containment isolation evaluation concluded that no single failure susceptibilities in the actuation system exist and that the isolation valve configurations are acceptable based on the San Onofre Unit 1 SEP criteria.

The evaluation of the Main Feedwater Isolation function identified common-cause and single failure susceptibilities which could result in continued feedwater addition or diversion of both trains of safety injection flow to the steam generators.

The evaluation of the Overpressure Mitigation System (OMS) ESF functions included an analysis of the OMS instrumentation as well as the pressurizer power operated relief valves and associated block valves. No single failure susceptibilities were identified. However, a potential failure for the dedicated shutdown control transfer switches for one train of PORV/block valve was discovered. As corrective action, the 120 V AC circuit breakers for the associated pneumatic control transfer solenoid valves will be maintained open by administrative control.

The proposed modifications to the Auxiliary Feedwater System (AFWS) and steam/feedwater flow mismatch were conceptually developed based on scoping studies which included hydraulic calculations and the event-specific single failure response analysis for the integrated RPS/AFW systems. The resulting design will ensure an acceptable RPS scram response for the available AFW flow into the intact feedwater lines for any applicable design basis event with or without concurrent loss of offsite power and a single active failure. Operator actions, when required (e.g., to equalize flow), are no longer needed outside the control room. In addition, water-hammer limits are precluded from being exceeded by design (hydraulic resistances and interlocks) rather than by operator action as in the existing configuration.

2.3 LER No 87-015, Revision 1

By Licensee Event Report (LER) No. 87-015 Revision 1, dated May 17, 1988, SCE identified a single failure susceptibility of the containment spray system. This susceptibility involves inadvertent closure of MOV-883 which would result in isolation of the suction path from the refueling water storage tank to the containment spray system. This susceptibility was discovered during SCE's recent review of the environmental qualification requirements for 480V MCC-3 located in the south end of the turbine building. The failure of this valve was previously identified in the 1976 Emergency Core Cooling System Single Failure Analysis and a modification to lock out control power was implemented. As a result of the recent evaluation, SCE identified a new failure mechanism which involved spurious closure of the motor controller contacts. Since motive powers to the valve is not locked out, this new failure mechanism could result in the inadvertent closing of the valve.

3.0 MODIFICATIONS

SCE provided design descriptions for the modifications to resolve the single failure susceptibilities by letters dated November 20, 1987 and April 5, June 21, and August 31, 1988.

3.1 Steam/Feedwater Mismatch Reactor Trip

(1) The current mismatch trip logic will be revised to provide a trip signal to the reactor trip circuit, two out of three reactor trip logic, for a high steam/feedwater flow mismatch as well as the original low flow mismatch. This modification is provided to resolve the design deficiencies associated with the number of channels provided per loop for single reactor coolant loop specific events. The current design would not provide a trip signal for a main feedwater line break downstream of the feed flow element, in which the steam generators remain pressurized. The affected loop would indicate high feedwater flow but the mismatch logic requires feed flow to be less than steam flow by 25% of the full power value, so that a trip signal would not be generated for this loop. If a single failure were to prevent the trip in one of the two unaffected loops, the two out of three loop trip logic would not be achieved and a reactor trip would not be generated by the mismatch logic. Without the early trip provided by the mismatch logic, acceptable transient results for this feedwater line break event would not be achieved. Therefore, to achieve acceptable transient results with the upgraded AFW system, the mismatch logic will be modified to also provide a trip signal when feedwater flow exceeds steam flow by a preset value. The mismatch would then generate a reactor trip for a main feedwater line break downstream of the flow element. The affect loop would generate a trip signal on high feedwater flow and the two unaffected loops would generate a trip signal on high steam flow.

(2) The pressurizer level trip will be retained at the 50% setpoint and a P-8 permissive will be added to the steam/feedwater flow mismatch

trip. This permissive will disarm the trip below 50% power. These features are provided to achieve acceptable transient results and reduce the possibility of spurious reactor trips. The mismatch cannot generate a trip signal for a single steam generator loss of feedwater event; although the affected loop would generate a trip signal, the automatic main feedwater control system would adjust flow to the two unaffected loops and hence prevent them from reaching a trip condition. Therefore, the high pressurizer level trip at the 50% setpoint will be retained in the modified RPS to provide a reactor trip early enough so that the upgraded AFW system response will be adequate. The P-8 permissive in the mismatch logic is provided in response to the plant trip reduction program. Since the steam and feedwater flows tend to fluctuate during startup and shutdown operations, the P-8 permissive will reduce the possibility of a spurious mismatch trip. The high pressurizer level with 50% setpoint or the current high pressurizer pressure reactor trips would provide protection when the mismatch is bypassed.

(3) A minimum floor value will be provided for the main steam header pressure signal in each of the channelized steam flow calculator modules. This feature will eliminate the potential for loss or spurious initiation of the mismatch trip due to a downscale failure of the common pressure transmitter PT-459.

(4) The power supplies and signal paths for each steam/feedwater flow mismatch instrument loop will be channelized. Additionally, isolation will be provided between the PT-459 instrument loop and each steam/feedwater flow mismatch channel and its associated feedwater control loop. These features will prevent loss of more than one channel of the mismatch trip due to a postulated single failure of power supplies, signal paths, PT-459 instrument loop or non-qualified control loop.

3.2 Recirculation System

(1) The power supply for charging pump suction valve MOV-1100D will be changed from the swing 480V Bus No. 3/MCC-3 to 480V Bus No. 2/MCC-2 (Train B). This modification will ensure that the power supply for charging pump suction valve MOV-1100D is electrically independent from the redundant charging pump suction value MOV-1100B which is powered from 480V Bus No. 1/MCC-1 (Train A) thereby preventing a single failure from disabling the power supplies for both valves.

(2) The power supply for recirculation valve MOV-358 will be changed from swing 480V Bus No. 3/MCC-3 to an Uninterruptible Power Supply (UPS). This modification will ensure that the power supply for recirculation valve MOV-358 is electrically independent from the two redundant recirculation valves MOV-356 (Train A) and MOV-357 (Train B) thereby preventing a single failure from disabling the power supply for more than one valve.

This modification will ensure that operation of MOV-358 from the control room is possible for at least 30 minutes after a postulated loss of offsite power. Should operation of MOV-358 be required after 30 minutes, operator action would be required to restore power to 480V Bus No. 3/MCC-3 which can be manually cross-tied to the UPS bus. This operator action would entail cross-tying 480V Bus No. 3 to 480V No. 1 or 2. Should a single failure disable a DC power train, manual operator action may be required to open the feeder breaker to 480V Bus No. 3 thereby satisfying the necessary interlocks to permit cross-tying. The feeder breaker is located in the 480V Room at the northwest corner of the Turbine building. The acceptability of the necessary operator action outside the control room has been evaluated and found acceptable as discussed below.

The delayed opening of MOV-358 beyond 30 minutes would be indicative of a small break LOCA (SBLOCA) in the size range of 2.5 inches or less. The radiological consequences resulting from the SBLOCA discussed above have been analyzed in Section 13.2 of the Final Safety Analysis, concluded that the operator actions to restore power to the 480V Bus No. 3 following a LOCA, in accordance with existing procedures, can be performed without unacceptable dose consequences to the operators. These actions are not required for breaks larger than 2.5 inches, which have the highest risk for unacceptable dose consequences, since MOV-358 would be opened within 30 minutes. The addition of recirculation valve MOV-358 to the UPS for safety injection valve MOV-850C also involves a change to the current UPS design basis and the associated San Onofre Unit 1 technical specifications. The basis for the acceptability of this change was provided in Enclosure 1 of the June 21, 1988 submittal.

3.3 Main Feedwater System

The following actions were required:

(1) Replace the solenoid valves for the main feedwater pneumatic control valves (FCV-456, 457 and 458) and their respective bypass valves (CV-141, 142 and 143), and the motor actuators and valves for main feedwater isolation valves (MOV-20, 21 and 22) with environmentally qualified replacements. This will eliminate the possibility of valve failure due to the environmental consequences of a steam line break or feedwater line break outside containment.

(2) Ensure that the actuators for the main feedwater control valves, bypass valves and isolation valves will close the valves in sufficient time to meet the transient analysis requirements. This modification will assure that any additional water mass provided to the steam generators for a steam line break inside containment does not challenge the containment pressure limits.

(3) Provide a redundant solenoid valve for each pneumatically operated bypass valve, which is powered and sequenced from the opposite train. This will ensure that a single failure of an electrical train or sequencer will not result in continued mass addition to the steam generators through the bypass lines.

(4) Provide nitrogen backup to the main feedwater control valves to eliminate the possibility of failure to close due to loss of the instrument air system.

(5) Change the power supply for main feedwater control valves FCV-457 and FCV-458 and respective bypass valves CV-144 and CV-143 to Train 2 to match the sequencer assignment. This will eliminate the potential for valve failure due to reliance on two independent electrical systems.

(6) Change motive and control power for main feedwater isolation valve MOV-22 from swing 480V Bus No. 3/MCC-3 to 480V Bus No. 1/MCC-1. The 480 V Bus No. 1 and associated MCCs are located in the area outside of the harsh environment for a main steam line break outside containment. Additionally, this modification eliminates the potential for valve failure due to reliance on two independent electrical systems.

3.4 Auxiliary Feedwater System Upgrade

The auxiliary feedwater system, once upgraded, will consist of two redundant, electrically independent trains which meet the single failure criteria. Train A will consist of existing motor driven pump G-10S, turbine driven pump G-10 and all respective valves and interlocks. The redundant Train B will consist of the new motor driven pump G-10W and respective valves and interlocks. The auxiliary feedwater system configuration will involve a lead/lag train arrangement with Train B (G-10W) as the lead pump. System flow limitations for water hammer and G-10S runout will be achieved by using passive mechanical means. The required modifications to achieve this system configuration are discussed in detail below:

(1) Two new AFW flow control valves will be added so that the upgraded system configuration has two flow control valves per AFW line. The parallel valves on each line will be on separate electrical trains. The valves on Train B will open upon loss of control power. This failure mode was selected because if Train B power fails, no credit for flow equalization between the AFW lines is taken for Train A, inasmuch as the flow indication on each line is Train B powered. The combined flow from the Train A pumps (G-10 and G10S) can meet the required flow for all conditions with the flow control valve wide open. Conversely, the Train A valves will fail closed upon loss of control power, so that the Train B pump (G-10W) can meet the flow requirements for all conditions with credit for flow equalization between the AFW lines.

(2) A cavitating venturi will be installed in each AFW line downstream of the flow control valves so that water hammer limits and Train A driven pump (G-10S) runout flow restrictions will be achieved for all conditions. An additional venturi will be installed in the discharge of the Train B pump (G-10W) so as to prevent exceeding the maximum flow limits to each steam generator for all conditions.

(3) The low discharge pressure trip for the motor driven Train A pump (G-10S) will be removed. This trip function does not currently meet single failure criteria. Pump runout will be prevented by passive mechanical means (cavitating venturis).

(4) The control room AFW panel will be modified to include the same controls, indications and alarms for the Train B pump (G-10W) as provided for the motor driven Train A pump (G-10S). In addition, since the Train B pump is credited for post-fire dedicated safe shutdown, a manual transfer switch will be provided outside the control room. This transfer switch will provide isolation between the normal Train B and the dedicated shutdown system power supply.

(5) The AFW auto initiation system and auto-mode control circuit of each pump and associated discharge valve will be modified to function as described below:

(a) Upon receipt of low steam generator level (either Train A or B), an AFWS auto initiation signal will be generated to the respective pump train.

(b) Upon AFWS auto initiation, the lead Train B pump (G-10W) will immediately start and provide flow. The turbine driven Train A pump (G-10) will begin turbine warm-up, if steam is available.

(c) After a set time delay, to allow the Train B pump to respond, the lag Train A pumps (both G-10 and G-10S) will begin to provide flow upon a low flow signal from the Train B pump discharge manifold. To prevent automatic operation of both pumping trains concurrently, separate flow switches will be interlocked with the Train A pumps and with the Train A pump discharge valves. Low flow signals from the Train B pump discharge manifold will be required to auto start the Train A pumps and open their discharge valves. The separate flow switches will prevent a signal failure from resulting in concurrent automatic initiation of both pumping trains.

(d) To assist the pumps in developing discharge pressure, an interlock between each AFW pump and respective discharge valve will be provided. The interlock will require pump discharge pressure in order to open the discharge valve in automatic mode.

(e) Instrument air and back-up nitrogen for the Train B pump discharge valve will be provided. The nitrogen back-up will ensure the capability to operate the control valve in the event instrument air is lost.

3.5 Containment Spray System

A second starter in series with the existing valve closing circuitry of RWST Isolation Valve MOV-883 will be added. This change will prevent a single failure of the existing motor controller contacts from providing motive power to cause inadvertent closure of MOV-883.

5.0 CONCLUSION

The RPS study concluded that the RPS meets the appropriate design basis except for the steam/feedwater flow mismatch trip. The mismatch trip was found to have additional design deficiencies beyond the common pressure transmitter P-459 single failure concern. The licensee modified systems to resolve the single failure susceptibilities of the RPS in conjunction with the AFW system upgrade. These modifications have resolved the single failure susceptibilities of the RPS that have been identified in these submittals and are, therefore, acceptable.

The ESF analysis results identified single failure susceptibilities associated with the safety injection realignment valves and with the swing Bus No. 3. The evaluation of the Main Feedwater Isolation function identified common-cause and single failure susceptibilities which could result in continued feedwater addition or diversion of both trains of safety injection flow to the steam generator. Modifications to the Auxiliary Feedwater System (AFWS) and steam/feedwater flow mismatch were proposed based on scoping studies which included hydraulic calculations and the event-specific single failure analysis for the integrated RPS/AFW systems. The proposed modifications to the ESF systems resolve the single failure susceptibilities of the ESF systems that have been identified and therefore are acceptable.

By LER No. 87-015 Revision 1, the licensee identified a single failure susceptibility of the containment spray system. This susceptibility involves inadvertent closure of MOV-883 which would result in isolation of the suction path from the refueling water storage tank to the containment spray system. The licensee provided a description of the modification that resolves the single failure susceptibilities concern. Based on our review, we conclude that the modifications are acceptable.

Principal Contributor:
S. Rhow, ICSB

Date: April 28, 1989