

# Final Precursor Analysis

Accident Sequence Precursor Program – Office of Nuclear Regulatory Research

Calvert Cliffs 2	Excessive Steam Demand — Reactor Trip Due to Low Steam Generator Water Level After Feed Pump Trip		
Event Date 1/23/2004	LER 318/04-001-00; IR 05000317/2004008 and 05000318/2004008	CCDP =	$4.0 \times 10^{-6}$

June 1, 2006

## Event Summary

At 3:26 pm on January 23 2004, Calvert Cliffs Nuclear Power Plant (CCNPP) Unit 2 tripped from 100 percent power, initiated by the Reactor Protective System due to low steam generator water level caused by an erroneous overspeed trip signal on 22 Steam Generator Feed Pump (SGFP). The control room operator could not reset the SGFP, and the reactor was scrammed upon an automatic reactor trip signal.

The Turbine Bypass Valves (TBVs) and Atmospheric Dump Valves (ADVs) opened as designed, but the “quick open” signal did not clear due to the failure of a relay in the reactor regulating circuit. The open valves (turbine bypass and atmospheric dump) resulted in overcooling of the Reactor Coolant System (RCS) and also generation of a Safety Injection Actuation Signal (SIAS) and a Steam Generator Isolation Signal (SGIS).

About three minutes after the reactor trip, both Main Steam Isolation Valves (MSIVs) were shut upon receipt of an SGIS, isolating steam flow through the TBVs and thereby slowing the rate of RCS cooldown. Approximately six minutes later, the operations crew could take control of the ADVs through the Auxiliary Shutdown Panel, terminating the RCS overcooling and depressurization.

During the recovery, a large insurge of subcooled water caused by full charging with a relatively high RCS heatup, cooled the pressurizer, lowering the RCS pressure to produce a second SIAS.

The following summarizes the sequence of actions on January 23, 2004, leading to the event from Unit 2 operating at 100 percent power:

- 3:26 pm: 22 Steam Generator Feed Pump (SGFP) tripped on overspeed.
- The Reactor Operator (RO) attempted to reset 22 SGFP but failed to achieve normal operation (three attempts to reset the SGFP controls).

- 3:27 pm: The RO manually tripped the reactor when the conditions for Steam Generator (SG) level warranted and entered Post Trip Immediate Actions EOP-0 (subsequent analysis of the performance of the reactor protection system indicated that the reactor tripped automatically 1 second prior to the insertion of the manual trip signal).
- Upon reactor trip, the “quick open” signal<sup>1</sup> opened the TBVs and ADVs, but these valves were not closed due to the persistent signal as a result of the K7 relay failure.
- The open TBVs and ADVs caused an excessive steam demand<sup>2</sup> that rapidly overcooled the RCS and the Main Steam System.
- 3:28 pm: The SG levels were lowered and the Auxiliary Feedwater Actuation Signal (AFAS) caused 21 and 23 AFW Pumps to start.
- The RCS pressure decreased to SIAS setpoint which caused the signal to automatically start standby safety systems, including 2A & 2B Diesel Generators, 21 & 23 High Pressure Safety Injection (HPSI) Pumps, 21 & 22 Low Pressure Safety Injection (LPSI) Pumps, and 21 & 22 Containment Spray (CS) Pumps.
- The SIAS caused RCS letdown to be isolated, and the operating crew secured two reactor coolant pumps for procedure requirements for receipt of a SIAS signal.
- 3:29 pm: The SG pressure decreased to SGIS setpoint, causing both MSIVs to close automatically.
- 3:36 pm: The operating crew transferred control of the ADVs to the Auxiliary Shutdown Panel where the “quick open” signal was removed and the steam flow was subsequently throttled, thereby terminating the RCS overcooling and depressurization.
- The pressurizer level trended up due to post-trip decay heat, RCP heat input, and full charging pump operation with letdown isolated.
- A second SIAS signal was received during the recovery phase.

A more detailed chronology of the events can be found in Appendix A, and References 1 and 2.

**Cause.** The root causes of the Calvert Cliffs Unit 2 Reactor Trip and the associated failures or malfunctions are as follows [1, 2]:

- The trip of 22 SGFP was caused by degradation of voltage from the power source supplying the digital speed monitor which generated an erroneous trip signal to the SGFP controls trip circuit. The voltage degradation was caused by corrosion on the contact surfaces of the power supply fuse due to high humidity in the control cabinet. All fuses and fuse holders in the Units 1 and 2 SGFP control cabinets were replaced.
- The inability to reset and start 22 SGFP was determined to have resulted from a shift in the mechanical calibration of the Electric to Hydraulic (E/H) Converter. The specific cause of the shift has not been identified in Reference 1.

---

<sup>1</sup> The “quick open” signal is generated by the Reactor Regulating System and serves to momentarily fully open the TBVs and ADVs when the reactor trips, provided that the RCS average temperature ( $T_{ave}$ ) is greater than 557°F.

<sup>2</sup> Each of the four TBVs is sized to pass 10% of the steam flow for a total of 40%, and each of the two ADVs is sized to pass 2.5% of the steam flow for a total of 5%. Therefore, the excessive steam demand was equivalent to 45% of the steam flow.

- The failure to re-close the TBVs and the ADVs was caused by a normally open contact sticking closed in the K7 relay of the Reactor Regulating System (RRS). The root cause of this failure has been identified as an under-rated K7 relay (i.e., the K7 relay contacts are rated for 29 VDC, but were installed in a 125 VDC circuit).

**Recovery Opportunity.** If the operators had correctly diagnosed the cause of the excessive steam demand within a relatively short time (e.g., 10 to 30 minutes depending on the specific sequences, such as functioning of MSIVs or control rods) and switched to the alternate channel of the Reactor Regulating System (RRS) [2] after failure of the RRS Channel X, the ADVs and TBVs would have properly controlled reactor temperature and terminated the uncontrolled cooldown. However, it is believed that the cause (i.e., the under-rated condition of the K7 relay) could not have been easily diagnosed in such a short time and under a stressful situation. Furthermore, CCNPP did not have an off-normal procedure for failure of the RRS, and as a result, no credit is taken for the availability of the alternate channel.

**Condition Duration.** The K7 relay of the Reactor Regulating System successfully functioned when the reactor tripped on May 28, 2003. Based on licensee review, the K7 relay contacts would have failed to open on the next relay actuation, following the May reactor trip [1,2]. There were no other demands or tests which would have demonstrated whether the quick open function was operational from May 28, 2003, until the reactor trip on January 23, 2004, when the RRS relay failure was identified by a self revealing event. Therefore, the K7 relay was in failure condition for a period of 240 days (May 28, 2003 ~ January 23, 2004).

**Other concurrent or windowed events.** No other significant operating events existed at Calvert Cliffs 2 while the K-7 relay was inoperable according to the LER Search Database.

## Analysis Results

### • Importance

Two different types of analyses were performed to evaluate the impact of the inoperable K7 relay and the associated excess steam demand event on plant risk: a) initiating event assessment and b) condition assessment. The initiating event assessment was carried out using the event tree for loss of main feedwater (i.e., LOMFW)<sup>3</sup> with the failure of the K7 relay. This relay failure has negative impact on all the potential accident scenarios<sup>4</sup> including activation of the quick open signal for the TBVs and the SG ADVs; however, the K7 relay and the associated excessive steam demand are not included in the SPAR model for Calvert Cliffs [3]. Therefore, all the event trees other than those for irrelevant

---

<sup>3</sup> The LOMFW event tree was used in lieu of the general transient (i.e., TRANS) event tree, because the loss of 22 SGFP led to SG low level which necessitated a reactor trip. The failure of the K7 relay is not directly included in the revised SPAR model; however, a basic event for excessive steam demand which results from the relay failure has been included in the model to enable the assessment of the risk impact.

<sup>4</sup> When the reactor tripped, the TBVs and ADVs opened to the full-open position upon receipt of the "quick open" signal provided to the valves, and thereby relieving stored energy in the secondary and primary systems for a short period. However, the TBVs and ADVs did not re-close automatically because of the contacts sticking closed in the K7 relay.

initiating events (i.e., large LOCA and medium LOCA) have been modified to properly evaluate the risk impact associated with the excessive steam demand. The modified LOMFW event tree projects an initiating event assessment CCDP of  $4.0 \times 10^{-6}$  for the ESD event. The uncertainty distribution for the CCDP is given below.

	CCDP		
	5%	Mean	95%
Calvert Cliffs 2	2.2E-7	4.1E-6	1.5E-5

Condition assessment also has been conducted by assuming that the K7 relay of the Reactor Regulating System was in failure condition for 240 days, based on the finding discussed in the Special Inspection Report [2]. The condition assessment for the excessive steam demand event yields a CCDP of  $1.2 \times 10^{-6}$ . As the initiating event assessment yields a higher CCDP than the condition assessment, the discussion below is focused on the former.

- **Dominant Sequences**

The dominant core damage sequences resulting from LOMFW in this analysis are: Sequence 51 (50.0% of the total CCDP) and Sequence 34 (47.5%). The LOMFW event tree with these dominant sequences highlighted is shown in Figure 1 (Appendix B).

The events and important component failures in LOMFW Sequence 51 are:

- Loss of main feedwater occurs,
- Reactor trip fails, and
- Excessive steam demand occurs.

The events and important component failures in LOMFW Sequence 34 are:

- Loss of main feedwater occurs,
- Reactor trip succeeds,
- Excessive steam demand occurs,
- Both MSIVs are closed,
- Steam generator cooling fails, and
- Once through cooling fails.

- **Results Tables**

- The conditional core damage probabilities for the dominant sequences are shown in Table 1.

- The event tree sequence logic for the dominant sequences is presented in Table 2a.
- Table 2b defines the nomenclature used in Table 2a.
- The most important cut sets for the dominant sequences are listed in Table 3.
- Definitions and probabilities for modified or dominant basic events are provided in Table 4.

## Modeling Assumptions

### ● Analysis Type

The Revision-3-Plus of the Calvert Cliffs Standardized Plant Analysis Risk (SPAR) model [3] was used for this assessment. The SPAR Revision-3-Plus does not model the excessive steam demand, and therefore, the SPAR model has been modified to enable the risk evaluation of the ESD event. These modeling updates are discussed below in detail.

Subsequent to the updating of the SPAR model, both initiating event assessment and condition assessment have been performed to evaluate the risk impact of the K7 relay failure and the resulting ESD event. In the initiating event assessment, the actual reactor scram in the midst of the K7 relay failure was evaluated using the LOMFW event tree; the generation of the initial SIAS was also accounted for in this assessment. On the other hand, the condition assessment was performed for the failure condition of the K7 relay for 240 days with consideration of all potential initiating events as mentioned earlier.

### ● Modeling Assumptions Summary

*Key modeling assumptions.* The key modeling assumptions are listed below and discussed in detail in the following sections. These assumptions are important contributors to the overall risk.

- The operators would not be able to diagnose the cause of the excessive steam demand because of the complicated nature of the cause and the relatively short time available in the midst of the stressful situation. Therefore, the alternate RRS channel [2] is not given credit.
- The K7 relay of the Reactor Regulating System successfully functioned when the reactor tripped on May 28, 2003. However, the under-rated relay would have failed to open the next time the relay de-energized following the May reactor trip [2]. Therefore, in the condition assessment that was compared with the initiating event assessment, the K7 relay was assumed in failure, from the last successful function until this event on January 23, 2004 (i.e., 240 days).
- The function of the TBVs and ADVs following turbine trip is modeled together in the event trees by the top event of excessive steam demand to evaluate the risk

impact of the K7 relay failure. Closure of the MSIVs isolates steam flow from the steam generators to the TBVs. Therefore, the impact of the open TBVs on the plant was modeled by specifically accounting for all the possible functional states of the MSIVs upon reaching SGIS setpoint, namely: (1) both MSIVs successfully close, (2) only one MSIV successfully closes, and (3) no MSIV closes. On the other hand, the impact of the open ADVs on the plant was considered along with the MSIV states in evaluating the available time for the operator to carry out once through cooling.

- When both MSIVs are closed upon SGIS, the steam demand is only from open ADVs (5% of the total steam flow) and the failure of AFW (i.e., SG cooling) would necessitate OTC. In this case, the operators must initiate OTC upon recognition of lowering SG levels (due to no MFW and AFW) prior to SG dryout and subsequent RCS pressure rise to greater than the HPSI shutoff head.<sup>5</sup> The operator performance in this case is modeled in terms of human error event OTC3 as shown in Figure 1 of Appendix B. The plant behavior as predicted by the thermal-hydraulic (T/H) analyses for similar conditions was considered in developing the associated sequence modeling and estimating the human error probability for OTC3. The T/H analyses by both the plant simulator and the plant-specific RELAP-5 model for Calvert Cliffs are discussed in Appendix C, and the human performance modeling by the SPAR-H method [4] in Appendix D.
- When only one MSIV closes upon SGIS, the operators first should block the AFW flow path to the affected steam generator (i.e., with the associated MSIV failing open) and then ensure that the RCS heat is properly removed by the AFW flow into the intact steam generator with the steam removed through the ADVs. Based on a review of the T/H analyses (Appendix C) for similar situations, it was assumed that core damage could be prevented if secondary cooling is established whether or not the affected SG is blocked. Further, it was also assumed that the performance requirements for operator action would be almost the same regardless of success or failure of blocking the affected SG. As a result, the two operator actions for OTC given blocking success or failure of the affected SG were modeled in terms of an identical human error event (i.e., OTC4). The estimation of the human error probability for OTC4 is discussed in Appendix D.
- Where both MSIVs fail to close upon SGIS, a review of the detailed plant-specific T/H analyses performed for this case indicates that core damage can be prevented as long as SG cooling is properly established (e.g., by motor-driven AFW flow into a SG). In this case, the results of the RELAP-5 runs show that SG level will first drop rapidly due to release of the large amount of steam through the open valves (i.e., TBVs and ADVs), but will increase to the normal level in

---

<sup>5</sup> If wide range SG level in both SGs is less than -350 inches or the RCS cold leg temperature (i.e.,  $T_c$ ) rises uncontrollably 5°F or greater, the emergency operating procedures (e.g., Contingency Action 9.1 of the Loss of All Feedwater Recovery Guideline) instruct the operators to establish RCS heat removal via once-through-cooling.

about one and a half hours as a result of the AFW flow due to the decreasing core heat. Consequently, the RCS temperature suddenly drops due to the overcooling caused by the ESD, but stays low as a result of the effective SG cooling (Appendix C). In addition, the results from the plant simulator also point out the effectiveness of the AFW flow under these circumstances (Appendix C). In light of these plant-specific T/H analyses, credit was taken for the motor-driven AFW pumps, but not for the turbine-driven AFW pumps because of insufficient steam pressure to drive them under these circumstances. If both motor-driven AFW pumps (i.e., AFW MDP-13 and MDP-23) or associated flow paths are unavailable for operation, the plant operators need to initiate OTC; this operator action is modeled by human error event OTC5 (Appendix D). Finally, also note in this case that credit was not taken for an interlock signal for closure of all the TBVs upon loss of condenser vacuum, nor for the operator intervention to close the TBVs and/or ADVs, based on the following insights from a review of the T/H runs (Appendix C):

- a) The plant simulator runs indicate that wide range SG level in both SGs is expected to drop below -350 inches within 10 minutes, and as a result, OTC will have to be initiated before the main condenser loses vacuum. The loss of condenser vacuum supposedly will take at least half an hour according to an ex-SRO (senior reactor operator) at Calvert Cliffs .
  - b) The RELAP-5 runs predict that only a small amount of steam will be released through the TBVs after 10 minutes into the ESD event, and as a result, the operator intervention to close the TBVs (which is unlikely to happen before 10 minutes into the ESD event) is not expected to significantly change the potential outcome of the event.
- In the cases where an anticipated transient without scram (ATWS) occurs in concurrence with an excessive steam demand (especially given that the cause of the ESD is unknown to the operators), it is conservatively assumed that core damage will result. The reason for this conservative assumption is as follows:
- a) The operators might be able to manually trip the reactor by injecting boric acid into the core in the event of mechanical rods failure, provided that the core was not at the beginning of the fuel cycle and the operators were not in a very stressful situation due to other co-existing or on-going failures.
  - b) However, it is expected that the operators would be subjected to extremely high stress in a very rapidly developing accident caused by the simultaneous occurrence of an ATWS and an excess steam demand (due to the K7 relay failure, unknown to the operators during the event). Therefore, even though credit is taken for the operator recovery action to inject borated water into the core in the specific case where the RPS failed due to immovable control rods during a fuel cycle other than the

early stage, the incorporation of this recovery action is not expected to have significant impact on the conditional core damage probability.

- The reactor vessel is subjected to a pressurized thermal shock (PTS) when an extended cooling transient to the vessel wall is accompanied by system pressurization. According to PTS experiments, a crack may initiate and propagate entirely through the vessel wall, involving large openings in the reactor vessel and also significant additional deformation of the vessel. However, there currently is an incomplete understanding concerning the progression of an accident following a postulated PTS-induced vessel failure. In light of the uncertainty about the PTS occurrence and also the subsequent accident propagation especially given lack of the plant-specific probabilistic fracture mechanics for the ESD event, a check was made to see how much impact the occurrence of a potential PTS will have on the likelihood of the two most dominant scenarios, i.e., Transient Sequence 51 and SGTR Sequence 38, shown in Figures 2 and 3, respectively. These scenarios contribute about 25% and 15% to the event CCDP (Table 1). The examination of these scenarios indicates that the likelihood of these dominant scenarios is essentially insensitive to the potential occurrence of a PTS during the event progression:
  - a) First, consider Transient Sequence 51 where a transient occurs followed by failure of a reactor trip and occurrence of an excessive steam demand. In this case, core damage was already assumed in the sequence modeling for this event assessment (see Figure 2). Therefore, this sequence modeling is still valid even if the core damage is caused by occurrence of a PTS in the midst of the ATWS and ESD conditions.
  - b) Second, consider the SGTR Sequence 38 where an SGTR occurs followed by a successful reactor trip, an excessive steam demand, closure of both MSIVs, successful SG cooling and high pressure injection, operator failure to depressurize the RCS below SG relief valve setpoint, and subsequent operator failure to depressurize the RCS given a SG relief valve opened. Considering that the closure of MSIVs and the SG cooling will generally take place in the very early stage by the automatic signals (i.e., SGIS and AFAS), the potential occurrence of a PTS may be contemplated for two periods: 1) before HPSI operation, and 2) after operator failure to depressurize the RCS given a SG relief valve opened. For the first period, the PTS is not likely to happen because the large amount of steam release through the TBVs was isolated early by the closure of both MSIVs, and as a result, the RCS will not be considerably overcooled. For the second period, even if a PTS occurs, a core damage is already assumed in Figure 3.
- Natural circulation cooling would not have been threatened during the event sequences (e.g., loss of offsite power) involving an excessive steam demand, because of the initial high differential temperature between the hot leg and the cold leg of the RCS which promotes natural circulation.



- The generation of the second SIAS signal during the recovery phase of the event does not have significant impact on core damage frequency (CDF).

- **Event Tree Modifications**

**All the Event Trees But LLOCA and MLOCA Event Trees (e.g., TRANS, LOMFW, SGTR, LOOP, etc.)** The following three new top events have been added to all the event trees of the original SPAR model other than those for large LOCA and medium LOCA initiating events:

- a) “Excessive Steam Demand (ESD)” to model the considerable steam release through the widely open TBVs and ADVs as a result of the K7 relay failure;
- b) “Main Steam Isolation Valves Closed (MSIV)” to model the function of the MSIVs subsequent to the excessive steam demand; and
- c) “One AFW Flow-Path Blocked” (SGBLOCK) to model the inefficiency of the steam generator with the associated MSIV open in the presence of all the TBVs fully open.

The second top event (i.e., MSIV) is associated with three alternatives, namely: (1) both MSIVs successfully closed; (2) only one MSIV closed; and (3) failure of both MSIVs to close. Therefore, the following rule has been added to the existing event tree linkage rules, so that an appropriate fault tree may be applied for each of the three cases implemented in terms of triple branches in the event trees:

```

if always then
  /MSIV = MSIV
  MSIV[1] = MSIV-1
  MSIV[2] = MSIV-2
endif

```

The first fault tree in the above rule (i.e., MSIV) models the success of both MSIVs being closed on demand, and the second and the third fault trees (i.e., MSIV-1 and MSIV-2) model successful closure of only one MSIV and failure of both MSIVs to close upon demand, respectively.

In addition, the event tree linkage rules such as the following also have been added to the event trees modified to incorporate the ESD event, so that an appropriate fault tree for steam generator cooling and once through cooling may be applied depending on the specific circumstances:

```

if /RPS*ESD*MSIV[2] then
  SGC = SGC-ESD;
endif

```

```

if /RPS*ESD*/MSIV*SGC then
  OTC = OTC3;
endif

if/RPS*ESD*MSIV[1]*/SGBLOCK*SGC then
  OTC = OTC4;
endif

if /RPS*ESD*MSIV[1]*SGBLOCK*SGC then
  OTC = OTC4;
endif

if /RPS*ESD*MSIV[2]*SGC then
  OTC = OTC5;
endif

```

The salient features in the modification of the original event trees are briefly summarized below using the revised event tree for general transients (i.e., TRANS) as an example (see Figure 2 in Appendix B):

- a) TRANS sequences 1-17 in the revised event tree are the same as TRANS sequences 1-17 of the original event tree, because excessive steam demand does not occur.
- b) TRANS sequences 18-34 in the revised event tree show the cases where both MSIVs are closed upon receipt of the steam generator isolation signal (SGIS). If steam generator cooling (SGC) is established through AFW prior to SG dryout, the subsequent sequences are essentially the same as for TRANS sequences 1-13. If SGC fails, the operators should initiate OTC to prevent core damage.
- c) TRANS sequences 35-44 reflect the cases where only one MSIV closes upon SGIS. In these circumstances, the operators first need to block the AFW flow path to the affected steam generator with the associated MSIV failed open so that the intact SG can be used for RCS heat removal by controlling the SG water level through the ADVs. Hence, the new top event SGBLOCK is asked following the MSIV top event. If the SG cooling cannot be properly established, the operators then should initiate OTC to avert core damage.
- d) TRANS sequences 45-49 show the cases where both MSIVs fail to close upon SGIS. Based on the plant-specific T/H analyses (Appendix C), the operators need to ensure SG cooling has been properly established; otherwise, they must initiate OTC to prevent core damage.
- e) TRANS sequence 50 transfers to ATWS event tree as in the original TRANS event tree because of the RPS failure and no demand for excessive steam.

- f) TRANS sequence 51 is assumed to lead to core damage because of the excessive steam demand in the midst of the ATWS condition caused by the RPS failure.

A similar modification has been made to all the event trees other than LLOCA and MLOCA event trees, because in these LOCA conditions the RCS average temperature (i.e.,  $T_{ave}$ ) is expected to be less than 557°F following reactor trip, and as a result, the quick open signal will not be generated. The modified event trees are shown in Figures 1-10 (Appendix B).

### ● **Fault Tree Modifications**

Fourteen new fault trees for the following top events have been developed and added to the SPAR model for CCNPP [3] in order to enable assessment of the excessive steam demand event:

- ESD: Excessive steam demand
- MSIV: Both MSIVs closed on demand
- MSIV-1: Only one MSIV closed on demand
- MSIV-2: No MSIV closed on demand
- SGBLOCK: AFW block fails on demand
- OTC3: Once through cooling when both MSIVs close on demand
- OTC4: Once through cooling when only one MSIV closes on demand
- OTC5: Once through cooling when both MSIVs fail to close on demand
- SGC-ESD: Steam generator cooling
- AFW-ESD: AFW flow from Unit 1 AFW system
- AFW-SG-11-ESD: Steam generator 11 cooling
- AFW-SG-12-ESD: Steam generator 12 cooling
- AFW-TDP-11-ESD: AFW TDP 11 flow
- AFW-TDP-12-ESD: AFW TDP 12 flow

These fault trees are shown in Figures 11-24 (Appendix B). Human error probabilities associated with initiating OTC under different conditions were quantified using SPAR-H [4] as mentioned before (Appendix D). The last six fault trees were added to model failure of the turbine-driven AFW pumps due to insufficient steam pressure.

### ● **Recovery Rule Modifications**

The recovery rules in the original SPAR model contain a number of dependency correction factors for human error probabilities to take into account the dependency of the operator failures in a sequence cut set. The recovery rules including the operator action for once through cooling in the original model (i.e., HPI-XHE-XM-OTC) were modified such that they also apply to other OTC actions defined for the event assessment. For example, the following recovery rule, i.e.,

```

elsif MFW-XHE-XO-ERROR * CDS-XHE-XM-LTSUPP * AFW-XHE-XL-LTSUPP
* MFW-XHE-XM-LPFLCHS * HPI-XHE-XM-OTC then
DeleteEvent = MFW-XHE-XM-LPFLCHS;
AddEvent    = MFW-XHE-XM-LPFLCHS1;
DeleteEvent = HPI-XHE-XM-OTC;
AddEvent    = HPI-XHE-XM-OTC1;

```

was expanded to include:

```

elsif MFW-XHE-XO-ERROR * CDS-XHE-XM-LTSUPP * AFW-XHE-XL-LTSUPP
* MFW-XHE-XM-LPFLCHS * HPI-XHE-XM-OTC3 then
DeleteEvent = MFW-XHE-XM-LPFLCHS;
AddEvent    = MFW-XHE-XM-LPFLCHS1;
DeleteEvent = HPI-XHE-XM-OTC3;
AddEvent    = HPI-XHE-XM-OTC1;

```

```

elsif MFW-XHE-XO-ERROR * CDS-XHE-XM-LTSUPP * AFW-XHE-XL-LTSUPP
* MFW-XHE-XM-LPFLCHS * HPI-XHE-XM-OTC4 then
DeleteEvent = MFW-XHE-XM-LPFLCHS;
AddEvent    = MFW-XHE-XM-LPFLCHS1;
DeleteEvent = HPI-XHE-XM-OTC4;
AddEvent    = HPI-XHE-XM-OTC1;

```

```

elsif MFW-XHE-XO-ERROR * CDS-XHE-XM-LTSUPP * AFW-XHE-XL-LTSUPP
* MFW-XHE-XM-LPFLCHS * HPI-XHE-XM-OTC5 then
DeleteEvent = MFW-XHE-XM-LPFLCHS;
AddEvent    = MFW-XHE-XM-LPFLCHS1;
DeleteEvent = HPI-XHE-XM-OTC5;
AddEvent    = HPI-XHE-XM-OTC1;

```

Note that the human error probability for once through cooling is increased to the human error probability for HPI-XHE-XM-OTC1 (i.e., 1.0), when such multiple human errors as specified by the recovery rules above are included in a sequence cut set.

- **Basic Event Probability Changes**

Table 4 provides all the basic events that are included in the dominant sequences of Table 3, or have been generated as part of this analysis in order to model event sequences associated with the excessive steam demand.

- **Other Items of Interest**

- Common cause failure (CCF) of the MSIVs was modeled using SPAR model values [3] for alpha factor parameters for two air operated valves with staggered

testing.<sup>6</sup>

- Process flag “I” (indicating the use of the system logic for failure and the use of the complement of the system logic for success) was attached to the basic event for excessive steam demand (i.e., ESD-BE) in order to appropriately account for success event when the associated probability is relatively large (e.g., as in sensitivity analyses).
- The re-quantification of the base case CDF by the revised SPAR model (with the assumed failure probability of  $1 \times 10^{-4}$  for the excessive steam demand basic event) yields a value of  $8.144 \times 10^{-6}$  per year which is essentially identical to the baseline CDF as obtained by the original SPAR model (i.e.,  $8.145 \times 10^{-6}$  per year).

- **Sensitivity Analyses**

Sensitivity analyses were performed to determine the effects of model uncertainties on results based on best estimate assumptions. The following table provides the results of the sensitivity analyses.

<b>Sensitivity Case</b>	<b>Importance</b>
<b>Case A:</b> Increase the failure probability for the excess steam demand basic event (ESD-BE) from $1E-4$ to $1E-3$ in the revised baseline model incorporating event sequences associated with the excessive steam demand (Base Case)	8.1E-6
<b>Case B:</b> Increase the fault exposure time for the K7 relay from 240 days to 365 days (Condition Assessment)	1.8E-6
<b>Case C:</b> Compute the conditional probability of core damage, given that the K7 relay was in failure and this condition would only be discovered through an excessive steam demand following some initiating event. This calculation assumes that the failure condition lasts as long as it takes to discover it through an initiating event, and is independent of actual duration. (Initiating Event Assessment)	1.1E-5
<b>Case D:</b> Increase the failure probability of each MSIV to close on demand by an order of magnitude (i.e., from $1.5E-3$ to $1.5E-2$ ) (Initiating Event Assessment)	4.1E-6

---

<sup>6</sup> The alpha factor parameters for air operated valves were used for MSIVs as per suggestion from the Idaho National Laboratories (INL), because the SPAR CCF database does not include the specific parameters for MSIVs.

Sensitivity Case	Importance
<b>Case E:</b> Increase the common cause failure probability for MSIVs to close on demand by a factor of 2 (i.e., from 4.6E-5 to 9.2E-5) (Initiating Event Assessment)	4.0E-6
<b>Case F:</b> Increase the failure probability for RCS-PHN-MODPOOR (Moderator Temperature Coefficient Not Enough Negative) by an order of magnitude (i.e., from 1.4E-2 to 1.4E-1) (Initiating Event Assessment)	4.0E-6
<b>Case G:</b> Compute the conditional probability of core damage assuming that the human actions for once through cooling in the midst of excessive steam demand (i.e., OTC3, OTC4, and OTC5) involve a significant amount of diagnosis activity in addition to the actual action needed (Initiating Event Assessment)	4.3E-6

- Case A shows that the change in the failure probability for the ESD-BE event by an order of magnitude has insignificant impact on the risk impact, because the dominant sequences involve no demand for excessive steam (i.e., the result is not influenced by whether the success probability for ESD-BE is  $9.999 \times 10^{-1}$  or  $9.99 \times 10^{-1}$ ).
- Case B shows that the condition assessment using the extended fault exposure time of 365 days (as opposed to 240 days) yields an importance (i.e.,  $\Delta$ CCDP) of  $1.8 \times 10^{-6}$ , which is still smaller than the best estimate importance for the event (i.e., a CCDP of  $4.0 \times 10^{-6}$ ).
- Case C represents a special situation to estimate the conditional probability that core damage will occur, given that the K7 relay contacts were stuck, assuming that the condition is discovered through the occurrence of some initiating event leading to excessive steam demand. Within this thought process, "duration" does not matter; it is assumed that the failure condition is discovered only through the occurrence of an initiating event leading to excessive steam demand. This calculation was done by the artifice of defining a change set in which the initiating event frequencies were proportionately scaled upward so that they summed to unity, and the ESD-BE event was set to True. This change set was run with a duration of one year. Arithmetically, this equates to multiplying each initiating-event CCDP by the conditional probability of that initiating event, given that some initiator occurred. This sensitivity analysis yields a CCDP of  $1.1 \times 10^{-5}$  that is a factor of about 2.8 greater than the initiating event assessment CCDP of  $4.0 \times 10^{-6}$ .
- Case D shows that the independent failure probability for each MSIV to close on demand (i.e., MSS-MSIV-OO-HV11 and MSS-MSIV-OO-HV12) has insignificant impact on the CCDP, because of diverse means of coping with the excess steam

demand event such as auxiliary feedwater or once through cooling.

- Case E shows that the double increase in the CCF probability for MSIVs to close on demand (i.e., MSS-MSIV-CF-CLOSE) has no impact on the CCDP primarily due to the effectiveness of the motor-driven auxiliary feedwater flow in averting core uncover in the midst of an ESD event coupled by failure of both MSIVs being closed.
- Case F shows that the variance in the moderator temperature coefficient as represented by the RCS-PHN-MODPOOR basic event has a negligible impact on the final result.
- Case G represents a special case where it has been assumed that the human actions for once through cooling in the midst of excessive steam demand (i.e., HPI-XHE-XM-OTC3, HPI-XHE-XM-OTC4, and HPI-XHE-XM-OTC5) involve a significant amount of diagnosis activity in addition to the actual action needed. The performance shaping factors (PSFs) used for this case are shown below:

Human Error Event	Multiplier for Diagnosis			Multiplier for Action			Total HEP
	Time	Stress	Complexity	Time	Stress	Complexity	
OTC3	1	2	2	10	2	2	0.08
OTC4	10	2	5	10	2	2	0.87
OTC5	10	5	5	10	2	2	0.97

The total human error probabilities (HEPs) for those situations (either diagnosis or action) involving multiple (i.e., 3 or more) non-nominal PSFs in the above table were calculated by applying an adjustment factor in accordance to the formula provided in the SPAR-H documentation [4] in order to represent the composite PSF influence. Note that the total HEPs used for OTC3, OTC4, and OTC5 in the best estimate evaluation are 0.04, 0.09, and 0.20, respectively, as shown in Table 4 and Appendix D. The initiating event assessment for this sensitivity case yields a CCDP of  $4.3 \times 10^{-6}$  that is just slightly greater than the best estimate event assessment CCDP (i.e.,  $4.0 \times 10^{-6}$ ). This relatively small sensitivity of OTC human actions on the CCDP results from the fact that once through cooling is necessary only when steam generator cooling cannot be properly maintained by use of auxiliary feedwater in most failure cases involving an excessive steam demand.

## References

---

1. LER 318/04-001, Revision 00, "Reactor Trip Due to Low Steam Generator Water Level After Feed Pump Trip," Event Date: January 23, 2004.
2. NRC Special Inspection (SI) Team Report, EA-04110, "Calvert Cliffs Nuclear Power Plant, Unit 1 and Unit 2 - NRC Inspection Report 05000317/2004008 and 05000318/2004008," July 29, 2004.
3. Idaho National Engineering and Environmental Laboratory, "Standardized Plant Analysis Risk Model for Calvert Cliffs 1 & 2," Revision 3.12, February 2, 2005.
4. Idaho National Engineering and Environmental Laboratory, "The SPAR-H Human Reliability Analysis Method," INEEL/EXT-02-01307, May 2004.
5. B. Mrowca, et al., "Calvert Cliffs Nuclear Power Plant Probabilistic Risk Assessment — Individual Plant Examination," December 1993.



Table 1. Conditional core damage probabilities of dominating sequences.

Event tree name	Sequence no.	CCDP <sup>1</sup>	Contribution
LOMFW	51	2.0E-6	50.0
LOMFW	34	1.9E-6	47.5
<b>Total (all sequences)<sup>2</sup></b>		<b>4.0E-6</b>	<b>100</b>

1. Values are point estimates.

2. Total CCDP includes all sequences (including those not shown in this table).

Table 2a. Event tree sequence logic for dominating sequences.

Event tree name	Sequence no.	Logic (“/” denotes success; see Table 2b for top event names)
LOMFW	51	RPS, ESD
LOMFW	34	/RPS, ESD, /MSIV, SGC, OTC3

Table 2b. Definitions of top events listed in Table 2a.

Top Event	Definition
ESD	Excessive steam demand occurs
MSIV	Main steam isolation valves fail to close
OTC3	Once through cooling fails
RPS	Reactor trip fails
SGC	Steam generator cooling fails

Table 3. Conditional cut sets for the dominant sequences.

CCDP	Percent Contribution	Minimum Cut Sets (of basic events)
<b>Event Tree: LOMFW, Sequence 51</b>		
1.2E-6	58.7	RPS-VCF-FO-MECH
7.0E-7	34.4	RPS-RTB-FC-FTO      RPS-XHE-ERROR
1.4E-6	6.9	RPS-XHE-XM-SCRAM      RPS-VCF-FO-ELEC
2.0E-6	100	Total (all cutsets) <sup>1</sup>
<b>Event Tree: LOMFW, Sequence 34</b>		
1.4E-6	72.8	CDS-XHE-XM-LTSUPP      AFW-XHE-XL-LTSUPP1      HPI-XHE-XM-OTC1 MFW-XHE-XM-LPFLFW1
2.8E-7	14.6	CDS-XHE-XM-LTSUPP      LPF-SYS-FC-LOMFW      AFW-XHE-XL-LTSUPP1 HPI-XHE-XM-OTC1
1.1E-7	5.7	AFW-CKV-CF-SGS      HPI-XHE-XM-OTC3
9.6E-8	5.0	CDS-TNK-FC-CST12      HPI-XHE-XM-OTC3
1.9E-6	100	Total (all cutsets) <sup>1</sup>

1. Total Importance includes all cutsets (including those not shown in this table).

Table 4. Definitions and probabilities for modified and dominant basic events.

Event Name	Description	Probability/ Frequency (per hour)	Modified
AFW-BLOCK <sup>1</sup>	AFW BLOCK FAILS ON DEMAND	1.5E-4	N/A
AFW-CKV-CF-SGS	CCF OF STEAM GENERATOR INLET CHECK VALVES	2.8E-6	No
AFW-XHE-XL-LTSUPP1	OPERATOR FAILS TO RECOVER FROM CST 12 LOW LEVEL (DEPENDENT EVENT)	1.4E-1	No
CDS-TNK-FC-CST12	CONDENSATE STORAGE TANK 12 IS UNAVAILABLE	2.4E-6	No
CDS-XHE-XM-LTSUPP	OPERATOR FAILS TO ALIGN A LONG-TERM WATER SUPPLY TO AFW SUCTION	1.0E-5	No
ESD-BE <sup>2</sup>	EXCESSIVE STEAM DEMAND EVENT OCCURS	1.0E-4	N/A
HPI-XHE-XM-OTC1	OPERATOR FAILS TO INITIATE ONCE THROUGH COOLING (DEPENDENT EVENT)	1.0E+0	No
HPI-XHE-XM-OTC3 <sup>3</sup>	FAILURE TO INITIATE OTC WITH BOTH MSIVS SUCCESSFULLY CLOSED	4.0E-2	N/A
HPI-XHE-XM-OTC4 <sup>3</sup>	FAILURE TO INITIATE OTC WITH ONE MSIV OPEN	9.0E-2	N/A

Event Name	Description	Probability/ Frequency (per hour)	Modified
HPI-XHE-XM-OTC5 <sup>3</sup>	FAILURE TO INITIATE OTC WITH BOTH MSIVS OPEN	2.0E-1	N/A
LPF-SYS-FC-LOMFW	LOW PRESSURE FEED HARDWARE FAILED GIVEN LOSS OF FEEDWATER	2.0E-1	No
MFW-XHE-XM-LPFLFW1	OPERATOR FAILS TO ESTABLISH LOW PRESSURE FEED TO SGs (DEPENDENT EVENT)	1.0E-2	No
MSS-MSIV-CF-CLOSE <sup>4</sup>	CCF OF MSIVS TO CLOSE	4.6E-5	N/A
MSS-MSIV-OO-HV11 <sup>5</sup>	MSIV HV11 FAILS TO CLOSE	1.5E-3	N/A
MSS-MSIV-OO-HV12 <sup>5</sup>	MSIV HV12 FAILS TO CLOSE	1.5E-3	N/A
RPS-RTB-FC-FTO	TRIP CIRCUIT BREAKERS FAIL TO OPEN	1.6E-6	No
RPS-VCF-FO-ELEC	ELECTRICAL (UV & ST) RPS FAILURE TO OPEN TRIP CIRCUIT BREAKERS	1.4E-5	No
RPS-VCF-FO-MECH	CONTROL ROD ASSEMBLIES FAIL TO INSERT	1.2E-6	No
RPS-XHE-ERROR	OPERATOR FAILS TO DE-ENERGIZE CEDM POWER SUPPLY (RECOVERY EVENT)	4.4E-1	No
RPS-XHE-XM-SCRAM	OPERATOR FAILS TO MANUALLY TRIP THE REACTOR	1.0E-2	No

1. This basic event has been generated to model the inefficiency of the steam generator with the associated MSIV open in the presence of all the TBVs fully open. The failure probability of 1.5E-4 for this event was taken from the IPE for Calvert Cliffs Nuclear Power Plant [5].

2. This basic event has been generated to model the excessive steam demand as part of event sequences following a reactor trip; however, no detailed system model (e.g., including specific relays) was developed in this analysis. The failure probability of 1.0E-4 has been assumed for the ESD-BE basic event based on engineering judgment. Note that the assumption of this value has no effect on the results of this analysis, because the ESD-BE basic event was set to True in both the initiating event assessment and the condition assessment for the base case (i.e., 240 days of fault exposure time for the K7 relay).

3. Refer to the SPAR HRA worksheet in Appendix C.

4. The CCF probability for MSIVs is based on the alpha factors for air operated valves with staggered testing scheme.

5. These basic events for MSIVs have been generated to model the event sequences following the excessive steam demand. The failure probability of 1.5E-3 for these events was taken from the IPE for Calvert Cliffs Nuclear Power Plant [5].

# **Appendix A**

## **Sequences of Key Events**

From NRC Special Inspection Team Report 50/317/318-2004-008:

- 15:26.02 Initial Conditions  
100% Reactor Power. 24 CWP secured for planned maintenance. RTCBs 1&5 open due to problems experienced earlier in the day during the performance of an IM STP Reactor Reg System selected to Channel X.
- 15:26.37 22 SGFP Trips (With direction from the CRS, the CRO attempts multiple resets of the 22 SGFP per plant stabilizing actions IAW AOP-3G. None of the resets are successful and the CRS orders a manual reactor trip when S/G Low Level Pre-Trips are received (coincident with -40" S/G levels per narrow range level indication).)
- 15:27.48 RPS Steam Generator Low Level Channel A & D Trip. RTCB's 2, 3, 4, 6, 7, 8 open. RPS manual reactor trip from 1C05 due to action of RO.
- 15:28.20 ADVs and TBVs are not responding as designed as they are still full open and RCS average temperature is well below 557°F.
- 15:28.26 All pressurizer backup and proportional heater banks automatically secure due to pressurizer level falling below 101". The RO places all heater hand switches in OFF shortly afterwards.
- 15:28.34 AFAS B actuation. ESFAS SIAS A & B actuation.
- 15:28.52 2B EDG, 21 & 22 LPSI pumps, 21 & 22 CS pumps, 21 HPSI pump all start.
- 15:28.53 22 Component cooling pump starts, 23 HPSI pump all start.
- 15:28.54 21 & 22 Boric acid pumps, 21/22/23 IRU, 24 CAC Fan all start.
- 15:28.57 ESFAS SGIS A & B Actuation.
- 15:28.59 Letdown secured. 2A & 2B EDG start.
- 15:29.00 21 & 22 MSIVs shut (with the MSIVs shut due to the SGIS actuation, the TBVs are no longer contributing to the excess steam demand event. For approximately the next seven minutes the RCS continues to cooldown at a rate of approximately 160°F/hr.
- 15:29.13 Pressurizer level goes off-scale low.
- 15:32.15 21B & 22A RCP secured in accordance with RCP Trip Strategy for SIAS actuation.
- 15:37.00 The Quick Open Dump Signal from RRS is removed from both ADVs when the TBO shifts the hand transfer valves in the 45' switchgear room to align ADV

control to 2C43. Over the next 32 minutes, an RCS heatup at approximately 57°F/hr takes place until RCS cold leg temperatures are restored to 515°F.

- 15:39.50 Pressurizer level returns to scale
- 15:47.30 The operating crew reduces AFW flow to each S/G from 300gpm to 150gpm.  
Summary of EOP-O, Post Trip Immediate Actions:  
Safety Function Status  
Reactivity Control - Complete  
Vital Auxiliaries - Complete  
RCS Pressure and Inventory Control - Not Met  
Core and RCS Heat Removal - Not Met  
Containment Environment - Complete  
Rad Levels External to Containment - Complete  
Safety System Actuations  
AFAS - Verified  
SIAS - Verified  
SGIS - Verified
- 15:55.00 EOP-1, Reactor Trip, is implemented from EOP-0. Upon entry, the crew recognizes the high RCS pressure and the rapidly rising pressurizer level and prepares to take stabilizing actions.
- 15:56.00 The RO takes manual control of the Main Spray Controller, 2HIC100, (which has been greatly reduced due to only having one RCP operating in the spray line loops) and places the output at approximately 30-35% to stop the RCS pressure rise at 2335 psia. Subsequent minor manual Main Spray Controller manipulations results in a stable RCS pressure at around 2318psia. Note - the main spray valves, 1CV100E and 1CV100F, did not start to open until 2300 psia (based on a pressurizer controller setpoint of 2250 psia).
- 15:58.00 Due to the insurge from the RCS heatup, along with approximately 4100 gallons of injection from the Charging system, Pressurizer level has reached ~210" and the Pressurizer temperature has reached a minimum value of 514°F (saturation for 771 psia).
- 15:59.00 The Pressurizer insurge continues as full Charging is still present at 128 GPM and the 57°F/hr RCS heatup continues. At this point, due to the large volume of "cold" water in the Pressurizer and the lack of full heater capability, RCS pressure begins to rapidly drop from ~2318 to ~1800 psia over the next 22 minutes.
- 16:01.46 22 & 23 charging pump are secured (H/S placed in PTL).
- 16:05.00 Based on Operator recall, the Main Spray Controller, 2HIC100, output signal is lowered from 30 – 35% to approximately -2% (although 2HIC100 can be driven

to an output as low as -20%, an output of 0% should represent a signal at which both Main Spray valves are full shut).

- 16:06.50 21 Charging pump is secured.
- 16:08.00 The RCS heatup is temporarily secured per the operating crew's decision to hold RCS cold leg temperature at 515°F.
- 16:09.00 Based on Operator recall, both Pressurizer Proportional Heaters are returned to AUTO and Backup Heaters 22 and 24 are placed in ON. Backup Heater 24 only has a capacity of 225 KW (normal capacity is 300 KW) due to a previous CMF that had one bank of heaters removed from service. Backup Heaters 21 and 23 can not be returned to service at this time due to the active SIAS signals.
- 16:17.28 SIAS A is reset remotely from the Control Room. SIAS B can not be reset from the Control Room due to a problem with the reset pushbutton.
- 16:27.36 SIAS B is reset locally from the Cable Spreading Room.
- 16:33.35 21 Charging Pump is started per OI-2A in an effort to restore Letdown to restore Pressurizer level. For approximately the next five minutes, the Operating Crew attempts to restore Letdown, but problems associated with the Control Room position indication for one of the Letdown isolation valves, 2-CV-516, delays the successful restoration.
- 16:38.50 21 Charging Pump is secured when the Operating Crew believes that the Letdown isolation valve, 2-CV-516, is not opening when attempts are made using the hand switch.
- 16:39.00 Based on Operator recall, Pressurizer Backup Heaters 21 and 23 are restored and placed in ON now that SIAS has been reset and both heater breakers have been closed locally.
- 16:45.30 A second heatup of the RCS at approximately 35°F/hr is commenced to return RCS cold leg temperatures to the EOP-1 acceptable range of 525 - 535°F. The heatup and resulting Pressurizer insurge contributes to RCS pressure lowering from ~1800 psia to ~1750 psia over the next 30 minutes. The combination of Letdown and the RCS heatup result in the RCS Pressure lowering to 1750 psia and a second SIAS actuation.
- 16:48.29 21 Charging pump is started per OI-2A in a second effort to restore Letdown to restore pressurizer level.
- 16:48.40 Letdown is successfully placed in service and raised to approximately 105gpm over the next nine minutes.
- 16:57.23 Letdown is maintained between 100 & 115gpm until about 17:14.34.

- 17:04.00 Per CRS/SM direction, the RO lowers the Main Spray Controller, 2HIC100, output signal to -20% (lowest possible output signal) to ensure that the Main Spray valves are fully closed in an attempt to minimize any leakby on the valves.
- 17:14.34 Letdown flow is reduced to ~70 GPM as the Operating Crew recognizes that RCS pressure is steadily lowering and re-approaching the SIAS setpoint.
- 17:18.01 ESFAS SIAS B actuation (lose capability to use pressurizer backup heater 23).
- 17:18.02 ESFAS SIAS A actuation (lose capability to use pressurizer backup heater 21).
- 17:20.53 21 charging pump is secured.
- 17:49.00 After using procedure guidance from EOP-4 and blocking SIAS, the Operating Crew resets SIAS A remotely from the Control Room. The decision to block and reset SIAS is made in order to recover full Pressurizer heater capability in an attempt to restore RCS pressure which has remained between 1750 and 1780 psia for the previous 50 to 60 minutes.
- 17:53.29 SIAS B is reset locally from the Cable Spreading Room.
- 17:58.00 Based on Operator recall, Pressurizer Backup Heaters 21 and 23 are restored and placed in ON now that SIAS has again been reset and both heater breakers have been closed locally. The Operating Crew now has full Pressurizer heater output. The Operating Crew decides to not attempt to reinitiate Charging and Letdown until RCS pressure reaches 2100 psia in order to assure that another RCS depressurization does not occur.
- 18:22.00 Based on Operator recall, the Main Spray Controller, 2HIC100, is returned to automatic control.
- 18:25.00 SGIS is reset using guidance from EOP-3.
- 18:29.20 AFAS A & B are reset in accordance with OI-32B.
- 18:32.29 21 Charging pump is started in preparation for restoring letdown.
- 18:33.35 Charging and Letdown is restored in attempt to return Pressurizer level to the EOP-1 acceptable band of 130 to 180". Letdown is established at approximately 45 – 50 GPM.
- 19:26.00 The Operating Crew exits EOP-1 and implements OP-2 and OP-4.
- 19:30.00 The 21B and 22A RCPs are restarted in accordance with OI-1A. The 21 AFW pump is secured.
- 19:50.00 Both MSIVs are reopened in accordance with OP-2.



19:55.00 Secured 21 AFW pump.

20.00.00 RCS parameters have reached normal post-trip levels and are considered steady state.

# **Appendix B**

## **Event Tree and Fault Tree Figures**

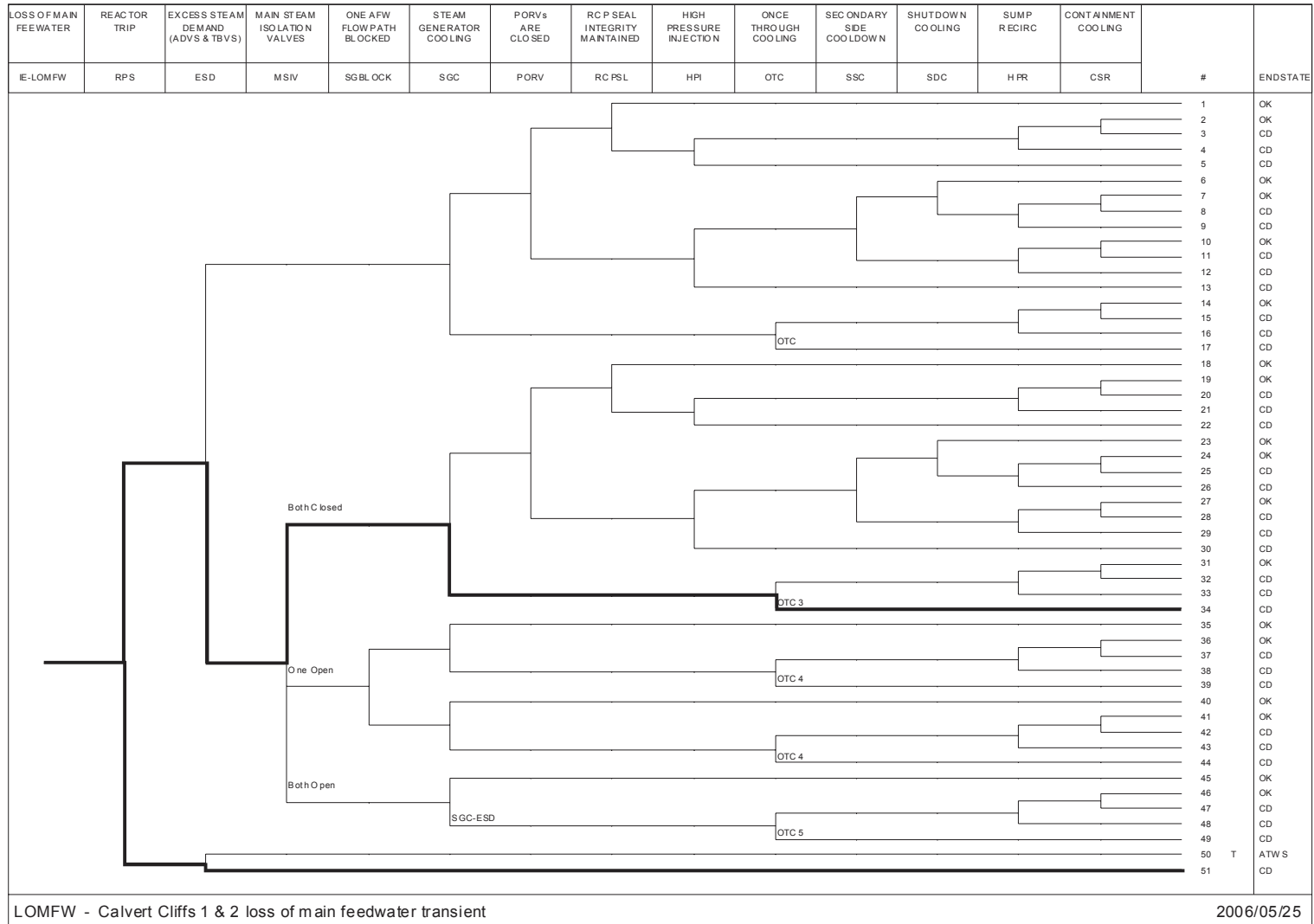


Figure 1. Event tree for loss of main feedwater transient.



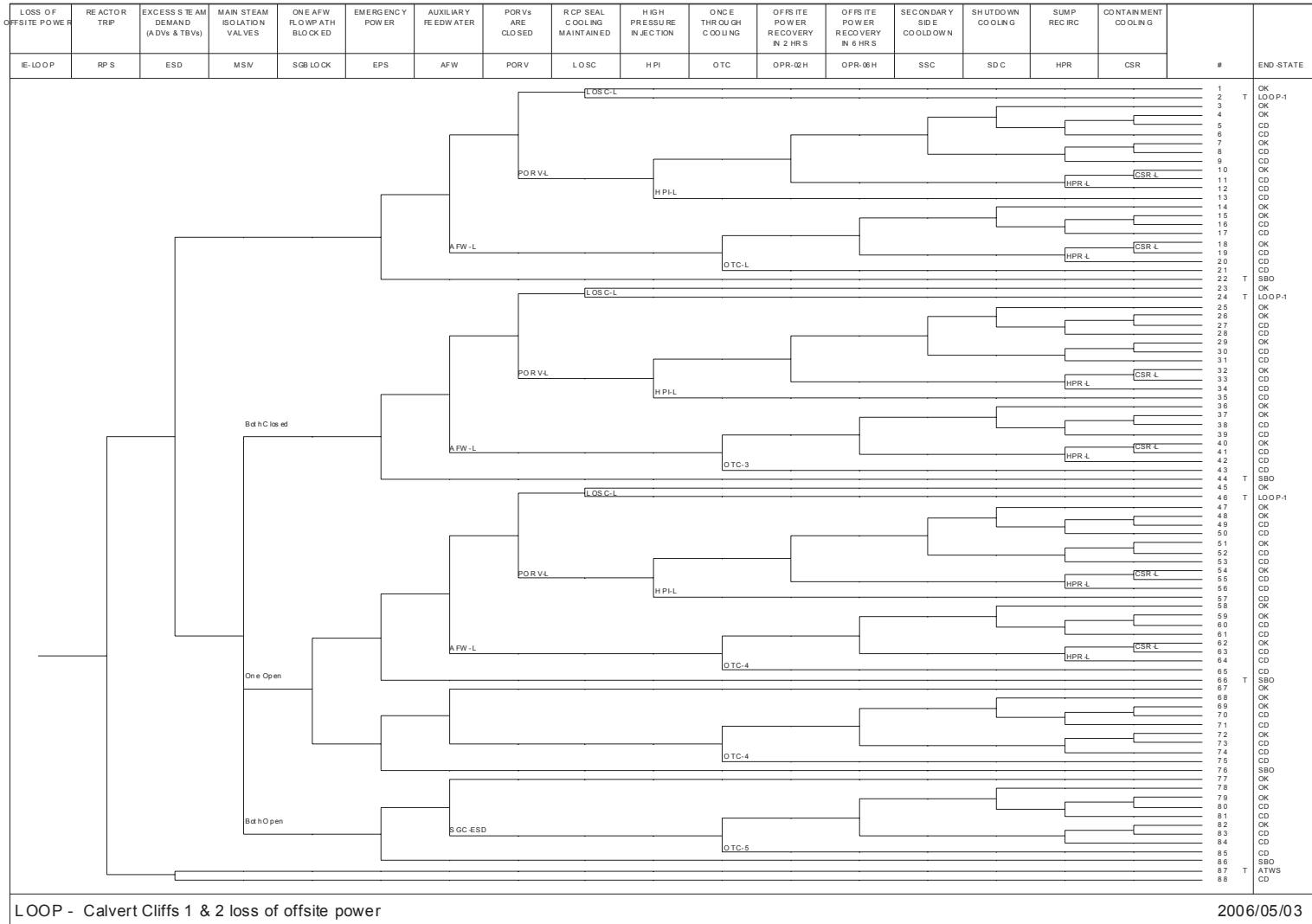


Figure 3. Event tree for loss of offsite power.

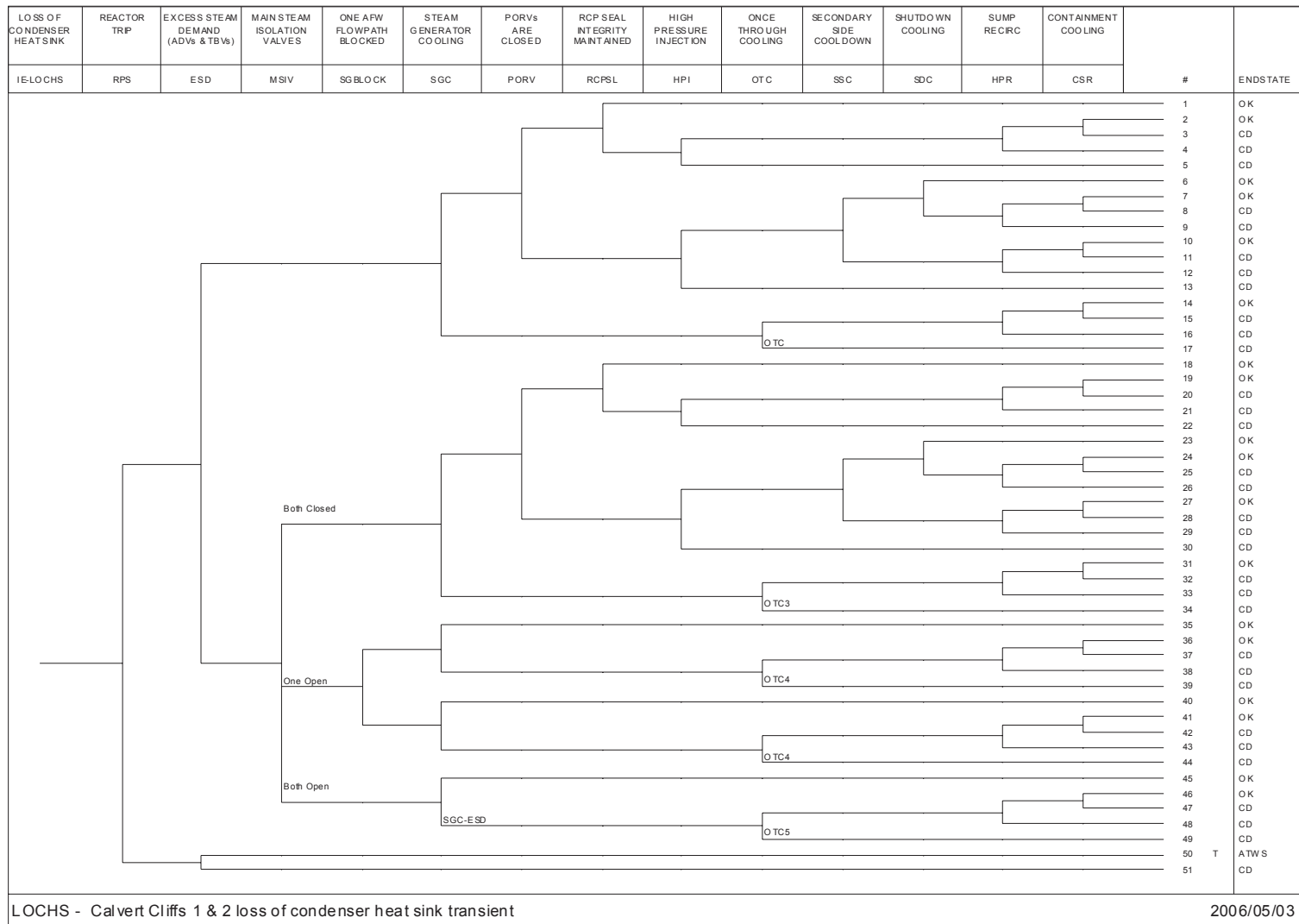


Figure 4. Event tree for loss of condenser heat sink transient.



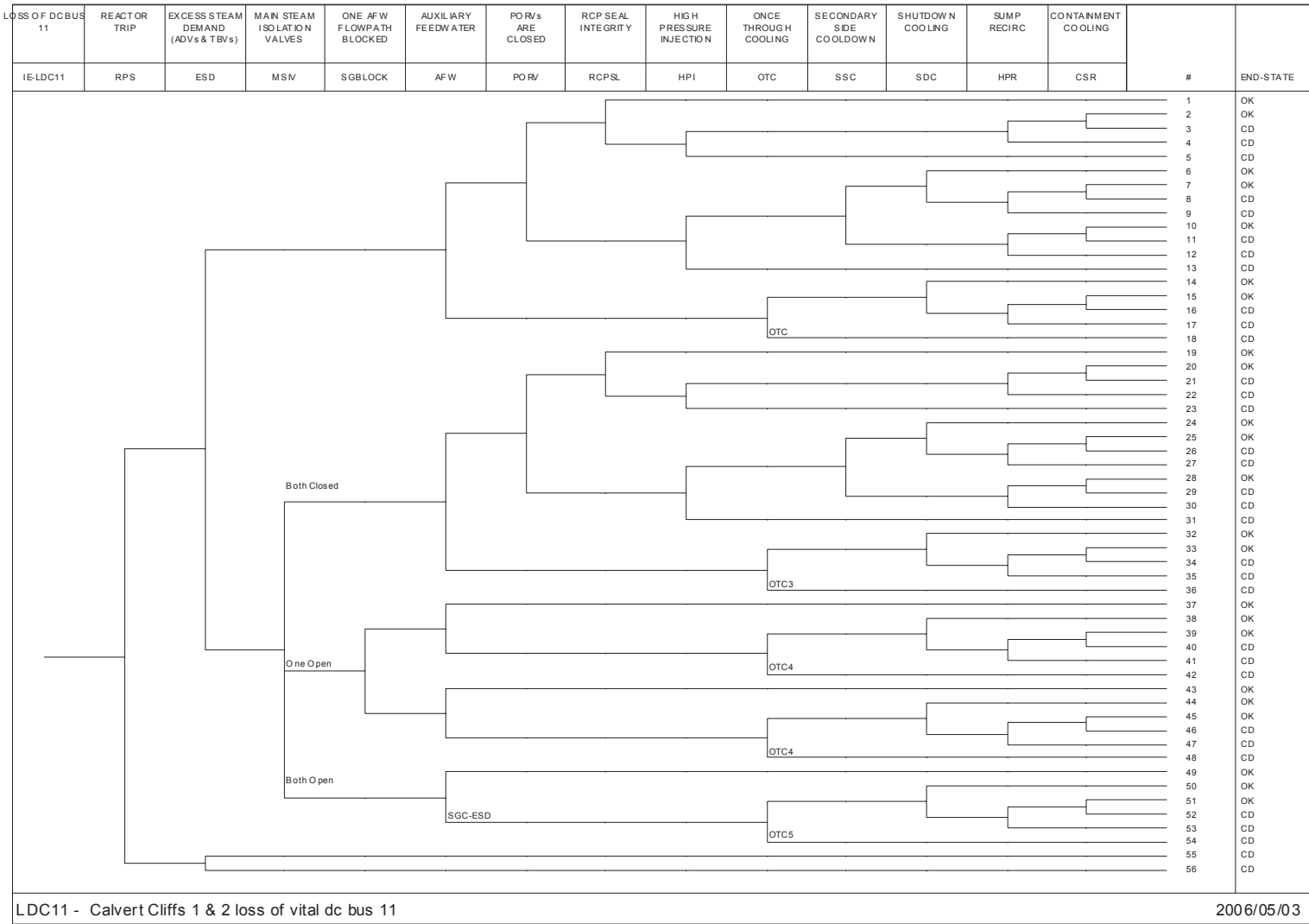


Figure 6. Event tree for loss of vital dc bus 11.



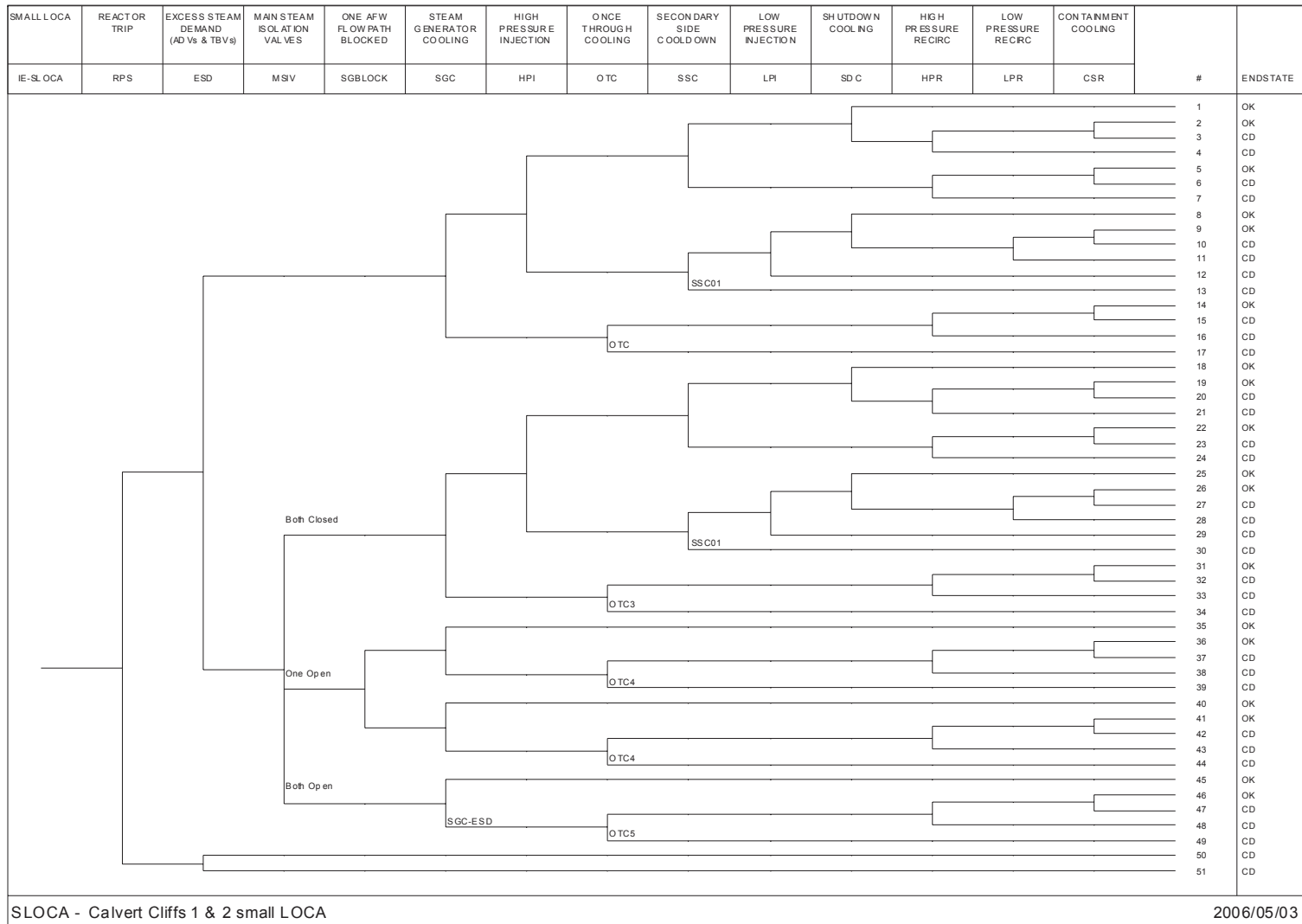


Figure 7. Event tree for small LOCA.

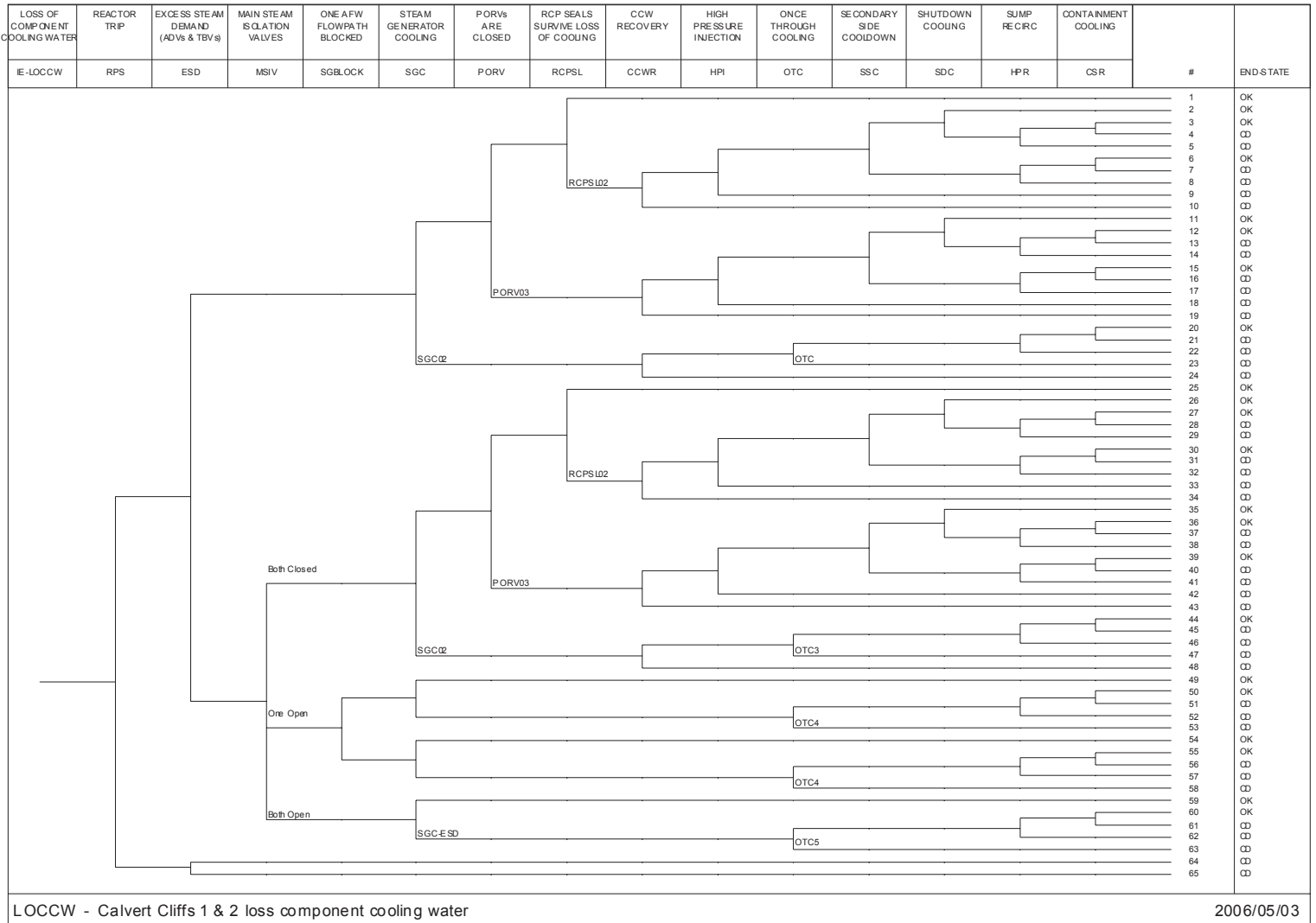


Figure 8. Event tree for loss of component cooling water.

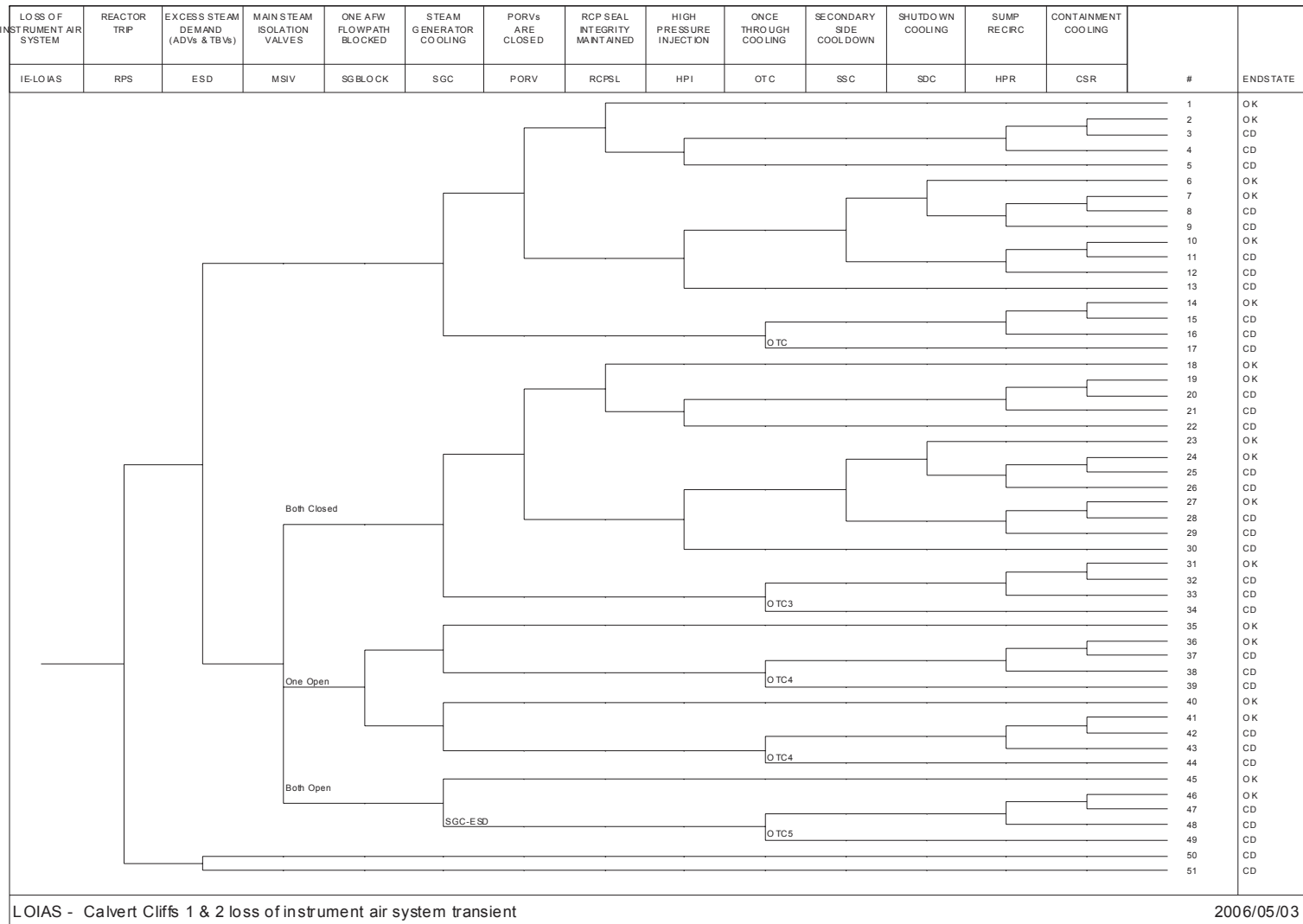


Figure 9. Event tree for loss of instrument air system transient.

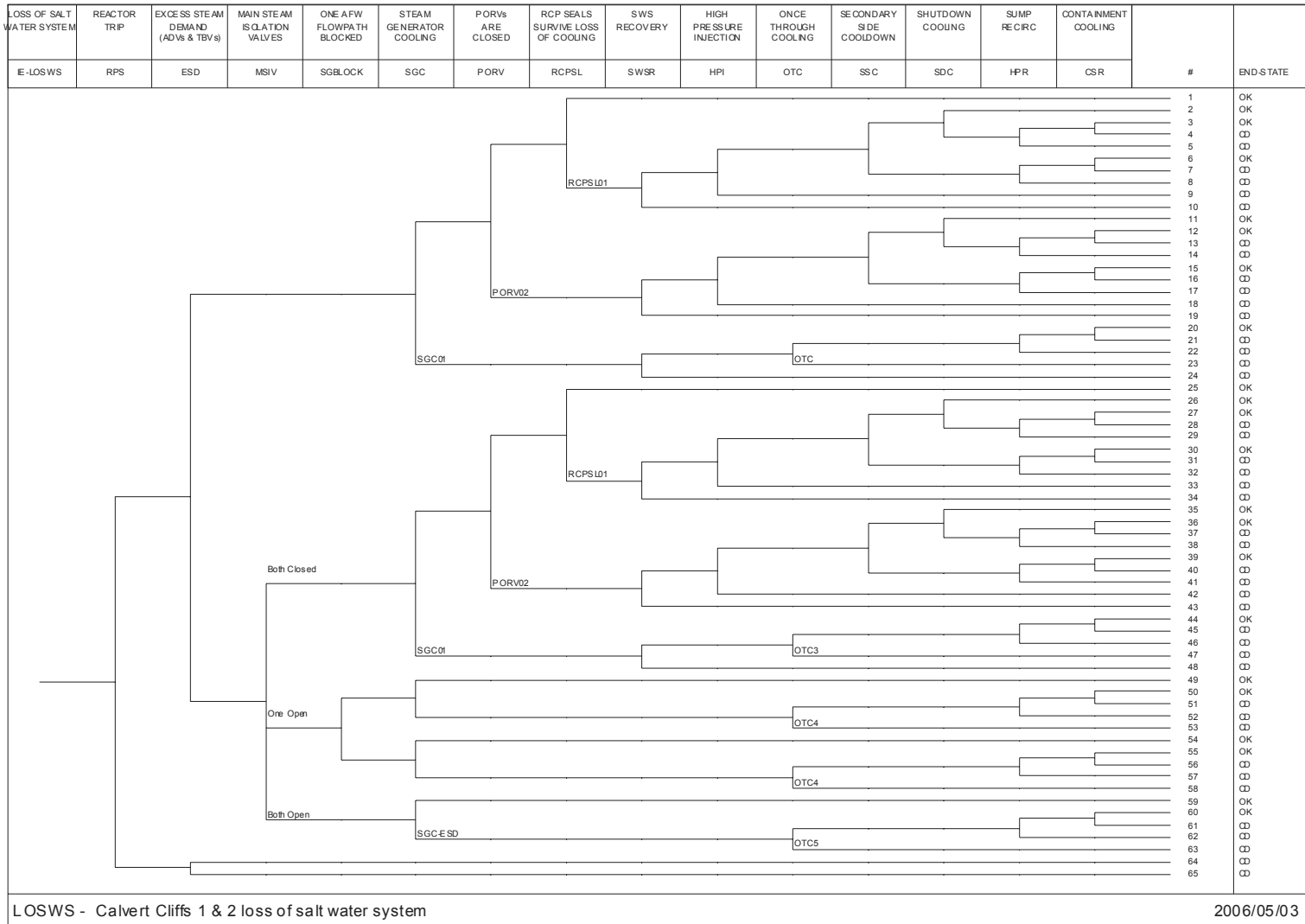


Figure 10. Event tree for loss of salt water system.

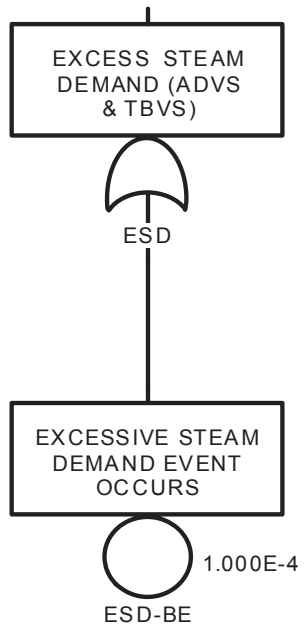


Figure 11. Fault tree for excess steam demand.

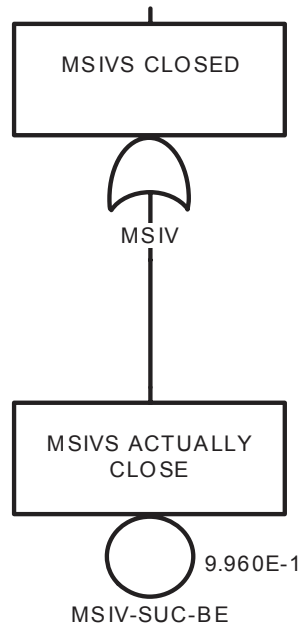


Figure 12. Fault tree for main steam isolation valves closed.

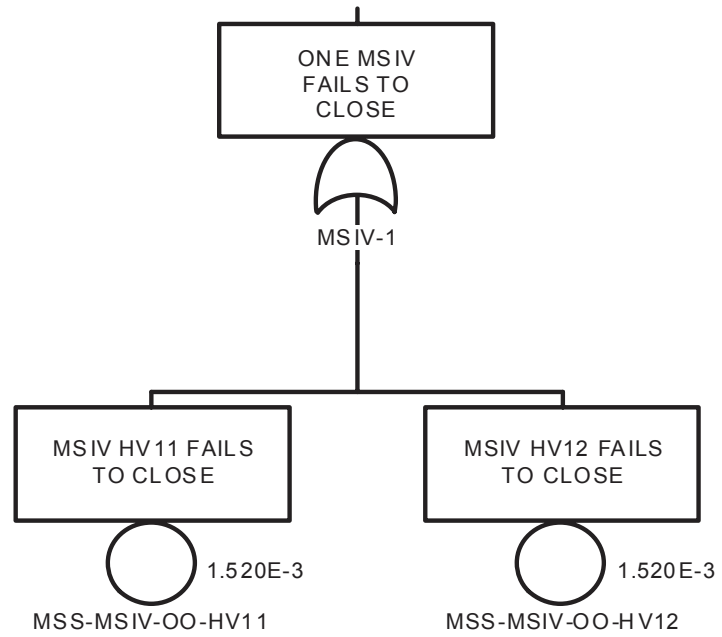


Figure 13. Fault tree for one MSIV closed.

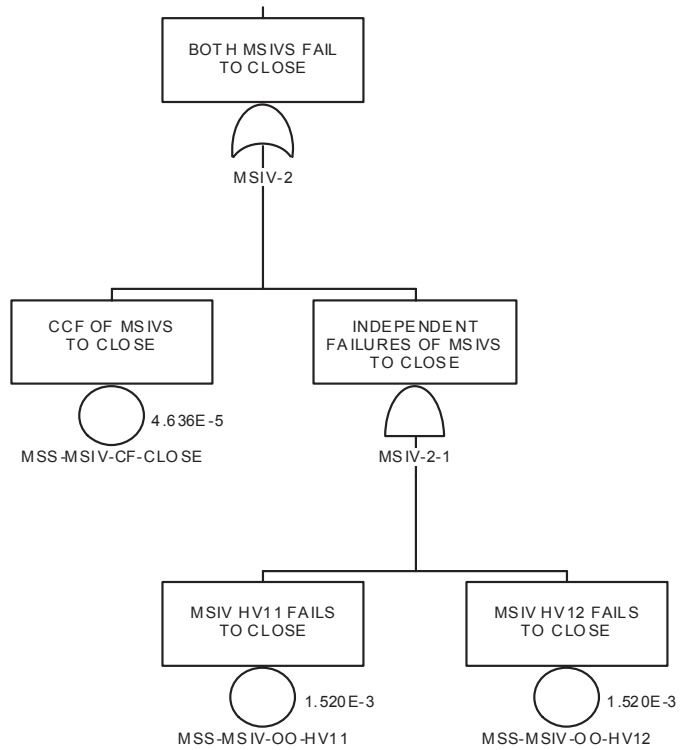


Figure 14. Fault tree for when both MSIVs fail to close.



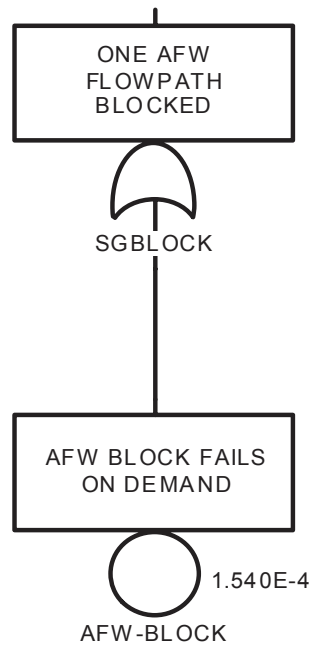


Figure 15. Fault tree for one AFW flow path blocked.

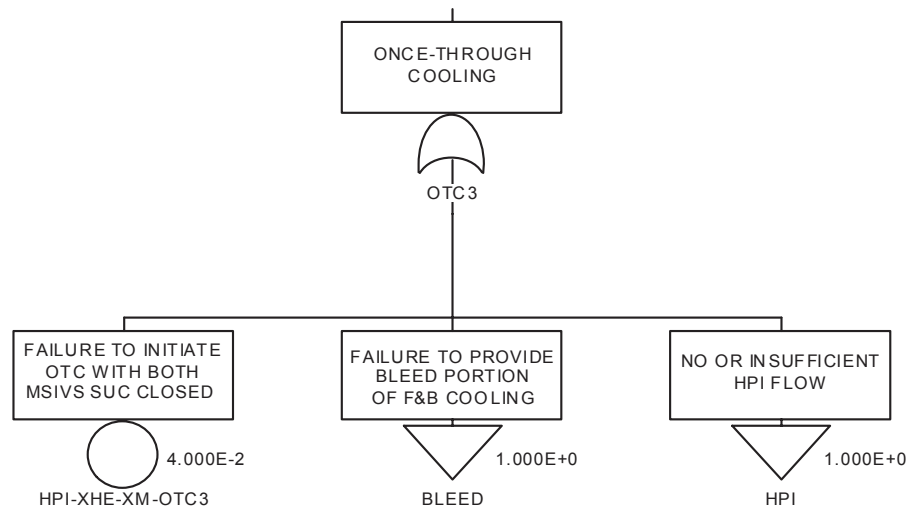


Figure 16. Fault tree for once-through cooling when both MSIVs close on demand.

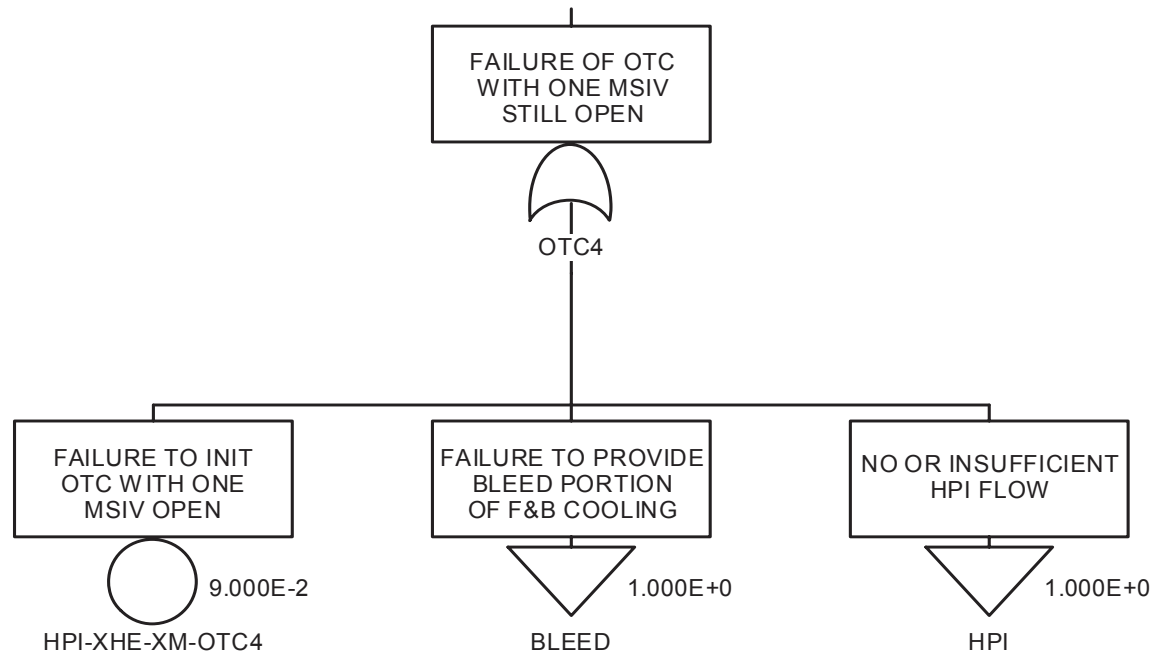


Figure 17. Fault tree for once-through cooling when only one MSIV closes on demand.

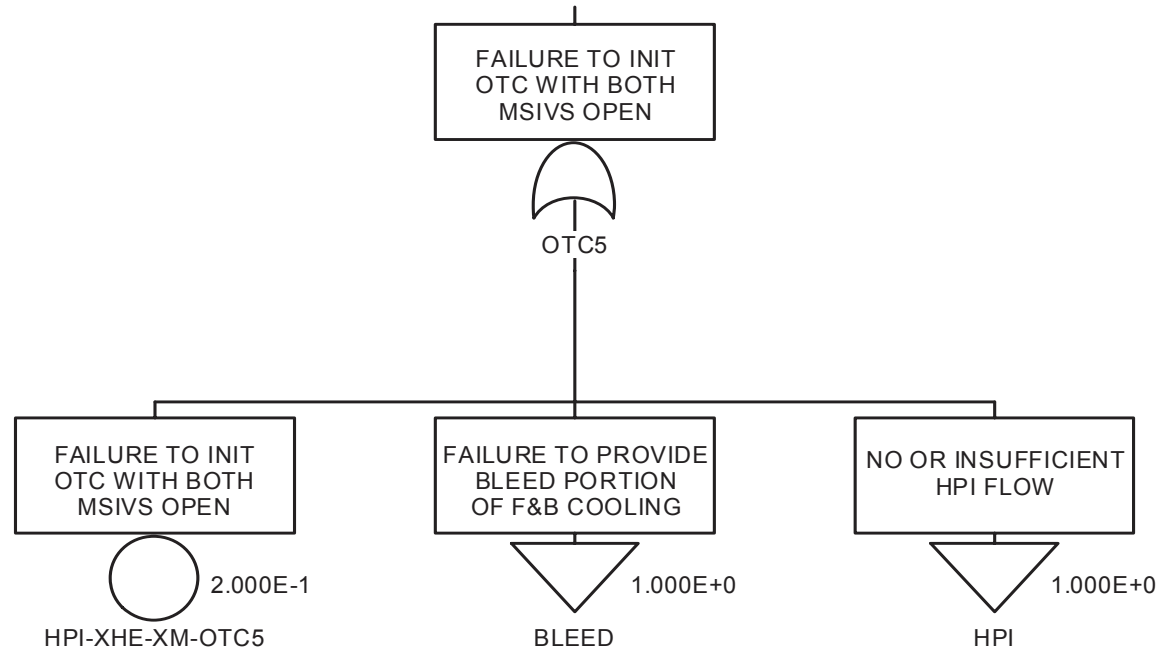


Figure 18. Fault tree for once-through cooling when both MSIVs fail to close on demand.

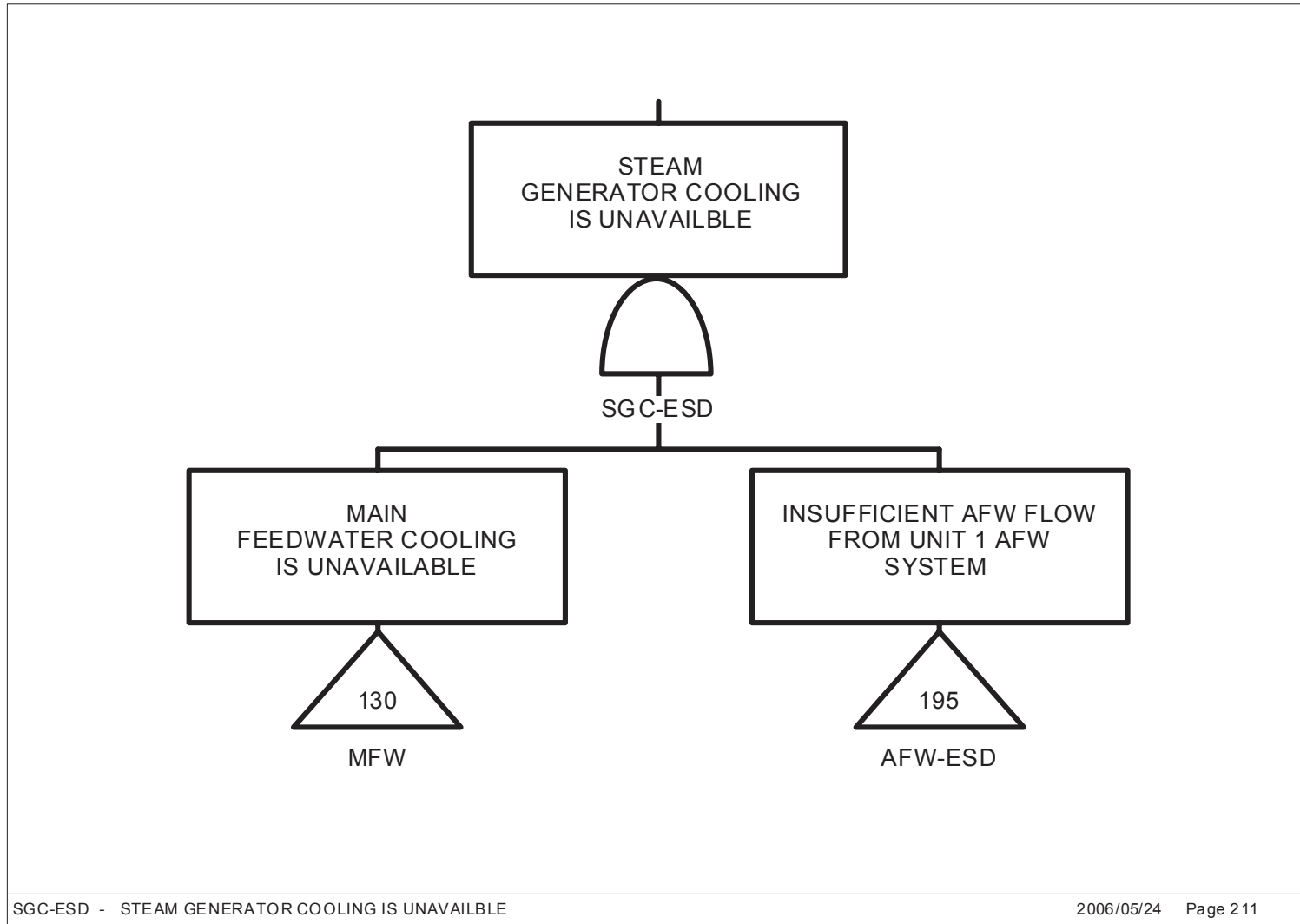


Figure 19. Fault tree for steam generator cooling.

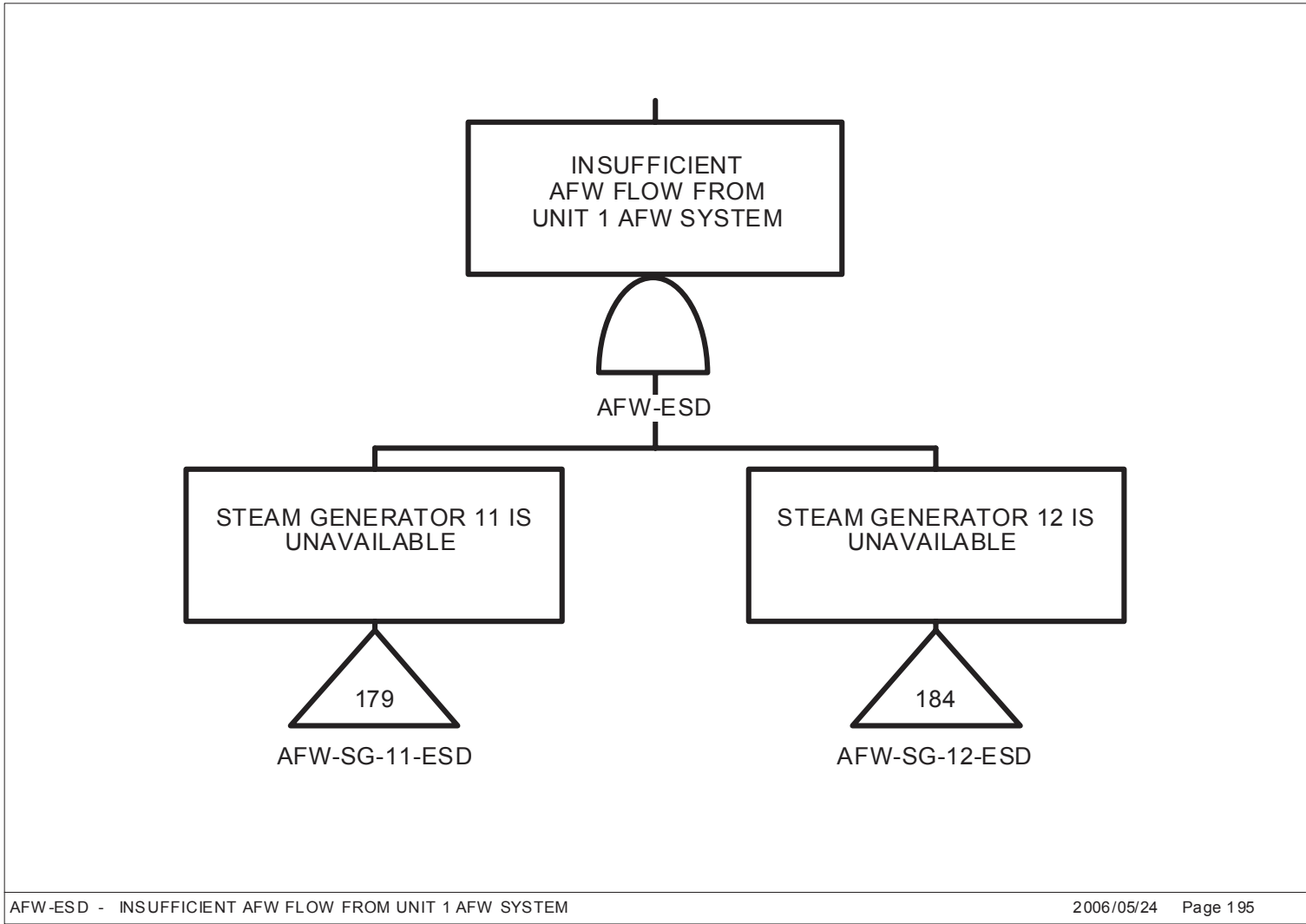


Figure 20. Fault tree for AFW flow from Unit 1 AFW system.



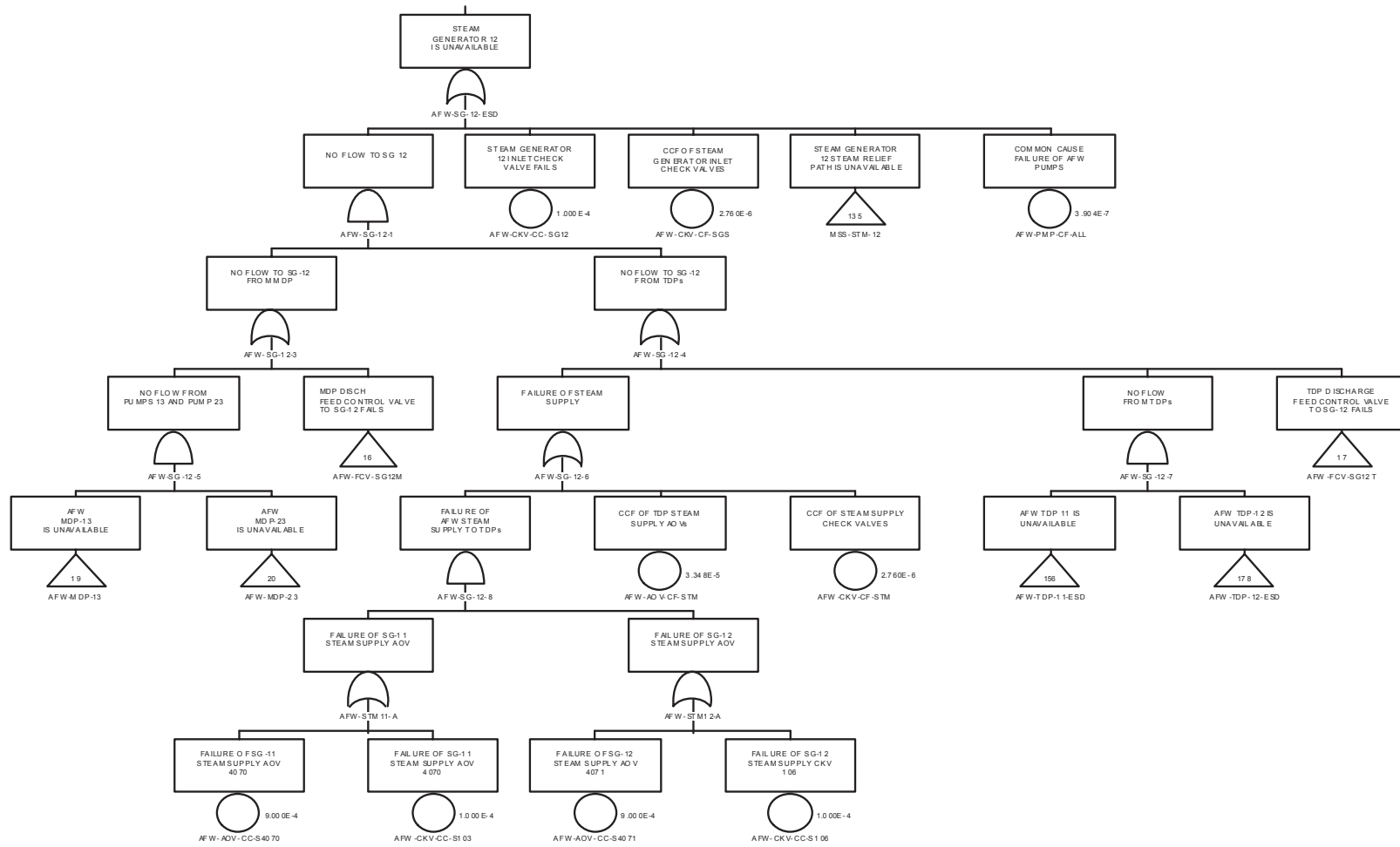


Figure 22. Fault tree for steam generator 12 cooling.





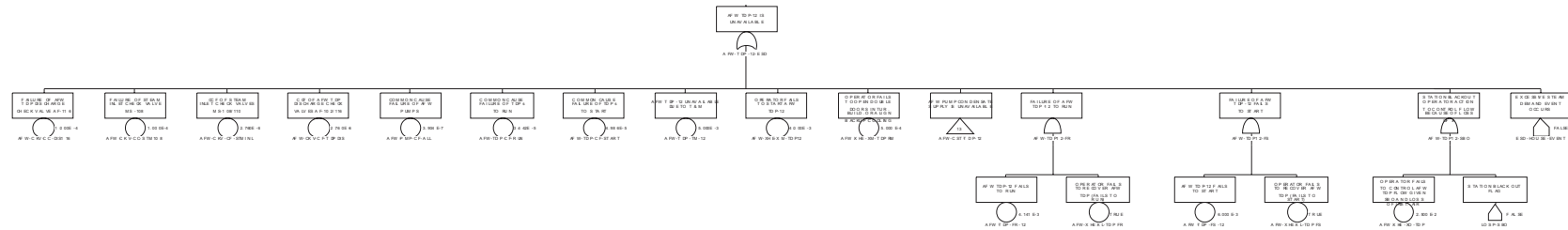


Figure 24. Fault tree for AFW TDP 12 flow.

# **Appendix C**

## **Plant Response to Excessive Steam Demand**

The preliminary event assessment was performed using a conservative assumption such that auxiliary feedwater (AFW) alone cannot provide sufficient steam generator (SG) cooling to prevent core damage in the following two cases of an excessive steam demand (ESD) event:

- 1) Both MSIVs fail to close upon Steam Generator Isolation Signals (SGIS), and
- 2) Only one MSIV succeeds to close upon SGIS.

In the first case, it was assumed that the ESD event is not recovered; namely, TBVs are not automatically closed by an interlock signal upon loss of condenser vacuum approximately half an hour into the transient due to failure of condenser air removal units on loss of service water as a result of Safety Injection Actuation Signals (SIAS), nor manually closed by the operators. In the second case, it was assumed that the AFW flow path to the affected SG is not properly blocked. Note that SG cooling by AFW and thereby prevention of core damage was credited in the preliminary event assessment, only in the case where the AFW flow path to the affected SG is properly blocked. The event assessment with the aforementioned conservative assumptions resulted in a conditional core damage probability (CCDP) of  $1.2 \times 10^{-5}$  (i.e., low yellow).

A peer review of this preliminary event assessment was conducted by Constellation Energy operating CCNPP.<sup>1</sup> During this review process, a simulator run was made with the quick open signal failing to clear and with the MSIVs failing to close on SGIS in order to evaluate plant response and operator actions. The simulation results (Figure C.1) indicate the following:

1. Upon receipt of Auxiliary Feedwater Actuation Signals (AFAS), all the AFW pumps were initially started. The turbine-driven AFW pumps functioned until steam pressure dropped to approximately 50 psia in the steam generators and they were secured at this point. Auxiliary feedwater flow, using the motor-driven AFW pump, was maintained during the entire transient after the AFAS actuation.
2. During the first 15~20 minutes into the transient, the High Pressure Safety Injection System (HPSI) provided significant flow into the Reactor Coolant System (RCS) following SIAS actuation.
3. The reactor core was not uncovered. There was an indication of lowering reactor coolant level as observed on the Reactor Vessel Level Monitoring System in the 5 to 12 minute time frame. At the lowest point, there was approximately 7 feet of water above the active fuel.
4. The RCS temperature leveled out above 350°F.
5. Pressure in the RCS leveled out at approximately 1000 psia. Pressure was controlled using operator actions to secure HPSI flow, charging flow, and pressurizer heaters. Auxiliary spray was also used to maintain pressure.

---

<sup>1</sup> Letter from Mr. J. A. Spina to NRC (Document Control Center), "Response to Preliminary Accident Sequence Precursor (ASP) Analysis for the Unit 2 January 2004 Operational Event," March 31, 2006.

6. For purposes of simulation, the TBVs remained open. However, the TBVs will be closed on a loss of condenser vacuum which is expected to take place about half an hour into the transient because the condenser air removal units will fail on loss of service water as a result of the SIAS generation, as mentioned earlier.

In short, the most important conclusion from the simulator run is that auxiliary feedwater can successfully prevent core uncover without once through cooling (OTC). However, the simulation results show that wide range SG level in both SGs drops to approximately -400 inches within the first 10 minutes into the transient and remains at this very low level for the entire time period shown by the results (i.e., ~30 minutes). Given the fact that auxiliary feedwater kept on injecting into the SGs and the core continuously cooled down, the water in the shell side of the SGs remaining at such a low level implies that the RCS heat was removed primarily by the injected AFW flashing into steam.

In view of a significance of properly understanding the plant behavior expected in the event of an excess steam demand, an independent thermal hydraulic (T/H) analysis was also performed using the Calvert Cliffs RELAP-5 model<sup>2</sup> for the following cases involving failure of both MSIVs upon SGIS:

- 1) Reactor/turbine trip with stuck-opening of MSIVs, TBVs and ADVs (all valves)
- 2) Reactor/turbine trip with stuck-opening of MSIVs, TBVs and ADVs (all valves) and a single Safety Relief Valve (SRV) in each SG
- 3) Reactor/turbine trip with stuck-opening of MSIVs, TBVs and ADVs (all valves) and all SRVs in each SG

In the first case (Figure C.2), the water level drops to a minimum of about -320 inches and AFW is able to recover SG water level. In the second case, the water level drops to a minimum of about -370 inches and again, AFW is able to recover SG water level. Finally, in case 3, the water level drops completely (no water left in the SGs) and again, AFW is able to recover SG water level, establishing SG cooling and consequently preventing core damage. Hence, the independent T/H analysis also points out that AFW (300 gpm per SG) can recover SG level because the primary water is relatively cool due to the RCS overcooling caused by the ESD and the declining decay heat.

Note that there are several discrepancies between the simulator runs and the RELAP-5 runs, among others:

- The SG level drops below -350 inches (a triggering condition for OTC in the emergency operating procedures) within 10 minutes according to the simulator run; however, the RELAP-5 run (the first case) shows that the SG level decreases only down to -320 inches in about 15 minutes into the transient.

---

<sup>2</sup> The RELAP-5 model for Calvert Cliffs, originally developed in the early 1980s by EG&G Idaho, was updated in 2001 as part of the NRC's Pressurized Thermal Shock (PTS) Rebaselining Study to reflect the current plant configurations and operating procedures, including system setpoints and control logic.

- The SG level is recovered by AFW after ~45 minutes as per the RELAP-5 run, but levels out at approximately -400 inches as per the simulator run.

In spite of these differences in the SG level prediction, both T/H analyses (i.e., by the plant simulator and the independent RELAP-5 model) conclude that AFW can prevent core damage without OTC. Therefore, the updated event assessment presented herein was carried out taking into account this conclusion.

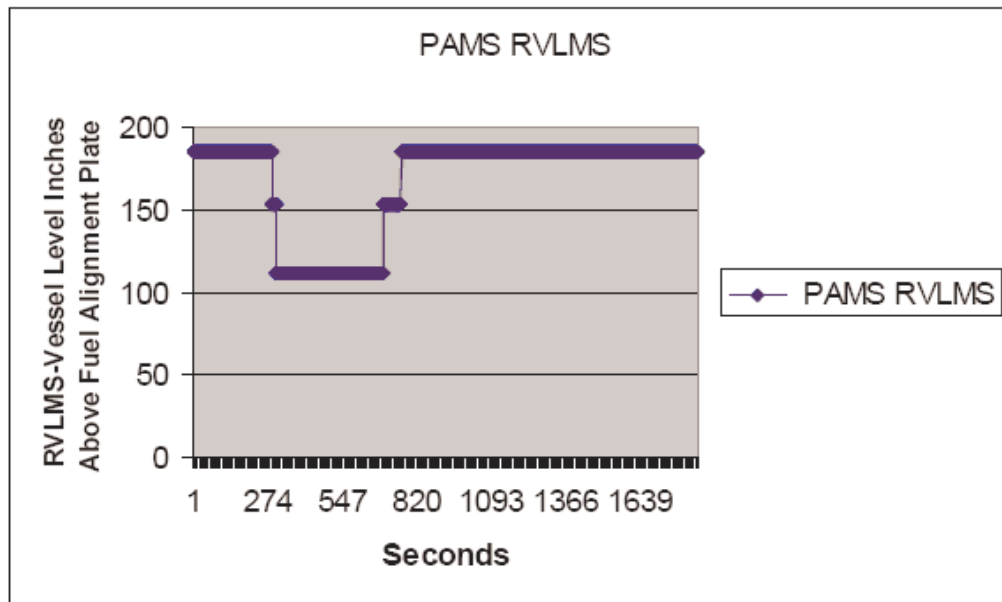
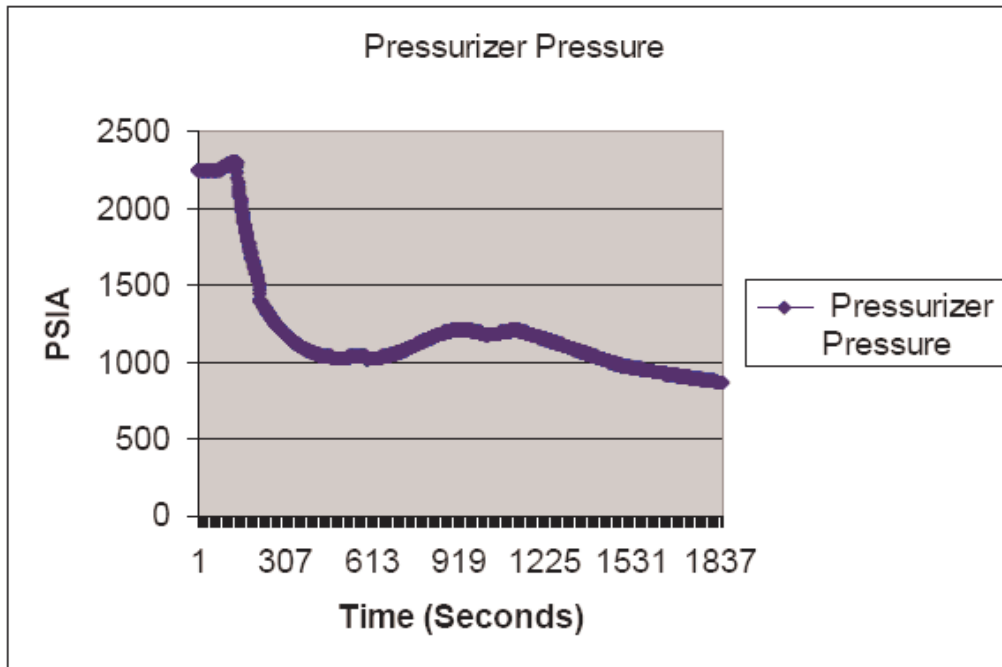


Figure C.1 Simulator run for excessive steam demand with both MSIVs failing to close

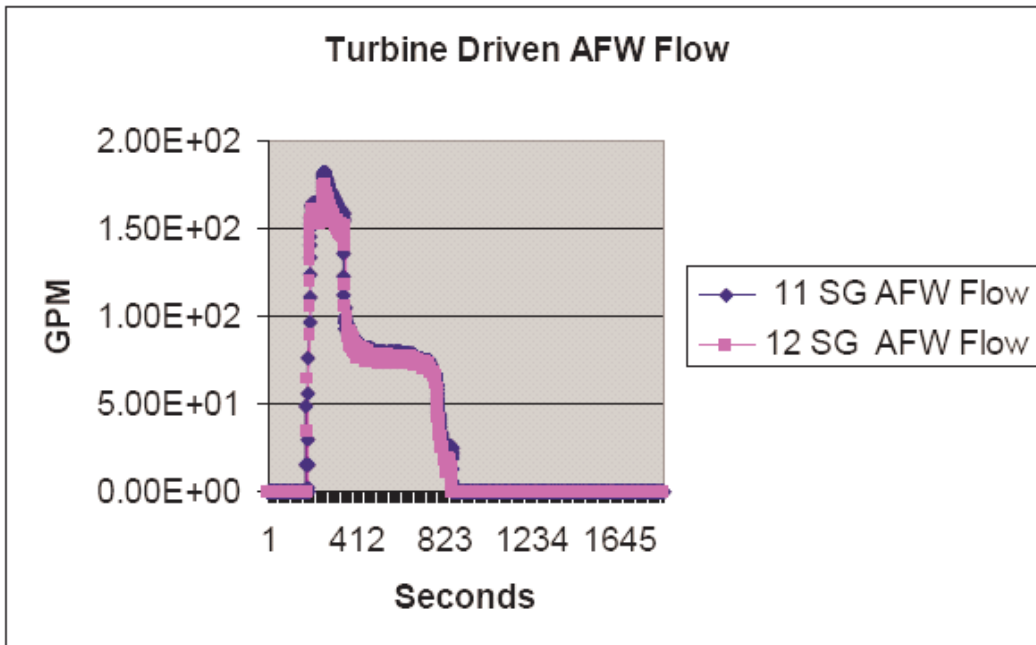
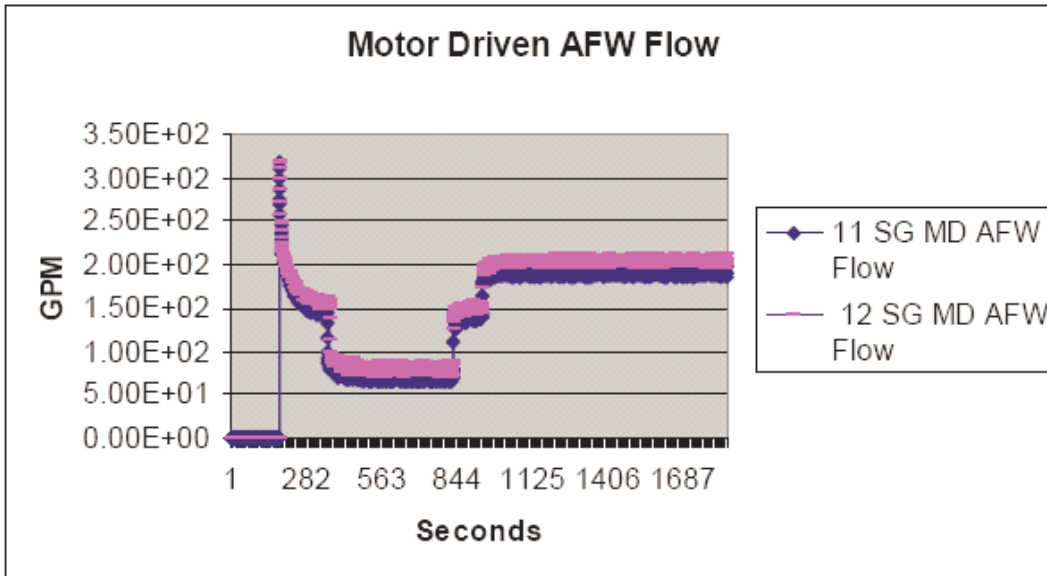


Figure C.1 (Cont'd)



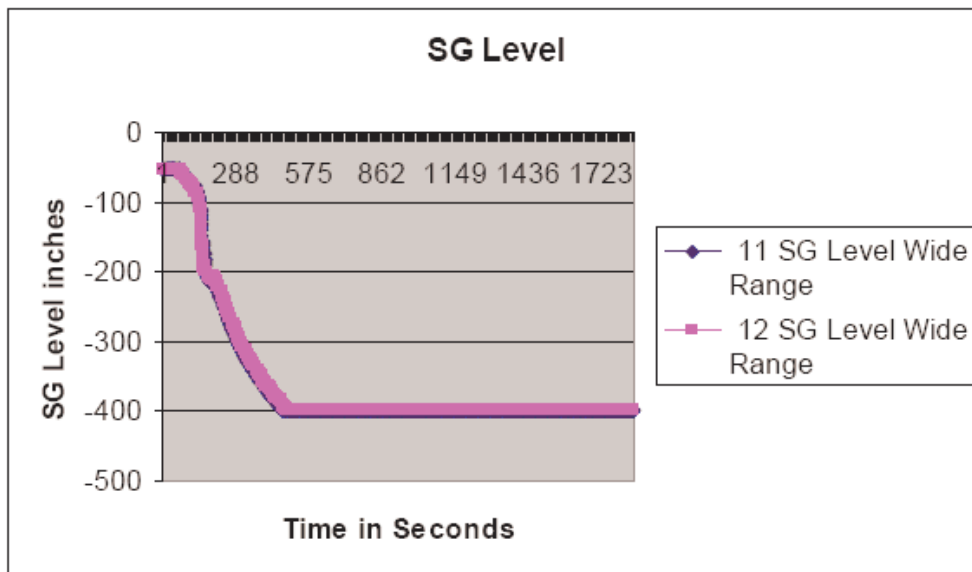
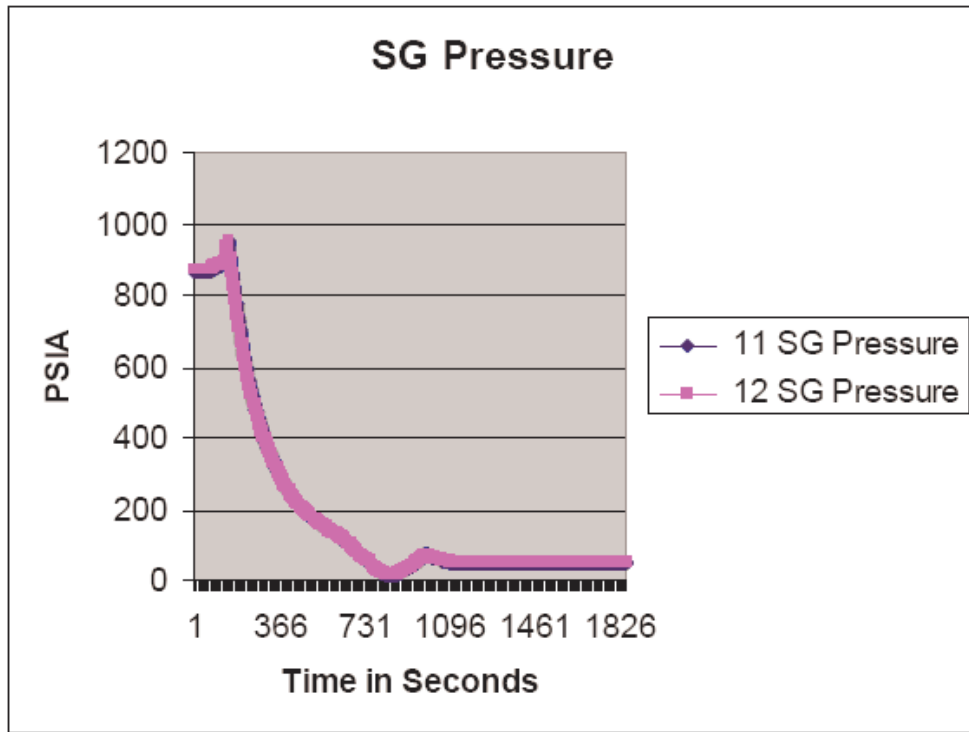


Figure C.1 (Cont'd)

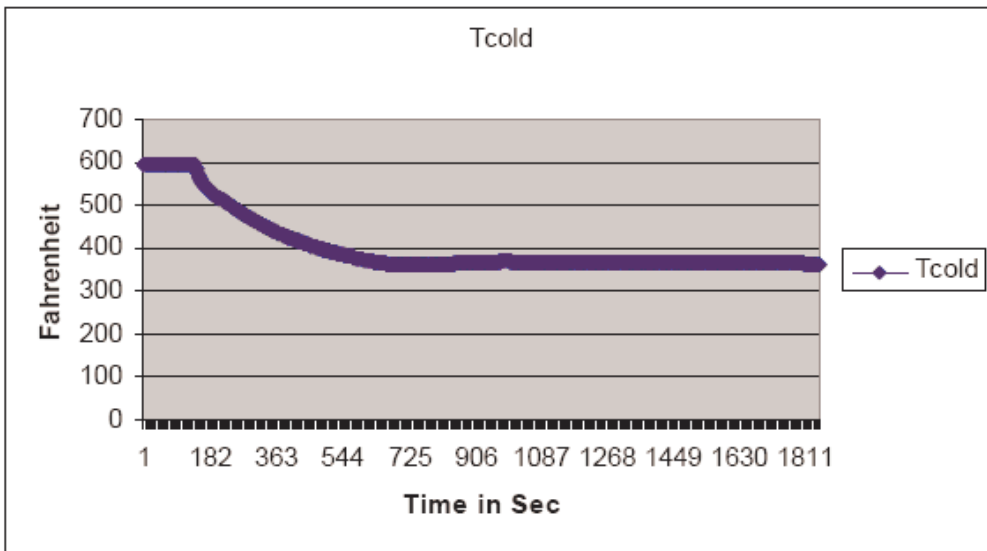
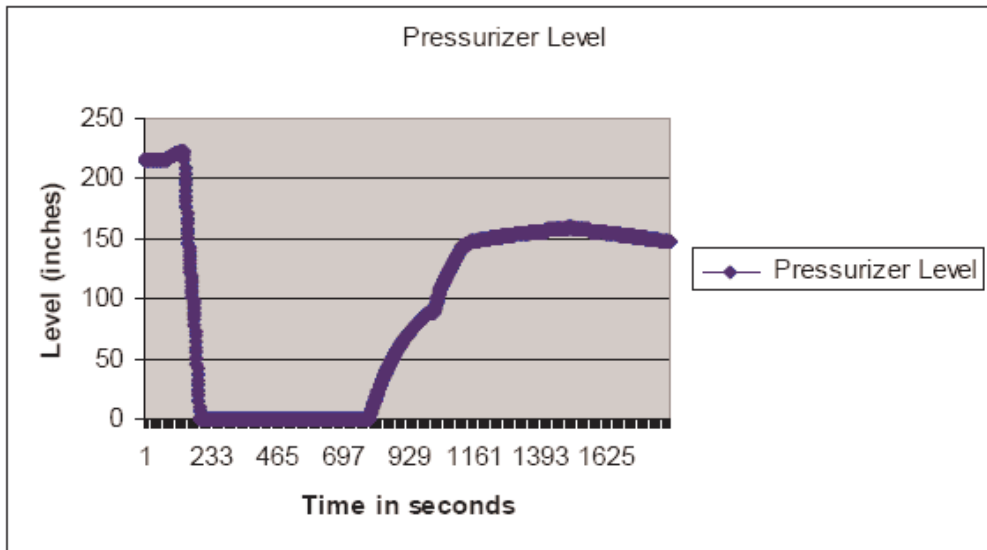


Figure C.1 (Cont'd)

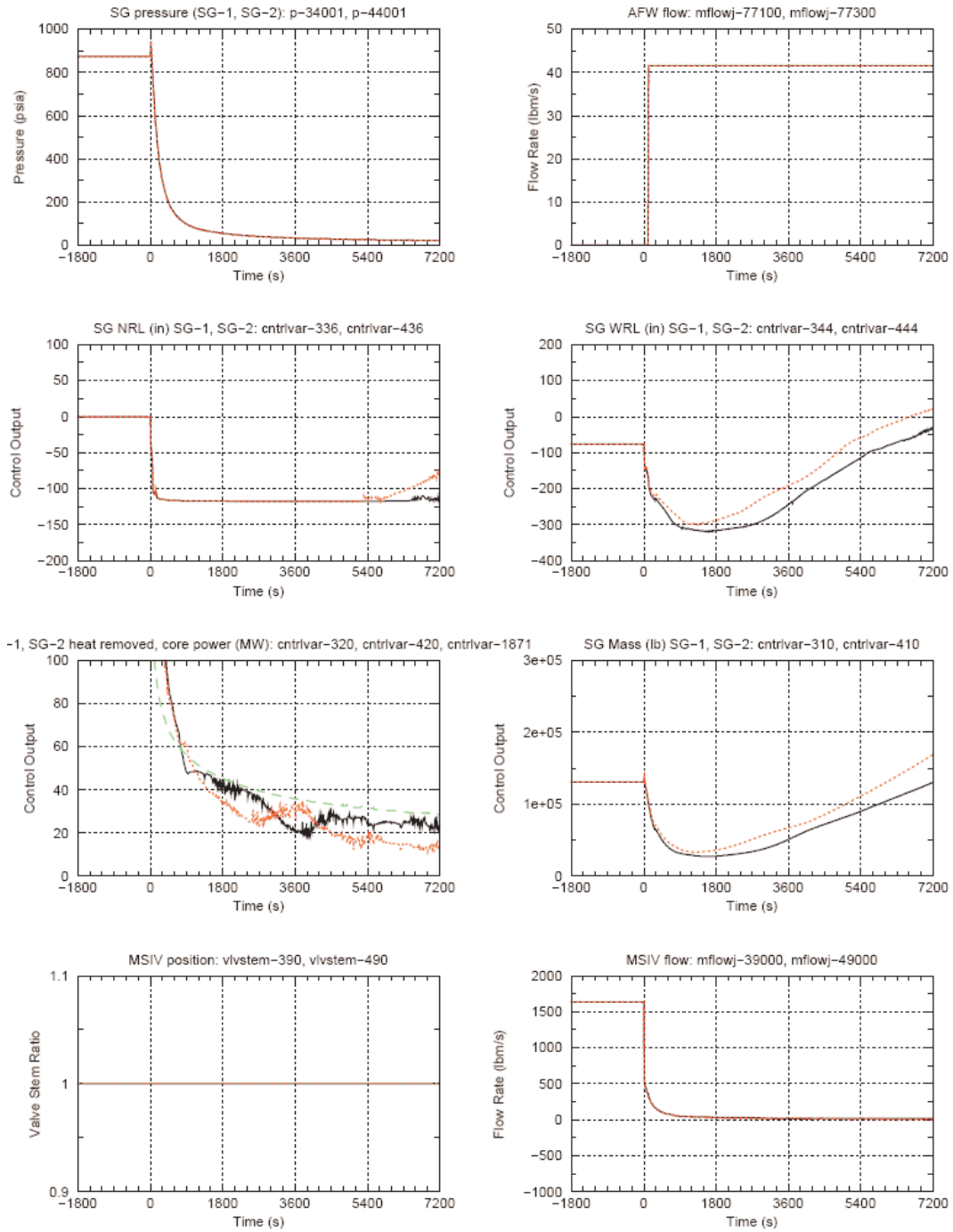


Figure C.2 RELAP-5 run for excessive steam demand with both MSIVs failing to close

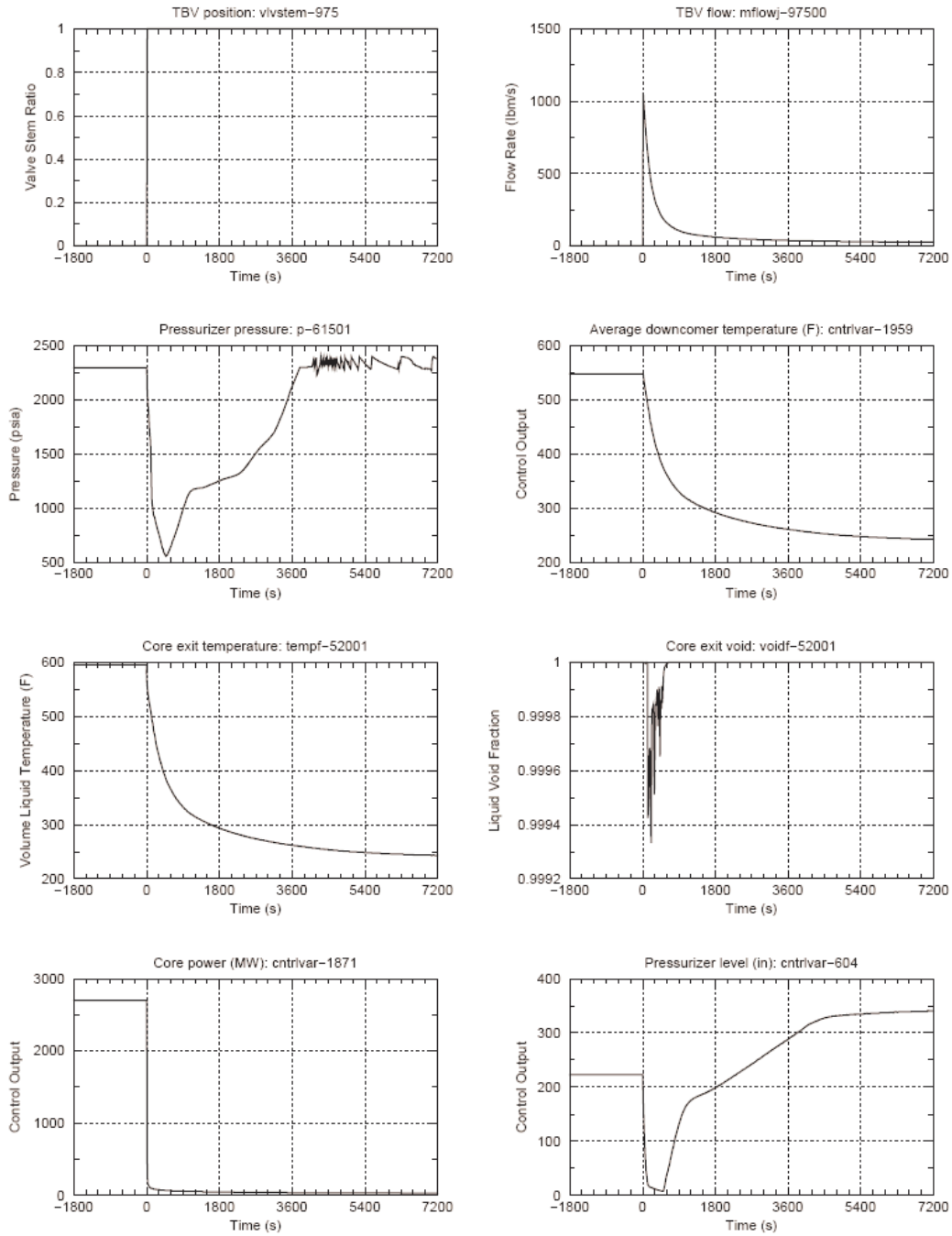


Figure C.2 (Cont'd)

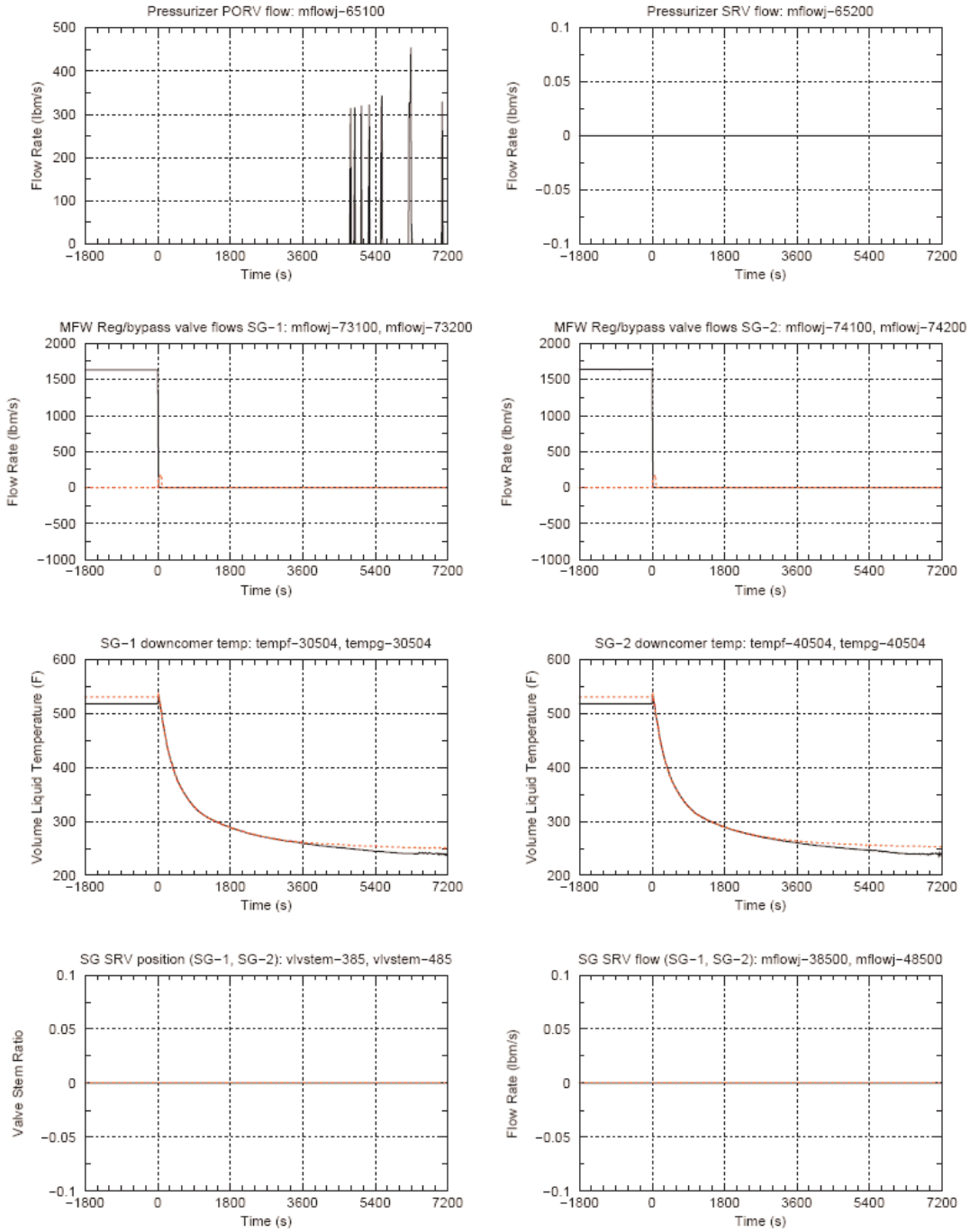


Figure C.2 (Cont'd)

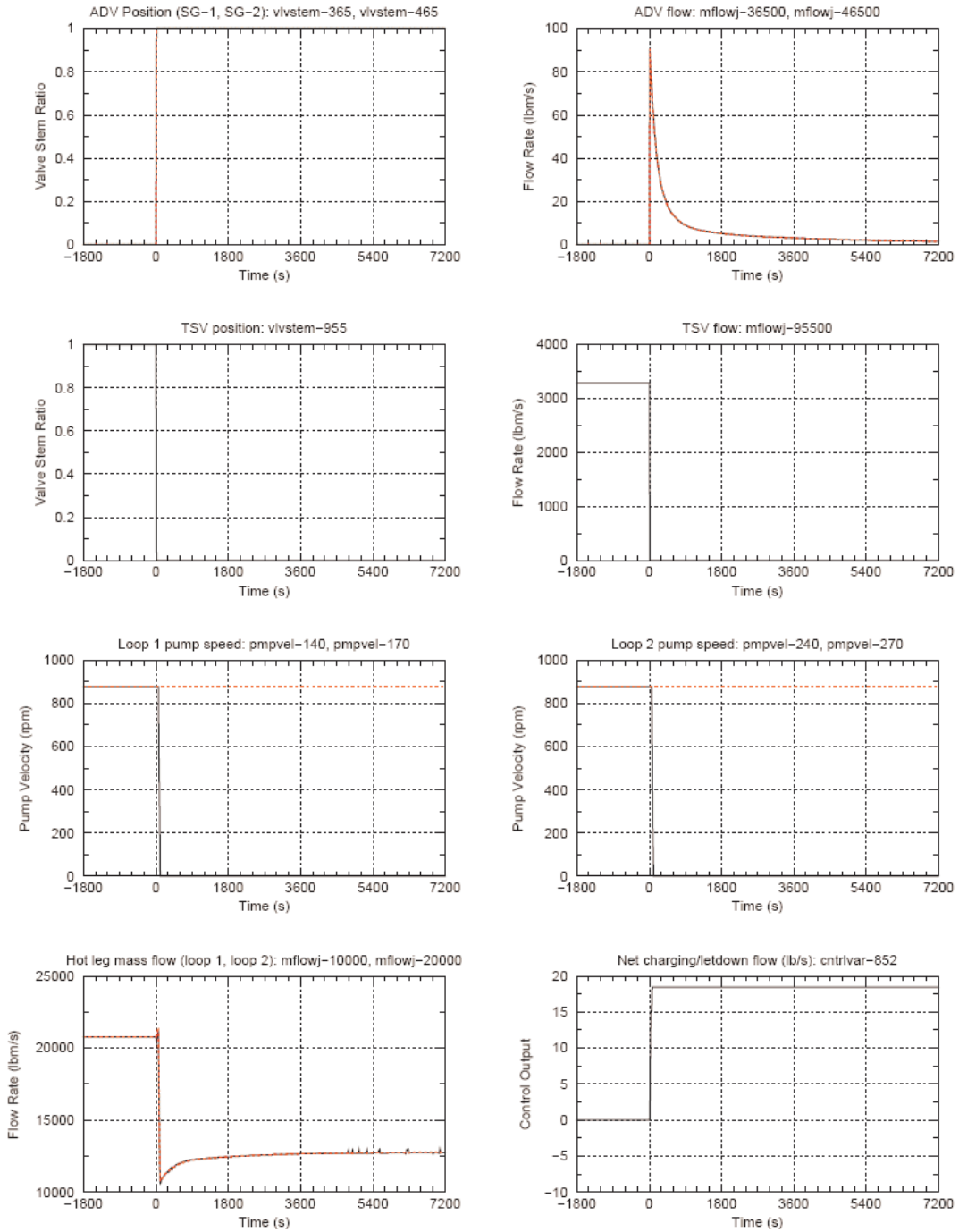


Figure C.2 (Cont'd)

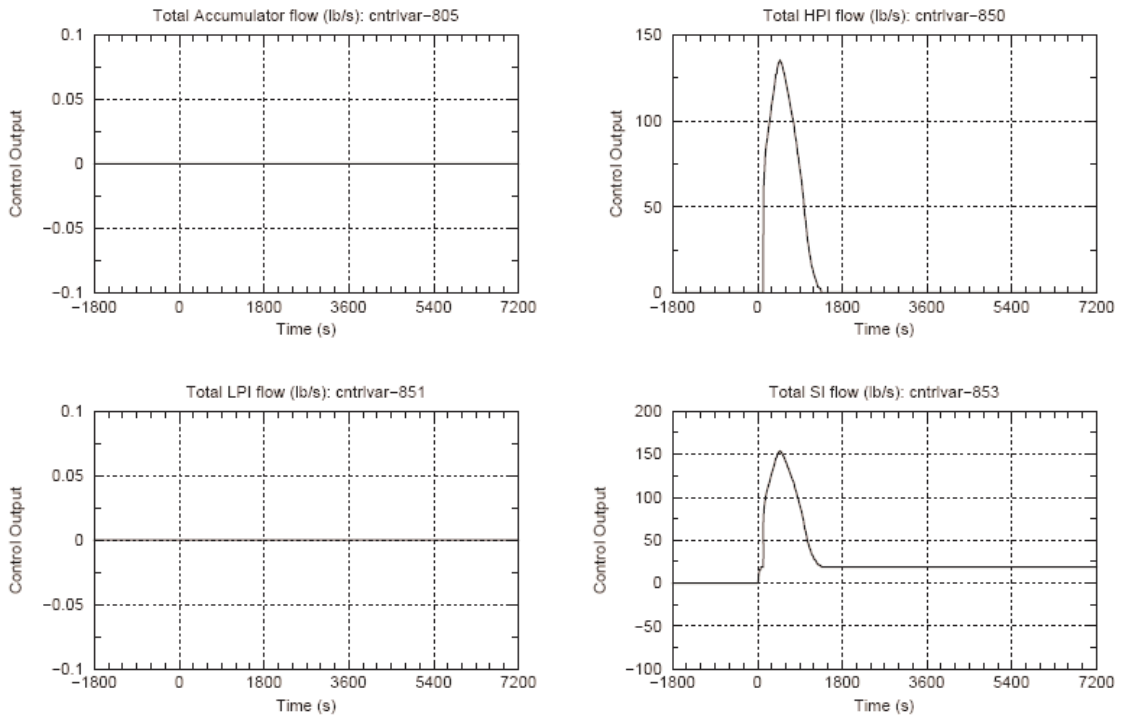


Figure C.2 (Cont'd)

# **Appendix D**

## **Human Performance Modeling**



The event assessment necessitates evaluating the human actions required to initiate once through cooling (OTC) under various circumstances relevant to the MSIV performance upon actuation of Steam Generator Isolation Signals (SGIS): 1) both MSIVs succeed to close, 2) only one MSIV succeeds to close, and 3) both MSIVs fail to close. The corresponding human actions are modeled in terms of human error events HPI-XHE-XM-OTC3,<sup>1</sup> HPI-XHE-XM-OTC4, and HPI-XHE-XM-OTC5, respectively.

It was assumed in evaluating these human error events that a significant amount of diagnosis activity would not be required for the operators to identify the need to initiate OTC, because the operators are typically familiar with the requirement of emergency operating procedures (EOPs) such that OTC should be initiated when wide range SG level in both SGs reaches -350 inches or the RCS cold leg temperature (i.e.,  $T_c$ ) rises uncontrollably 5 °F or greater<sup>2</sup>.

A summary of the human performance evaluation is provided in Table D.1 with the quantified human error probabilities (HEPs) in the last column. More details can be found in the SPAR-H worksheets of this appendix.

Table D.1 shows that three different types of performance shaping factors (i.e., time, stress, and complexity) were adjusted to capture the increased failure probability for the OTC human actions. In particular, it may be noted that higher complexity was applied to actions HPI-XHE-XM-OTC4 and HPI-XHE-XM-OTC5 as compared to action HPI-XHE-XM-OTC3; the reason is discussed below.

Human factors and procedural issues were identified at Calvert Cliffs during the inspection for the excess steam demand event. In particular, the inspection report<sup>3</sup> indicates that:

“Calvert Cliffs has increased the time allowed to execute EOP-0, to allow the operators to concurrently implement procedure steps from other EOPs, without executing the entire EOP. Calvert Cliffs allows this practice while in EOP-0, so that key plant parameters can be restored to normal operating bands. This philosophy resulted in the operators performing actions using knowledge-based skills as opposed to procedure-base skills during high stress condition. This practice significantly increased the potential for operator errors, and in the case of the January 23, 2004 event, it resulted in improper transitions in the EOP procedures.”

---

<sup>1</sup> HPI-XHE-XM-OTC3 is similar to human error event HPI-XHE-XM-FB (Operator fails to initiate feed and bleed cooling) in the original SPAR model for CCNPP which assumes that an excessive steam demand event does not occur. Because both MSIVs will close upon the SGIS within about 2-3 minutes following the ESD, the human performance requirements for HPI-XHE-XM-OTC3 and HPI-XHE-XM-FB are considered to be almost identical (i.e., the same performance shaping factors for both cases), and as a result, the same human error probability was estimated for these human actions.

<sup>2</sup> Example EOPs requiring OTC include: 1) Contingency Action 31.1 in the HR-1 Functional Recovery Guideline, 2) Contingency Action 9.1 in the Loss of All Feedwater Recovery Guideline, and 3) Contingency Action 19.1 in the Excess Steam Demand Recovery Guideline.

<sup>3</sup> NRC Special Inspection (SI) Team Report, EA-04110, “Calvert Cliffs Nuclear Power Plant, Unit 1 and Unit 2 - NRC Inspection Report 05000317/2004008 and 05000318/2004008,” July 29, 2004.

Especially because of the operational practice which was in place at Calvert Cliffs during the event (i.e., performing actions using knowledge-based skills as opposed to procedure-based skills), actions HPI-XHE-XM-OTC4 and HPI-XHE-XM-OTC5 for the cases where at least one MSIV failed to close are expected to be more difficult to perform, as compared to action HPI-XHE-XM-OTC3 for the case where both MSIVs successfully closed upon SGIS.

In addition, actions HPI-XHE-XM-OTC4 and HPI-XHE-XM-OTC5 are determined to be more complex than action HPI-XHE-XM-OTC3 to perform particularly because of multiple faults, multiple equipment unavailable, and more likelihood of parallel tasks and transitioning between multiple procedures due to an increased possibility of not satisfying safety functions (see Section 2.4.4.3 of the SPAR-H report<sup>4</sup>).

Finally, it is also notable that the OTC human actions were modeled as not requiring a significant amount of diagnosis activity even though the Calvert Cliffs Unit 2 operators actually mis-diagnosed plant conditions during their response to the ESD event, because:

- a) The term diagnosis in the SPAR-H method generally has to do with attributing the most likely causes of the abnormal event to the level required to identify those systems or components whose status can be changed to reduce or eliminate the problem.
- b) The operators mis-diagnosed the actual plant conditions; however, this mis-diagnosis relates to not the OTC human actions, but other actions to return the key plant parameters to normal operating bands.
- c) In the actual event, the operators did not need to diagnose in connection with OTC, since the OTC operation was not required due to the early termination of the ESD by the automatic closure of both MSIVs about one minute after the reactor trip, and the subsequent SG cooling by the motor-driven AFW pump and the ADVs.

---

<sup>4</sup> Idaho National Engineering and Environmental Laboratory, "The SPAR-H Human Reliability Analysis Method," INEEL/EXT-02-01307, May 2004.

Table D.1 Summary of human performance evaluation

HUMAN ERROR EVENT	Description	Performance Shaping Factors (PSFs)								HEP
		Time	Stress	Complexity	Experience	Procedure	Ergonomics	Fitness	Work Process	
HPI-XHE-XM-OTC3	Operator fails to initiate once through cooling (given excessive steam demand and both MSIVs succeed to close upon SGIS)	10	2	2	1	1	1	1	1	4.0E-02
HPI-XHE-XM-OTC4	Operator fails to initiate once through cooling (given excessive steam demand and only one MSIV closes upon SGIS)	10	2	5	1	1	1	1	1	9.0E-02
HPI-XHE-XM-OTC5	Operator fails to initiate once through cooling (given excessive steam demand and both MSIVs fail to close upon SGIS)	10	5	5	1	1	1	1	1	2.0E-01

Note: Each of these human error events involves multiple (i.e., 3 or more) non-nominal PSFs, and therefore, the human error probabilities (HEPs) were calculated by applying an adjustment factor in accordance to the formula provided in the SPAR-H report in order to represent the composite PSF influence.

## SPAR Model Human Error Worksheet (Page 1 of 3)

Plant: Calvert Cliffs 1 & 2 Event Name: HPI-XHE-XM-OTC3Task Error Description: Operator fails to initiate once through cooling (given excessive steam demand and both MSIVs succeed to close upon SGIS)Does this task contain a significant amount of diagnosis activity? YES  NO 

If Yes, Use Table 1 below to evaluate the PSFs for the Diagnosis portion of the task before going to Table 2. If No, go directly to Table 2.

Table 1. Diagnosis worksheet.

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	
	Barely adequate < 20 m	10	
	Nominal ≈ 30 m	1	
	Extra > 60 m	0.1	
	Expansive > 24 h	0.01	
2. Stress	Extreme	5	
	High	2	
	Nominal	1	
3. Complexity	Highly	5	
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	10	
	Nominal	1	
	High	0.5	
5. Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1	
	Diagnostic/symptom oriented	0.5	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
	Nominal	1	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1	
8. Work Processes	Poor	2	
	Nominal	1	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

### SPAR Model Human Error Worksheet (Page 2 of 3)

**Table 2.** Action worksheet.

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	It is assumed there is just enough available time for the operators to initiate feed and bleed cooling.
	Time available $\approx$ time required	10✓	
	Nominal	1	
	Available > 50x time required	0.01	
2. Stress	Extreme	5	It is assumed that the stress level is greater than nominal.
	High	2✓	
	Nominal	1	
3. Complexity	Highly	5	It is assumed that the complexity level is greater than nominal.
	Moderately	2✓	
	Nominal	1	
4. Experience/ Training	Low	3	
	Nominal	1✓	
	High	0.5	
5. Procedures	Not available	50	

	Available, but poor	5	
	Nominal	1✓	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1✓	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1✓	
8. Work Processes	Poor	2	
	Nominal	1✓	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

**Table 3.** Task failure probability without formal dependence worksheet.

Task Portion	Nom. Prob.	Time	Stress	Compl.	Exper./ Train.	Proced.	Ergon.	Fitness	Work Process	Prob.
Diag.										N/A
Action	1.0E-3	x 10	x 2.0	x 2.0	x 1.0	x 1.0	x 1.0	x 1.0	x 1.0	4.0E-2 <sup>a</sup>
Total										4.0E-2

a. The human error probability was adjusted following a special formula of SPAR-H to represent the composite PSF influence, because multiple (i.e., three or more) non-nominal PSFs are involved .

**SPAR Model Human Error Worksheet (Page 3 of 3)**

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence.



## SPAR Model Human Error Worksheet (Page 1 of 3)

Plant: Calvert Cliffs 1 & 2 Event Name: HPI-XHE-XM-OTC4Task Error Description: Operator fails to initiate once through cooling (given excessive steam demand and only one MSIV closes upon SGIS)Does this task contain a significant amount of diagnosis activity? YES  NO 

If Yes, Use Table 1 below to evaluate the PSFs for the Diagnosis portion of the task before going to Table 2. If No, go directly to Table 2.

Table 1. Diagnosis worksheet.

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	
	Barely adequate < 20 m	10	
	Nominal ≈ 30 m	1	
	Extra > 60 m	0.1	
	Expansive > 24 h	0.01	
2. Stress	Extreme	5	
	High	2	
	Nominal	1	
3. Complexity	Highly	5	
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	10	
	Nominal	1	
	High	0.5	
5. Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1	
	Diagnostic/symptom oriented	0.5	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	



PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
	Nominal	1	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1	
8. Work Processes	Poor	2	
	Nominal	1	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

### SPAR Model Human Error Worksheet (Page 2 of 3)

**Table 2.** Action worksheet.

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	It is assumed there is just enough available time for the operators to initiate feed and bleed cooling.
	Time available $\approx$ time required	10✓	
	Nominal	1	
	Available > 50x time required	0.01	
2. Stress	Extreme	5	It is assumed that the stress level is greater than nominal.
	High	2✓	
	Nominal	1	
3. Complexity	Highly	5✓	It is assumed that the complexity level is much higher than nominal due to the sustained excessive steam demand through the open MSIV and TBVs.
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	3	
	Nominal	1✓	
	High	0.5	
5. Procedures	Not available	50	

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
	Available, but poor	5	
	Nominal	1✓	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1✓	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1✓	
8. Work Processes	Poor	2	
	Nominal	1✓	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

**Table 3.** Task failure probability without formal dependence worksheet.

Task Portion	Nom. Prob.	Time	Stress	Compl.	Exper./ Train.	Proced.	Ergon.	Fitness	Work Process	Prob.
Diag.										N/A
Action	1.0E-3	x 10	x 2.0	x 5.0	x 1.0	x 1.0	x 1.0	x 1.0	x 1.0	9.0E-2 <sup>a</sup>
Total										9.0E-2

a. The human error probability was adjusted following a special formula of SPAR-H to represent the composite PSF influence, because multiple (i.e., three or more) non-nominal PSFs are involved.

### SPAR Model Human Error Worksheet (Page 3 of 3)

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence.

**Table 4.** Dependency condition worksheet.

Condition Number	Crew (same or different)	Location (same or different)	Time (close in time or not close in time)	Cues (additional or not additional)	Dependency	Number of Human Action Failures Rule
1	s	s	c	–	complete	If this error is the <b>3<sup>rd</sup> error in the sequence</b> , then the dependency is at least <b>moderate</b> .
2	s	s	nc	na	high	
3	s	s	nc	a	moderate	
4	s	d	c	–	high	If this error is the <b>4<sup>th</sup> error in the sequence</b> , then the dependency is at least <b>high</b> .
5	s	d	nc	na	moderate	
6	s	d	nc	a	low	
7	d	s	c	–	moderate	This rule may be ignored only if there is compelling evidence for less dependence with the previous tasks.
8	d	s	nc	na	low	
9	d	s	nc	a	low	
10	d	d	c	–	moderate	
11	d	d	nc	na	low	
12	d	d	nc	a	low	
13 ✓					zero	

Using  $P$  = Task Failure Probability Without Formal Dependence (calculated on page 2):

- For Complete Dependence the probability of failure = 1.0
- For High Dependence the probability of failure =  $(1 + P)/2$
- For Moderate Dependence the probability of failure =  $(1 + 6P)/7$
- For Low Dependence the probability of failure =  $(1 + 19P)/20$
- ✓ For Zero Dependence the probability of failure =  $P$

Task Failure Probability With Formal Dependence =  $(1 + ( \quad * \quad )) / \quad = \underline{9.0E-2}$

## SPAR Model Human Error Worksheet (Page 1 of 3)

Plant: Calvert Cliffs 1 & 2 Event Name: HPI-XHE-XM-OTC5Task Error Description: Operator fails to initiate once through cooling (given excessive steam demand and both MSIVs fail to close upon SGIS)Does this task contain a significant amount of diagnosis activity? YES  NO 

If Yes, Use Table 1 below to evaluate the PSFs for the Diagnosis portion of the task before going to Table 2. If No, go directly to Table 2.

Table 1. Diagnosis worksheet.

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	
	Barely adequate < 20 m	10	
	Nominal ≈ 30 m	1	
	Extra > 60 m	0.1	
	Expansive > 24 h	0.01	
2. Stress	Extreme	5	
	High	2	
	Nominal	1	
3. Complexity	Highly	5	
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	10	
	Nominal	1	
	High	0.5	
5. Procedures	Not available	50	
	Available, but poor	5	
	Nominal	1	
	Diagnostic/symptom oriented	0.5	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1	

PSFs	PSF Levels	Multiplier for Diagnosis	If non-nominal PSF levels are selected, please note specific reasons in this column
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1	
8. Work Processes	Poor	2	
	Nominal	1	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

### SPAR Model Human Error Worksheet (Page 2 of 3)

**Table 2.** Action worksheet.

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
1. Available Time	Inadequate	1.0 <sup>a</sup>	It is assumed there is just enough available time for the operators to initiate feed and bleed cooling.
	Time available $\approx$ time required	10✓	
	Nominal	1	
	Available > 50x time required	0.01	
2. Stress	Extreme	5✓	It is assumed that the stress level is much higher than nominal due to the excessive steam demand and the failure of both MSIVs to close upon SGIS.
	High	2	
	Nominal	1	
3. Complexity	Highly	5✓	It is assumed that the complexity level is much higher than nominal due to the sustained excessive steam demand through the open MSIVs and TBVs.
	Moderately	2	
	Nominal	1	
4. Experience/ Training	Low	3	
	Nominal	1✓	
	High	0.5	
5. Procedures	Not available	50	

PSFs	PSF Levels	Multiplier for Action	If non-nominal PSF levels are selected, please note specific reasons in this column
	Available, but poor	5	
	Nominal	1✓	
6. Ergonomics	Missing/Misleading	50	
	Poor	10	
	Nominal	1✓	
	Good	0.5	
7. Fitness for Duty	Unfit	1.0 <sup>a</sup>	
	Degraded Fitness	5	
	Nominal	1✓	
8. Work Processes	Poor	2	
	Nominal	1✓	
	Good	0.8	

a. Task failure probability is 1.0 regardless of other PSFs.

**Table 3.** Task failure probability without formal dependence worksheet.

Task Portion	Nom. Prob.	Time	Stress	Compl.	Exper./ Train.	Proced.	Ergon.	Fitness	Work Process	Prob.
Diag.										N/A
Action	1.0E-3	x 10	x 5.0	x 5.0	x 1.0	x 1.0	x 1.0	x 1.0	x 1.0	2.0E-1 <sup>a</sup>
Total										2.0E-1

a. The human error probability was adjusted following a special formula of SPAR-H to represent the composite PSF influence, because multiple (i.e., three or more) non-nominal PSFs are involved.

**SPAR Model Human Error Worksheet (Page 3 of 3)**

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence.

**Table 4.** Dependency condition worksheet.

Condition Number	Crew (same or different)	Location (same or different)	Time (close in time or not close in time)	Cues (additional or not additional)	Dependency	Number of Human Action Failures Rule
1	s	s	c	–	complete	If this error is the <b>3<sup>rd</sup> error in the sequence</b> , then the dependency is at least <b>moderate</b> .
2	s	s	nc	na	high	
3	s	s	nc	a	moderate	If this error is the <b>4<sup>th</sup> error in the sequence</b> , then the dependency is at least <b>high</b> .
4	s	d	c	–	high	
5	s	d	nc	na	moderate	This rule may be ignored only if there is compelling evidence for less dependence with the previous tasks.
6	s	d	nc	a	low	
7	d	s	c	–	moderate	
8	d	s	nc	na	low	
9	d	s	nc	a	low	
10	d	d	c	–	moderate	
11	d	d	nc	na	low	
12	d	d	nc	a	low	
13 ✓					zero	

Using P = Task Failure Probability Without Formal Dependence (calculated on page 2):

- For Complete Dependence the probability of failure = 1.0
- For High Dependence the probability of failure =  $(1 + P)/2$
- For Moderate Dependence the probability of failure =  $(1 + 6P)/7$
- For Low Dependence the probability of failure =  $(1 + 19P)/20$
- ✓ For Zero Dependence the probability of failure = P

Task Failure Probability With Formal Dependence =  $(1 + ( \quad * \quad )) / \quad = \underline{2.0E-1}$

**Additional Notes:**