NUCLEAR SAFETY GROUP

PROBABILISTIC RISK ASSESSMENT REPORT

# PROBABILISTIC RISK ASSESSMENT

of

LER 2-96-012 based on AR 960201089
(Spurious operation of valves, controllers, and/or pumps due to seismic or raceway interactions could result in diversion of safe shutdown condensate from CST T-120)

May 6, 1998

REPORT NSG-98-013


Prepared by: P. Moieni
(P. Moieni)

Reviewed by: M. P. Carr
(M. P. Carr)

Reviewed by: [signature]
(D. Henneke)

Approved by: T G Hook
(T. G. Hook)

**PROBABILISTIC RISK ASSESSMENT**
**LER 2-96-012 based on AR 960201089**
**(Spurious operation of valves, controllers, and/or pumps due to seismic or raceway interactions could result in diversion of safe shutdown condensate from CST T-120)**

## PURPOSE

The purpose of this study is to determine the increase in core damage frequency as a result of CST T-120 flow diversion during seismic or HELB events inside the turbine building.

## BACKGROUND

The Condensate Storage Tank (CST) T-120 has branch connections to non safety-related makeup (e.g., condenser makeup, Blowdown Process System (BPS) sluice water, condensate makeup pump P049) in addition to its safety-related makeup connection to CST T-121. Non-1E controlled process devices in these branch connections could spuriously actuate, diverting inventory from T-120, as a result of control relay failures or raceway circuit interactions ("toaster wire" failures) following a seismic event or high energy line break (HELB) in the turbine building (AR 980201089, Operability Assessment). The seismic event or HELB could also cause failure of piping systems (near the high energy lines) that result in diversion of water from T-120. Normal makeup to T-120, from the HFMUD system, may also be unavailable following these events. The Technical Specification level for T-120 (i.e., 280,000 gallons) does not include an allowance for these newly identified inventory diversions.

An administrative level of 382,000 gallons level (equivalent to 86.2%) for T-120 allows 30 minutes of diversion at an assumed rate of 6,000 gpm before reaching to the required 200,000 gallons of water for 24 hours of AFW supply before Shutdown Cooling (SDC) System is initiated (AR 980201089, Operability Assessment; NCR 980201089). A low level alarm at 86.2% will warn the operators in the control room of CST T-120 level reaching the administrative level of 382,000 gallons. The operators, then have 30 minutes to isolate the T-120 diversion by locally closing manual valves S2(3)1414MU092 and 2(3)HV-5715 using SO23-13-3 and SO23-9-5 procedures.

According to DBD-SO23-780, CST T-121 has sufficient storage capacity (i.e., 144,000 gallons) to maintain the plant in a hot standby condition for 2 hours, and the additional water needed to remove decay heat and stored heat to cool down the reactor to a temperature where the SDC System can be used. The T-120 required volume of 200,000 gallons, combined with T-121 of 144,000 gallons, allows 24 hours of AFW supply before SDC initiation conditions are reached. Based on 24 hours water supply available from T-120 and T-121, the San Onofre Living PRA does not require success of or credit the SDC function. Furthermore, the water supply from T-120 is only needed about 8 hours after the initiating event based on the 144,000 gallons of water in T-121 (see Figure 1 in Attachment 9 of SO23-12-7). This is the time, when the SDC has to be initiated by the operators or water has to be supplied to T-121 from T-120 by opening manual valve(s).

## METHODOLOGY

The CST T-120 has branch connections to non-safety related makeup such as condenser makeup and BPS sluice water, in addition to its safety-related makeup connection to CST T-121. Non-1E controlled process devices in these branch connections could spuriously actuate, diverting inventory from T-120, as a result of control relay failures or raceway circuit interactions ("toaster wire" failures) following a seismic event or high energy line break (HELB) in the turbine building. The seismic event or HELB could also cause failure of piping systems (near the high energy lines) that result in diversion of water from T-120. A potential flow diversion scenario is the seismic-induced failure of the two 8 inch lines from CST T-120 through condensate transfer pump and main condenser makeup (Seismic Category II pipes). It is noted that the flow diversion from these lines can be isolated by operators by closing manual valves MU-092 and HV-5715.

The potential flow diversion from CST T-120 during seismic or HELB events would cause a reduction in the water supply for the AFW system beyond the 8 hours inventory provided by CST T-121. As a result, the operators are expected to realize the reduced capacity of the condensate water and to initiate the RCS cooldown and shutdown cooling in a timely manner following the Emergency Operating Instructions (EOIs).

The increase in core damage frequency as a result of CST T-120 flow diversion during seismic or HELB events inside the turbine building was evaluated using the San Onofre Living PRA model contained in the Safety Monitor. The models for seismic event and main steam line break (SLB) event (representing HELB in the turbine building) were modified to include the following three operator actions as well as the fault tree for the SDC System:

1. Operator failure to isolate CST T-120 flow diversion by locally closing valves S2(3)1414MU092 and 2(3)HV-5715 (OP1).

2. Operator failure to initiate RCS cooldown in time to get to the SDC conditions given CST T-120 flow isolation failure (OP2).

3. Operator failure to initiate SDC in a timely manner given RCS cooldown is successful (OP3).

It is noted that OP3 here is different from the normal SDC initiation action with 24 hours of CST inventory available, because operators have less time available to perform the action in this case.

To simplify the calculations, the following expression was used to calculate the core damage frequency (CDF) resulting from CST T-120 flow diversion during seismic or HELB events in the turbine building (later, if needed, Safety Monitor will be used to assess the risk in a more detailed fashion):

$$CDF_i = f_i * OP1 * (OP2 + OP3 + SDC), \quad i = \text{Seismic event, SLB event}$$

Where $f_i$ represents the initiating event frequency and SDC represents the hardware failure probability of the Shutdown Cooling System.

## ANALYSIS

The seismic initiating event frequency for the postulated pipe break scenario is estimated to be 7.6E-3/yr (see Assumptions 1-3). The SLB frequency is 5.4E-4/yr (Ref. IPE). The SDC system hardware failure probability is estimated to be 1.3E-4 (see Assumption 4). The three operator actions (i.e., OP1, OP2, and OP3) are proceduralized and are stated in several EOIs (SO23-12-1, SO23-12-3, SO23-12-7, SO23-5-1.5). The following scenario is postulated (Ref. Ted Vogt's E-Mail, 4/22/98):

Time: 0 — Major earthquake occurs, switchyard is lost and unit trips.

1 — SO23-12-1 Standard post trip actions started. SO23-13-3 Natural disaster/severe weather procedure entered.

11 — Standard post trip actions completed up to the diagnosis. Crew diagnoses a LOFC/LOOP and enters SO23-12-7.

15 — Common operator dispatches field operators to perform post seismic inspections per SO23-13-3 Attachment #2.

20 — Condensate tank low level alarm annunciates, operators review ARP and report critical alarm to the control room supervisor.

21 — Control room supervisor reaches step twelve in SO23-12-7 to check condensate inventory. From the condensate tank low level alarm and the procedures requirement to check inventory the control room supervisor dispatches an operator to check for tank leakage.

25 — Control room supervisor directs RO's to initiate Attachment# 3 cooldown and depressurize the RCS.

30 — The eight inch condensate line is isolated (by closing MU-092 and HV-5715) by either the operator performing post seismic checks or the operator dispatched by the control room supervisor due to loss of condensate tank inventory (OP1).

30 — Reactor Operators starts RCS cooldown (OP2).

With respect to the ability of T-120 to cooldown the plant following a seismic event with loss of offsite power, per CE calculation S PEC 221 and assuming that shut down cooling entry conditions can be made at a $T_{hot}$ of 400 degrees the CE calculation conservatively shows that this can be accomplished with 1 ADV in approximately 5 hours if the cooldown can start at 45 minutes. When system valve leakages and steam generator shrinkage are factored in, the T.S.

volume of 144,000 gallons would still be sufficient (Ref. David Brahms's E-Mail, 4/22/98).

If 2 ADVs were available the cooldown could proceed at 75 degrees per hour and assuming the cooldown begins at 1 hour could be accomplished in 3.75 hours with less than 115,000 gallons of water in T-121. This is based on entering $T_{hot}$ at 400 degrees. NOTE: The calculations are based on cooling down to a $T_{cold}$ of 352 with a steam generator delta T of 30 degrees and an 18 degree margin for instrument error (Ref. David Brahms's E-Mail, 4/22/98).

Based on the above statements, the time available for the CR operators to initiate RCS cooldown (i.e., OP2) is calculated herein. Figure 1 in Attachment 9 of EOI SO23-12-7 (LOFC/LOP) indicates that with 144,000 gallons of water available (from CST T-121), the time available before SDC is required is 8 hours. Subtracting 5 hours required for RCS cooldown (with 1 ADV) from the 8 hours to SDC, leaves 3 hours of "maximum time available" for operators before they initiate RCS cooldown and still be able to safely initiate SDC. Assuming 200 gpm of water feeding each SG from CST T-121 for 3 hours consumes 72,000 gallons of water from CST T-121, and leaves 72,000 gallons for RCS cooldown. Figure 1 in Attachment 9 of EOI SO23-12-7 indicates a 5 hour time period available before SDC is required with 72,000 gallons water available from CST T-121. This is consistent with the 5 hour cooldown period stated above and supports the statement that the 144,000 gallon in CST-121 is sufficient for reaching SDC as long as the operators initiate the RCS cooldown within 3 hours of the seismic event (with 1 ADV).

When 2 ADVs are available, the operators have about 4.25 hours (i.e., 8 - 3.75 = 4.25 hours) to initiate RCS cooldown, and proceed with RCS cooldown for another 3.75 hours until they reach SDC conditions. The case with 1 ADV available is selected here for analysis, because it is more limiting with respect to the time available for operator action OP2. However, this is not a significant conservatism.

The three operator actions were quantified using the human reliability analysis methodology and database documented in NUREG/CR-4772 (Ref. 1) and NUREG/CR-1278 (Ref. 2). The results of the human reliability analysis with the supporting assumptions are provided in Table 1.

## ASSUMPTIONS

The following assumptions were made in this risk assessment:

1. A worst case flow diversion of 6,000 gpm is assumed based on a full guillotine break of the two 8 inch lines from CST T-120 through condensate transfer pump and main condenser makeup (Ref. NCR-960201089).

2. The CST T-120 flow diversions from the two 8 inch lines are isolatable by operators (the pipes between CST T-120 and manual valves MU-092 and HV-5715 are Seismic Category I pipes).

3. The mean failure frequency of the two 8 inch lines from CST T-120 is estimated to be 7.6E-3/yr (for a median seismic capacity of 0.4g, $\beta_R = 0.4$, and $\beta_U = 0.4$ ) given a seismic

event in the range of 0.25g to 8g occurs (Ref. IPEEE; AR-960201089, Seismic Fragilities Assessment).

4. The shutdown cooling system hardware (pumps, valves, heat exchangers, pipes) will survive the seismic events postulated in IPEEE (Ref. IPEEE). The MOVs HV-8150, 8151, 8152, and 8153 relays were not reviewed in IPEEE as part of fragility analysis, however, these MOVs are locked closed with power removed. Therefore, only random failure probabilities are considered for SDC system failure. A SDC system unavailability of 1.3E-4 was used based on the system fault tree analysis.

5. It is assumed that the CST T-120 level is normally slightly above the new administrative level of 382,000 gallons.

6. The low level alarm for CST T-120 is at 382,000 gallons (or 86.2%) (Ref. AR-960201089, Operability Assessment).

7. The average time taken by the operators to isolate the CST T-120 flow diversion would be 10 minutes (Ref. Ted Vogt's E-Mail, 4/22/98).

8. The high energy line break (HELB) events in the turbine building causing flow diversion from CST T-120 are included in the steam line break (SLB) events modeled in the San Onofre Living PRA.

9. Conservatively, no credit is given to recovery of SDC system from hardware failures when the recovery time available is less than 2 hours. Some of the component failures such as MOVs and breakers fail to open can be recovered by the operators within 2 hours.

10. The time window for the operator action to initiate SDC (i.e., OP3) is assumed to be 2 hours. In other words, the time to core uncovery from the SDC conditions (at or before 8 hours after the seismic event and reactor trip) given the SDC system fails is assumed to be 2 hours.

11. There are other non-seismic sources of water to CST T-121 that may not be damaged by an earthquake. Examples of such sources are: 1) the three Demineralized Water Storage Tanks T-266, T-267, and T-268 (Hill Tanks) that provide manual or automatic filling of CST T-121 and T-120, 2) condensate flow from the Condenser by opening manual valve MU-476, and 3) fire water by opening manual valves MU-474 or MU-475 (Ref. DBD-SO23-780). No credit is given to these sources of water to CST T-121.

## RESULTS

The following results are obtained using the human error probabilities (HEPs) in Table 1 and the assumptions made above.

Seismic Event

CDF = 7.6E-3/yr * 0.1 * (3.0E-4 + 1.5E-4 + 1.3E-4) = 4.4E-7/yr

SLB Event

Similarly, the CDF for the SLB event is calculated as follows using the HEPs from Table 1 (conservatively, the seismic PSFs were not removed).

CDF = 5.4E-4/yr * 0.1 * (3.0E-4 + 1.5E-4 + 1.3E-4) = 3.1E-8/yr

Total CDF

The total CDF is calculated as follows:

CDF = CDF (seismic) + CDF (SLB) = 4.7E-7/yr

It is noted that the above CDF estimate does not include the potential recovery of certain SDC system hardware failures such as MOVs and breakers fail to open (see Assumption 9). Operating experience shows that such failures can be recovered by the operators within 1 to 2 hours following the system failure. NSAC/161 (Ref. 3, Figure 3.1-1) provides non-recovery probabilities of 0.2 at 1 hour and 0.15 at 2 hours for PWR RHR system. The dominant accident sequence cutsets generated by the Safety Monitor can be examined to identify those cutsets for which SDC system recovery are applicable.

No uncertainty analysis is performed because the analysis is conservative and the results are believed to represent an upper bound. Removing some of the conservatism (e.g., Assumptions 1, 5, 9, 10) will further reduce the CDF estimated above.

REFERENCES

1. Swain, A., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure", NUREG/CR-4772, February 1987.

2. Swain, A. and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, August 1983.

3. Booth, H. R., et. al., "Faulted Systems Recovery Experience", NSAC-161, May 1992.

4. SONGS Unit 2 and 3 Individual Plant Examination (IPE), Cycle 9 Updated Models, April 1997.

5. SONGS Unit 2 and 3 Individual Plant Examination for External Events (IPEEE), Cycle 9 Updated Models, April 1997.

6. SONGS Unit 2 and 3 Action Request (AR) # 960201089, Operability Assessment.

7. SONGS Units 2 and 3 Non Conformance Report (NCR) # 960201089, Disposition Item 05.

8. SONGS Unit 2 and 3 AFWS Design Basis Document, DBD-SO23-780, Rev. 3.

9. SONGS Units 2 and 3 Loss of Forced Circulation/Loss of Offsite Power Emergency Operating Instructions, SO23-12-7.

10. E-Mail from Ted Vogt to Tom Hook: T120 Inventory Loss due to Earthquake (Timeline), 4/22/98.

11. E-Mail from David Brahms to Tom Hook: Comments on Ted Vogt's E-Mail on T120 Inventory Loss due to Earthquake (Timeline), 4/22/98.

12. SONGS Unit 2 and 3 Action Request (AR) # 960201089, Seismic Fragilities, 4/30/98.

## Table 1. Human Reliability Analysis (HRA) Summary

| Operator Action | Time to Core Damage ($T_W$) | Indication Time ($T_I$) | Time to Perform Action ($T_A$) | Time Available to Perform Diagnosis ($T_D$) (#) | Diagnosis Human Error Probability ($HEP_D$) (Figure 8-1, Ref. 1) | Post-Diagnosis Action Human Error Probability ($HEP_A$) (Ref. 2) | Total Human Error Probability [HEP = ($HEP_D$ + $HEP_A$) * (Seismic PSF)] |
|---|---|---|---|---|---|---|---|
| **Operator failure to isolate CST T-120 flow diversion (OP1)** | 30 minutes (##) | 1 minute (LL Level Alarm) | 10 minutes (+) | 30-1-10 = 19 minutes | 0.01 (Nominal Curve Used) (###) | 0.01 (HEP, Item 4, Table 20-7) x 0.005 (RF, Item 10, Table 20-22) x 2 (time stress PSF; Table 8-1, Ref. 1) x 2 (outside CR task PSF) = 2.0E-4 | (0.01 + 2.0E-4) x 10 (seismic PSF) = 0.1 (*) |
| **Operator failure to initiate RCS cooldown given CST T-120 flow isolation failure (OP2)** | 3 hours (++) | 30 minutes (time spent on CST-120 flow diversion isolation) | 10 minutes (time to perform actions in the control room) | 180-30-10 = 140 minutes | 5.0E-5 (Nominal Curve Used) | 0.01 (HEP, Item 4, Table 20-7) x 0.01 (RF, Item 4, Table 20-22) = 1.0E-4 | (5.0E-5 + 1.0E-4) x 2 (seismic PSF) = 3.0E-4 (**) |
| **Operator failure to initiate SDC given RCS cooldown is successful (OP3)** | 2 hours (+++) | Procedural steps (EOI SO23-12-7, steps 17 & 18) * (RCS $T_H$ and Pzr pressure) | 30 minutes | 120-30 = 90 minutes | Negligible (already included in the diagnosis error probability for OP2) | 0.003 (HEP, Item 2, Table 20-7) x 0.01 (RF, Item 4, Table 20-22) = 3.0E-5 | (3.0E-5) x 5 (seismic PSF) = 1.5E-4 (***) |

Notes:

# $T_D = T_W - T_I - T_A$

## This is the time available between the initial 382,000 gallons (new administrative level) in CST T-120 and the required 200,000 gallons for 24 hours AFWS water supply before SDC is required given a diversion flow rate of 6,000 gpm. The flow diversion rate is based on a full guillotine break of the two 8 inch lines from CST T-120 (Ref. NCR-960201089).

### Operator failure probability to miss the CST T-120 low level alarm in the CR is 1.0E-4 (if that is the only alarm received by the operators at a given time) (Ref. Table 8-4 in Ref. 1).

* A seismic PSF of 10 was assumed for a task outside the CR and time available between 20 minutes and 1 hour (Ref. IPEEE).

**Although the IPEEE study assumes a PSF of unity for a task inside the CR and time available between 1 hour and 24 hours (Ref. IPEEE), conservatively, a seismic PSF of 2 was assumed for this operator action.

*** A seismic PSF of 5 was assumed for a task outside the CR and time available between 1 hour and 24 hours (Ref. IPEEE).

+ The specific tasks with their times are: 1) isolate condenser flow by closing valve S2(3)1414MU092, and 2) isolate flow to both condensate storage transfer pumps P049 and the BPS Sluice pumps P431 and P461 by closing valve 2(3)HV5715) [$T_A$ = 10 min]. (Ref. Ted Vogt E-Mail, 4/22/98)

++ This is the time available based on 1 ADV available for RCS cooldown (see main text).

+++ The time window for the operator action to initiate SDC (i.e., OP3) is assumed to be 2 hours (Assumption 10).

LOSS OF FORCED CIRCULATION/LOSS OF OFFSITE POWER

DETERMINE TIME UNTIL SHUTDOWN COOLING REQUIRED

FIGURE 1 - REMAINING TIME S/Gs AVAILABLE AS HEAT SINK