Westinghouse
Electric Corporation

Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-96-4739
DCP/NRC0528
Docket No.: STN-52-003

June 6, 1996

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

ATTENTION: T. R. QUAY

SUBJECT: DRAFT MARKED UP OF AP600 PRA CHAPTER 54

Dear Mr. Quay:

Enclosure 1 to this letter is a draft mark up of Chapter 54 of the AP600 Probabilistic Risk Assessment (PRA) covering the low power and shutdown PRA assessment. The PRA section has been revised to incorporate commitments Westinghouse made in responses to RAIs.

The highlighted information on the draft mark up of the previously transmitted PRA chapter, indicates the new information. The striked-out information indicates the information that is to be removed. Please note that Tables 54-3 through 54-7 have not changed and are not included in the enclosure. The enclosed information will be cleaned up (strikeout info removed) and included in Revision 7 of the PRA, which has an expected transmittal date to the NRC of June 28, 1996.

This draft mark up of the AP600 PRA is being submitted for NRC use in writing Chapter 19 of the AP600 Final Safety Evaluation Report.

Enclosure 2 to this letter provides a revised response to three shutdown PRA RAIs.

As discussed between Westinghouse and NRC PRA personnel in a meeting on May 8, 1996, an assessment of design changes that have occurred since PRA Revision 6 have been evaluated for potential impact on the shutdown PRA results and insights. Enclosure 3 provides a summary of design changes and their impact on the PRA Chapter 54 analysis.

E004
1/1

100045

Please contact Cynthia L. Haag on (412) 374-4277 if you have any questions concerning this transmittal.

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

/nja

Enclosure

cc: J. Sebrosky, NRC (without enclosures)
D. Jackson, NRC (Enclosures)
J. Flack, NRC (without enclosures)

Enclosure 2 to Westinghouse
Letter NSD-NRC-96-4739
June 6, 1996

RESPONSE TO RAIs

Re: Shutdown PRA question from NRC letter dated November 9, 1995

Question 1 (#2939)

Open item 19.1.3.3-1 requested Westinghouse to justify the low human error rate for inadvertent draining of reactor vessel inventory though the Normal Residual Heat Removai (RHR) system. In response, Westinghouse quantified the likelihood of the operator overdraining the reactor coolant system during drain down operations to reach midloop conditions. Westinghouse also quantified the likelihood that a LOCA could occur by inadvertent opening of Normal RHR valve V024. The staff needs the following information to conclude that the frequency of overdraining the reactor vessel to reach midloop conditions is on the order of E-6 per year, which is much lower than current operating experience.

a. Westinghouse should use operating experience to determine the frequency of the operator inadvertently overdraining the RCS during midloop, or justify that current operating experience is not applicable by describing any AP600 design improvements over current plants.

b. Westinghouse needs to add more information in the shutdown PRA about the available level instrumentation during the drain down process. A description of how the pressurizer wide range level instrumentation is connected to the RCS would be helpful.

c. Westinghouse needs to clarify in the PRA how the two hot leg instruments are connected and clarify whether they share common reference legs.

d. Westinghouse needs to document in the PRA the basis for the beta factor of 0.05 for the hot leg instruments. This value is not listed in Chapter 29 or Section 54.7 of the PRA.

e. For drain down scenario 2, Westinghouse needs to justify the likelihood that the air operated valves fail to close on demand. Westinghouse needs to (1) document the testing interval for these valves and (2) calculate valve unavailability using ((standby failure rate)*(testing interval)/2) or a demand failure rate (such as 1E-3 listed in Table 54-58).

Response:

a. The AP600 has incorporated many design features that address mid-loop operations including features that reduce the probability of overdraining the RCS to a point where a loss of the normal residual heat removal system would occur. These features are described in SSAR section 5.4.7.2.1 and are described below:

   - **Loop Piping Offset** - As described in SSAR subsection 5.3.4.1, the reactor coolant system hot legs and cold legs are vertically offset. This permits draining of the steam generators for nozzle dam insertion with hot leg level much higher than traditional designs. The reactor coolant system must be drained to a level which is sufficient to provide a vent path from the pressurizer to the steam generators. This is nominally 80 percent level in the hot leg. This loop piping offset also allows a reactor coolant pump to be replaced without removing a full core.

- **Step-nozzle Connection** - The normal residual heat removal system employs a step-nozzle connection to the reactor coolant system hot leg. The step-nozzle connection has two effects on mid-loop operation. One effect is to substantially lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

  Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction has been shown experimentally to be no greater than 5 percent. This level of air ingestion will make air binding of the pump much less likely.

- **No Normal Residual Heat Removal Throttling During Mid-Loop** - The normal residual heat removal pumps are designed to minimize susceptibility to cavitation. The plant piping configuration, piping elevations and routing, and the pump net positive suction head characteristics allow the normal residual heat removal pumps to be started and operated at their full design flow rates with saturated conditions in the reactor coolant system. The normal residual heat removal system operates without the need for throttling a residual heat removal control valve when the level in the reactor coolant system is reduced to a mid-loop level. This eliminates the failure to throttle the residual heat removal pumps causing a loss of the residual heat removal system during mid-loop .

- **Hot Leg Level Instrumentation** - The AP600 reactor coolant system contains independent level instrumentation in each hot leg with indication in the main control room. In addition, the wide-range pressurizer level instrumentation used during cold plant operations is available to measure to the bottom of the hot legs. There is continuous level indication in the main control room from the normal level in the pressurizer to the range of the two narrow-range hot leg level instruments. Alarms are provided to alert the operator when the reactor coolant system hot leg level is approaching a low level. The isolation valves in the line used to drain the reactor coolant system automatically close on a low reactor coolant system level during shutdown operations to preclude overdraining the RCS. Operations required during mid-loop are performed by the operator in the main control room. The level monitoring and control features significantly improve the reliability of the AP600 heat removal system during mid-loop operations.

These design features contribute to the reduction in the probability of overdraining the RCS for the AP600 as compared to current plants.

Other design features have been incorporated in the AP600 design to address the consequences of a loss of the normal residual heat removal system due to overdraining and/or excessive air ingestion into the residual heat removal pumps. These features, addressed in SSAR section 5.4.7.2.1, are described below:

- **Passive Core Cooling System** - The passive core cooling system in-containment refueling water storage tank (IRWST) injection lines are available in the event of a loss of the normal residual heat removal system during reduced inventory operations. Upon a loss of water level in the hot leg, the operator would take actions to restore the water level with the nonsafety-related chemical and volume control system makeup pumps. If the makeup pumps are not available and / or operable, the operator can actuate the safety-related IRWST injection valves to restore water level in the RCS and provide safety-related core cooling. In addition, the normal residual heat removal system contains a diverse means for gravity injection from the IRWST via the pump suction line to the IRWST. By opening valve RNS-V023, gravity injection can be provided to the RCS hot leg in the event of a loss of the normal residual heat removal system.

- **ADS Valves** - The automatic depressurization system first-, second-, and third-stage valves, connected to the top of the pressurizer, are open whenever the core makeup tanks are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurization of the reactor coolant system during shutdown conditions when decay heat removal is lost. This also allows the IRWST automatically provide injection flow if it is actuated on a loss of decay heat removal.

- **Reactor Vessel Outlet Temperature** - Reactor coolant system hot leg wide range temperature instruments are provided in each hot leg. The orientation of the wide range thermowell-mounted resistance temperature detectors enable measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. In addition, at least two incore thermocouple channels are available to measure the core exit temperature during midloop residual heat removal operation. These two thermocouple channels are associated with separate electrical divisions.

- **Self-Venting Suction Line** - The residual heat removal pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This eliminates potential problems with refilling the pump suction line if a residual heat removal pump is stopped when cavitating due to excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

In addition, Westinghouse has submitted emergency response guidelines for shutdown operations that will be used to implement shutdown emergency operating procedures. These procedures will guide the operator to recover from overdraining events. These design features contribute to the reduction in the calculated core damage frequency for the AP600 at shutdown as compared to current plants.

This information will be provided in the AP600 Shutdown Evaluation Report and will be referenced in the shutdown PRA.

b & c There are two safety-related RCS hot leg level channels, one located in each hot leg. These level indicators are provided primarily to monitor the RCS water level during mid-loop operation following shutdown operations. One level tap is located at the bottom of each hot leg and the other tap on the top of each hot leg as close to the steam generator as possible. These level instruments are independent, and do not share instrument lines.

During post-accident conditions, these instruments provide indication of the water level in the reactor vessel. They provide reactor vessel level indication for a range from the bottom of the hot leg to approximately the elevation of the reactor vessel flange mating surface.

Each level instrument reading is provided in the main control room and the remote shutdown workstation. This instrumentation provides an accurate readout of the RCS level in the control room. Alarms are provided to alert the operator when the RCS level is approaching a low level. These transmitters also provide input to the PMS to initiate in-containment refueling water storage injection on a low level during mid-loop operations.

In addition, the wide-range pressurizer level instrumentation used during cold plant operations is available to measure to the bottom of the hot legs. This provides a continuous level indication in the main control room from the normal level in the pressurizer to the range of the two narrow-range hot leg level instruments.

This information will be provided in the AP600 Shutdown Evaluation Report and will be referenced in the shutdown PRA.

d. The beta factor of 0.05 for the hot leg level instruments was taken from the URD, Chapter 1, Appendix A, Section A3 (Page A.A-29); 0.05 is the recommended generic beta factor for "failure to continue functioning or spurious operation" of components not specified in the URD, Table A3-1. Westinghouse will provide this reference source for this beta factor in the shutdown PRA report.

e. ~~Air-operated valves CVS-045 and CVS-047, modeled in drain down scenario #2, are to be tested quarterly but are expected to be used more often during normal operation. Therefore, the failure probability of these valves failing to close on demand will be recalculated using a demand failure rate of 2.0E-03 from the Data Analysis section of the PRA.~~

For drain down scenario #2 discussed in Section 54.4.6, air-operated valves CVS-045 and CVS-047 were modeled in the shutdown PRA. However, there is an additional air-operated valve (CVS-059) in the drain down path that can be closed to prevent overdraining of the RCS.

The three valves are sized the same and fail closed on loss of air. However, valves CVS-045 and CVS-059 are of the same design, are in the same environment (inside containment), and their operational and functional requirements are the same. On the other hand, CVS-047 is a control valve designed with special trim to accommodate its positioning and throttling mechanisms, and is located outside containment. Based on these considerations, AOV CVS-047 is believed to be diverse from AOVs CVS-045 and -059.

Overdraining scenario #2 is recalculated below, using a demand failure rate of 2.0E-03 for each valve failing to close. This recalculation shows that the failure probability for overdraining scenario #2 is changed from 4.82E-06 to 1.75E-06.

SCENARIO #2:

All level instruments are assumed to be operating correctly. The operator initiates draining through the chemical and volume control system and is assumed to stop monitoring the RCS level. The RCS drains down to low hot leg level. Air-operator valves CVS-V045, -V047, and -V059 (arranged in series) are required to close automatically upon receipt of low hot leg level signal. Each of these AOVs is assigned a demand failure rate of 2.0E-03. If automatic closure of the valves does not occur, the operators are required to close them. It is assumed that the operators have a very short time window (approximately 5 minutes to close the valves).

The failure probability for this scenario is estimated as follows:

a) Random failure of CVS-V045, V047 & V059 is: $(2.0E\text{-}03)^3$ = 8.00E-09

b) Common cause failure of CVS-V045 & V059 is: (2.0E-03 x 0.088) = 1.76E-4

c) CCF of CVS-V045 & V059 multiplied by random failure of V047 = 3.52E-07

From (a) and (c), the failure probability of the AOVs is: 8.00E-09 + 3.52E-07 = 3.60E-07.

d) Failure of AOV automatic actuation signal is assigned a probability of 1.0E-04 per demand. This failure probability is based on data provided in Chapter 26.

e) "Operator fails to respond to low hot leg level alarm and fails to stop RCS draining" is identified by RCS-MANOD2S. This operator action is evaluated in Chapter 30. The HEP for this action is 1.39E-02. Credit for this operator action assumes that there is a hot leg level alarm independent of the AOV actuation signal.

From (d) and (e), failure of AOVs to close automatically and manually is: 1.0E-04 x 1.39E-02 = 1.39E-06.

Therefore, the failure probability for SCENARIO #2 is estimated to be 3.60E-07 + 1.39E-06 = 1.75E-06.

Re: Shutdown PRA question from NRC letter dated December 22, 1995

Question 720.305 (#3009)

In the shutdown PRA, many of the potential boron dilution initiating events are discussed and dropped as being not significant. However, since the shutdown core damage frequency is 5.5E-8 per year, the staff cannot conclude that these initiators have frequencies less than this value. Based on previous screening calculations and the Surry shutdown PRA, the staff requests Westinghouse to quantify the following boron dilution events identified in the AP600 PRA:

a. Chemical and Volume Control System (CVS) during safe shutdown using the DILUTE mode of operation.

b. CVS water injection and boron dilution during plant startup.

c. CVS water injection and boron dilution following a loss of offsite power event, with subsequent startup of the reactor coolant pumps.

d. Steam generator tube rupture event with transfer of water to and from the primary circuit.

Response:

~~The basis for excluding boron dilution events from the shutdown PRA quantification will be reexamined. These events will be included in the quantification if they are determined to be significant contributors to the shutdown core damage frequency.~~

The AP600 shutdown PRA identified several potential events which could result in a dilution of the primary system boron concentration and possible power excursion concerns. These events included:

a. Chemical and Volume Control System operation during Safe Shutdown using the DILUTE mode of operation.

b. CVS water injection and boron dilution during plant startup.

c. CVS water injection and boron dilution following a loss of offsite power event, with subsequent startup of the reactor coolant pumps.

d. Steam generator tube rupture event with transfer of water to and from the primary circuit.

The first three events on the above list occur during low power or shutdown operation. During shutdown the control rods are inserted. If the operators are diluting the RCS boron concentration and the dilution rate exceeds the programmed rate, the operators will be notified of this problem by high flux alarms. The AP600 control system is designed to terminate the dilution event when the alarm setpoint is reached. If the automatic termination of dilution fails, the operators would have sufficient time to recognize the problem and manually terminate the dilution before any power excursion would occur.

During low power operations, the operators would be notified of boron dilution by the high flux alarms. The AP600 control system will insert the control rods and terminate the dilution event. Again, the operators would have sufficient time to recognize the problem and terminate the dilution event before any power excursion would occur.

Thus, there is not a significant risk of a power excursion due to boron dilution for the AP600. The automatic mitigation function with the long time for the operators to respond to a failure combine to prevent boron dilution from becoming a problem. Nonetheless, an evaluation of these dilution events follows, to provide a quantification of them.

The potential for boron dilution following the rupture of a steam generator tube is evaluated. In conventional PWRs, it has been postulated that dilute reactor coolant could collect in the crossover leg and cause a criticality problem if the associated reactor coolant pump were subsequently restarted. Since the AP600 does not contain a crossover leg, the amount of dilute water that could collect in the reactor cooolant system is limited. Dilute water entering from the secondary side to the primary side would enter the cold leg and sufficiently mix prior to entering the core. The amount of water that could collect in the reactor coolant pump is limited. Evaluations have been performed to show that if the reactor coolant pump collected unborated water following a steam generator tube rupture, subsequent startup of that pump would not cause a boron dilution event.

To provide additional protection against the possibility of an unborated slug of water being directly injected to the core, the AP600 Emergency Response Guidelines instruct the operators to restart a reactor coolant pump in the opposite loop of a faulted steam generator during recovery from a tube rupture event. This operation will cause reverse flow in the faulted steam generator, thus mixing any unborated water in the steam generator, prior to it entering the core.

Based on the above considerations, boron dilution events following a steam generator tube rupture are not credible events for the AP600.

a. **Chemical and Volume Control System Operation during Safe Shutdown using DILUTE Mode of Operation**

As stated in the shutdown PRA, revision 6, Section 54, page 54-31, boron dilution resulting in reactor criticality is only a concern during the beginning of the fuel cycle, which represents a small fraction of the total cycle. However, it will be conservatively assumed that dilution is a concern throughout the fuel cycle. The frequency of shutdowns is 2.7/yr. and the fraction of the total shutdowns which are safe shutdowns is 0.8. Therefore the number of safe shutdown is, 2.7 x 0.8, or 2.16/year. While the plant is in safe shutdown, the CVS is in the DILUTE mode to counteract the buildup of Xenon.

The HOTSD simplified event tree was constructed to estimate the magnitude of possible boron dilution frequency during safe shutdown due to operation in the dilute mode. The initiating event would be the frequency that the reactor would be at safe shutdown conditions (2.16/yr). It was then postulated that the operator (OPF) fails to follow procedures to switch from the DILUTE to the AUTO mode during startup from safe shutdown. Startup is a routine, well-monitored phase with frequent checks, therefore this is a non-stressed action with a typical failure probability of 1 x 10^{-4}. If the operator fails to switch to the AUTO mode, the control system (AUTO) should stop the dilution on a high flux alarm. The failure probability of the control system is approximately 1 x 10^{-4}. If the operator is successful in switching from the DILUTE mode, the valve (VAL3) might fail to operate and the system would remain in the DILUTE mode. The failure probability for such a valve is approximately 1 x 10^{-3}. If the control system succeeds in trying to close the DWS valve, the valve (VALDW) might remain open; the failure probability for such a valve is approximately 1 x 10^{-3}. If dilution occurs, then there should be a high flux alarm. The operator should respond to this alarm to correct the event. Normally, the operator should monitor and detect dilution well before the alarm occurs. The human error probability to respond to the appropriate alarm is estimated to be approximately 1 x 10^{-4}, with a worst case value of 1 x 10^{-3}. Finally, even if dilution were to occur, the reactor coolant pumps would continue to run, resulting a slow dilution of the primary system which should be detectable and controllable. The failure of both reactor coolant pumps (common cause) would be approximately 1 x 10^{-5}.

Reviewing the HOTSD event tree, only end states 4, 8 and 12 could result in rapid dilution of the core, the estimated frequency of these end states are 2.16 x 10^{-10}, 2.16 x 10^{-14} and 2.16 x 10^{-15} respectively. Since the low power/shutdown core damage frequency (CDF) was calculated to be 4.72 x 10^{-6}, end states 8 and 12 are sufficiently low that even significant uncertainties in their value should not affect the CDF. End state number 4 is approximately three orders of magnitude less than the CDF. However, if a worst case value for OPP above (1 x 10^{-3}) is assumed and another order of magnitude is allowed for uncertainties in the failure rates selected, the frequency of dilution (end state 4) could rise to 2.16 x 10^{-6}. This would represent approximately 45% of the CDF. Therefore, the dilution frequency during safe shutdown should not result in a significant increase in the CDF; it could result in a small increase about 45% for this worst case (very conservative) situation.

b. CVS Water Injection and Boron Dilution during Plant Startup

Another possible dilution scenario identified in the previous analysis was a dilution during startup due to the operator inadvertently setting the wrong demineralized water flow. Again, it is assumed that the fuel is at a condition where dilution would be a concern. Therefore, the frequency of startups is 2.7/year (the number of startups equal the number of shutdowns). The simplified STARE event tree was constructed to evaluate this dilution event. The first postulated event following the startup is the failure of the operator (OPP1) to follow startup procedures and set the proper flow. Again, this event is occurring during startup which is a routine, well-monitored phase with frequent checks, therefore this is a non-stressed action with a typical failure probability of 1 x 10^{-4}. If the operator is successful in setting the proper flow, the valve (VAL4) might fail to operate; the failure probability for such a valve is approximately 1 x 10^{-3}. If the operator does not set the flow or the valve does not adjust as set, the dilution will begin. At this point a reactor trip (RTRIP) should occur on flux doubling. The control system reactor trip would have a failure probability of approximately 1 x 10^{-3}. If the reactor trip succeeds, the demineralized water valve (DWSF) should close. The failure probability for this type of valve is estimated to be 1 x 10^{-3}. If the reactor trip or the DWS valve fail, then the operator (OPP2) should respond to the flux doubling or trip alarm. The human error probability to respond to the appropriate alarm is estimated to be approximately 1 x 10^{-4}, with a worst case value of 1 x 10^{-3}.

In the STARE event tree, only end states 4, 6, 9 and 11 could result in dilution of the core. The estimated frequencies of these end states are 2.7 x 10^{-13}, 2.7 x 10^{-10}, 2.7 x 10^{-11} and 2.7 x 10^{-11} respectively. As shown previously, end states 4, 9, and 11 are significantly smaller than the shutdown core damage frequency (CDF), so their value should not affect the CDF. End state number 6 is approximately two orders of magnitude less than the CDF. However, if a worst case value for OPP2 above (1 x 10^{-3}) is assumed and another order of magnitude is allowed for uncertainties in the failure rates selected, the frequency of dilution (end state 6) could rise to 2.7 x 10^{-8}. This would represent approximately 56% of the CDF. Therefore, the dilution frequency during startup should not result in a significant increase in the CDF. If the worst case (most conservative) assumptions were taken, the CDF could increase by 56%; however, this new CDF is still very low.

c. CVS Water Injection and Boron Dilution following Loss of Offsite Power, with subsequent Startup of Reactor Coolant Pumps

Another possible dilution scenario identified in the previous analysis was a dilution due to CVS water injection and boron dilution following a loss of offsite power event, with subsequent startup of the reactor coolant pumps. Again, it is assumed that the fuel must be at a condition for dilution to be a concern. The frequency of LOSP is 8.13 x 10^{-3}/year. The simplified LOSP event tree was constructed to evaluate this dilution event. Assuming a LOSP, the first postulated event is the failure of the automatic control system (AUTOF) to sense the LOSP and close the DWS valve, preventing dilution. The failure probability for such control systems is 1 x 10^{-4}. If the control system is successful in closing the valve, the DWS valve (VALVF) may fail to close. The failure probability for such a valve is approximately 1 x 10^{-3}. If the control system fails to close the DWS valve or there is a failure of the DWS valve, the control system should also automatically align the V115 valve to the borate tank, thus preventing dilution. The failure probability of this type of valve is approximately 1 x 10^{-3}. If the control fails to close the valve or both of the valves fail to close, then the operator (OPFA1) should still follow proper procedures during CVS pump restart, and verify alignment to the borate tank prior to restart. This restart is a routine, well-monitored phase, therefore this is a non-stressed action with a typical failure probability of 1 x 10^{-4} (worst case, 1 x 10^{-3}). If the operator fails to properly align the borate tank at startup, the operator (OPFA2) would then have to respond to the flux doubling or high temperature alarm. As above, the operator should monitor and detect dilution well before the alarm occurs. The human error probability to respond to the appropriate alarm is estimated to be approximately 1 x 10^{-4}, with a worst case value of 1 x 10^{-3}

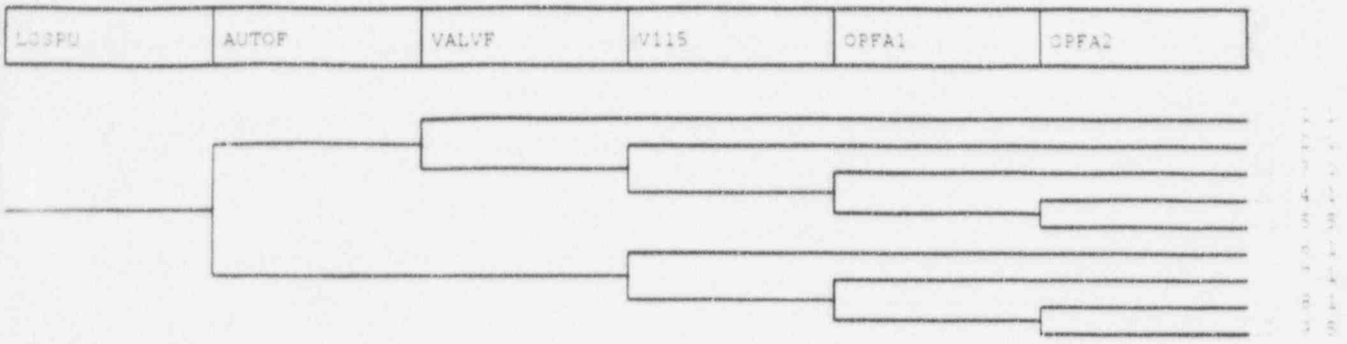
The LOSP event tree indicates only end states 5 and 9 could result in dilution of the core; the estimated frequency of these end states are 8.13 x 10^{-16} and 8.13 x 10^{-17} respectively. As above, these end states are significantly smaller than the shutdown core damage frequency (CDF), so their value should not significantly affect the shutdown/low power CDF.

04/12/96 10:58:12 [illegible]

LOSP_DIL

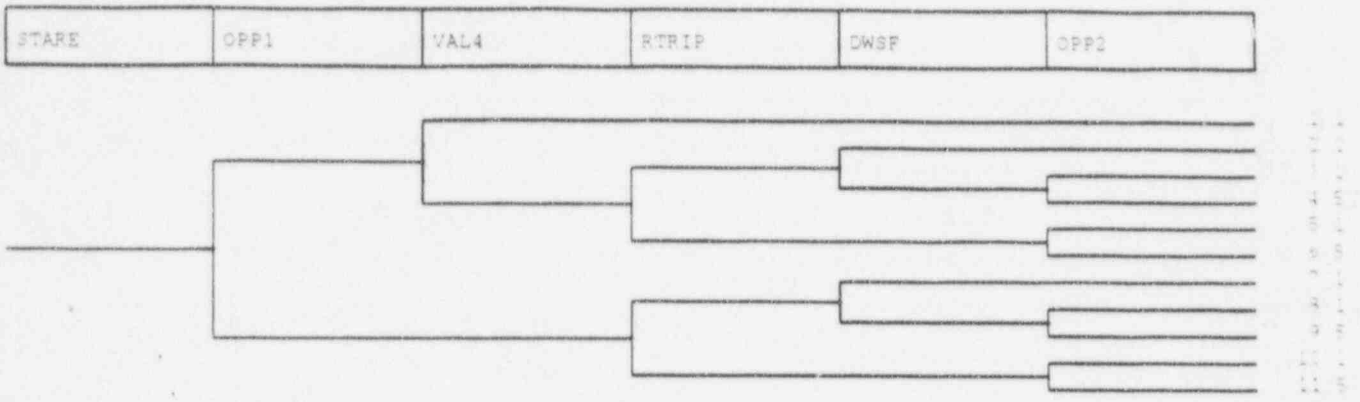
LOSP AT UET CAUSES DILUTION

Page 1 of 1



```
14-12/98 10:58:12         File: 03/13/92 15:02:00 186218    Path: E:\CODES\CADET.EXE                    CADET [illegible]
LOSP_DIL
LOSP AT UET CAUSES DILUTION
List of top events


Event                          Description

LOSPU                          LOSS OF OFF-SITE POWER WHILE AT UET
AUTOP                          AUTO CONTROL SYSTEM SENSES LOSP AND INTIATES DWS CLOSURE
VALVP                          DWS VALVE CLOSES
V115                           VALVE V115 ALIGNS TO BORATE TANK
OPFA1                          OPERATOR FOLLOWS PROCEDURE TO RESTART CVS PUMPS
OPFA2                          OPERATOR RESPONDS TO HIGH FLUX/HIGH TEMP. ALARM
```

04/12/96 11:10:41
STARE
BORON DILUTION AT STARTUP
Page 1 of 1



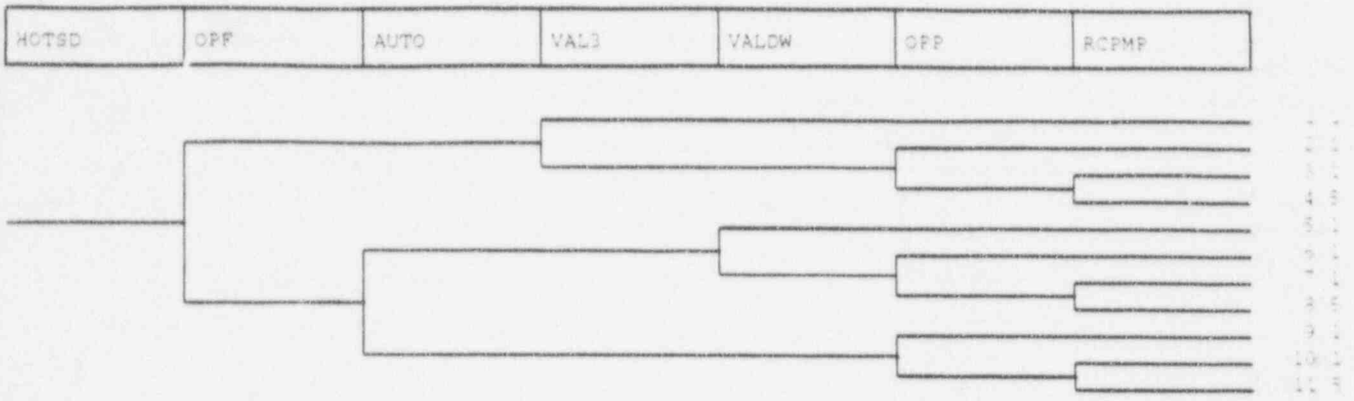
```
04/10/96 11:17:42          File: 03/13/90 15:10:00 136218     Path: E:\CODES\CADET.EXE                    CADET 1.
STARE
BORON DILUTION AT STARTUP
List of top events

Event                      Description

STARE                      BORON DILUTION DURING STARTUP AT UET
OPP1                       OPERATOR SETS PROPER FLOW
VAL4                       VALVE SETS PROPER FLOW BASED ON OPERATOR SETTING
RTRIP                      REACTOR TRIPS ON FLUX DOUBLING
DWSF                       DWS VALVE CLOSES ON TRIP SIGNAL
OPP2                       OPERATOR RESPONDS TO FLUX DOUBLING OR TRIP ALARM
```

04/12/96 11:10:41 IADET 2.[illegible]

HOTSD

DILUTION DURING STARTUP FROM HOT SHUTDOWN

Page 1 of 1



```
04-10-92 11:03:41        File: 03/13/92 19:02:00 136218    Path: E:\CODES\CADET.EXE                    CADET ...
HOTSD
DILUTION DURING STARTUP FROM HOT SHUTDOWN
List of top events


Event                          Description

HOTSD                          HOT SHUTDOWN WHILE AT UET
OPF                            OPERATOR SWITCHES FROM DILUTE TO AUTO MODE TO STARTUP
AUTO                           CONTROL SYSTEM DETECTS AND SHUTS OFF DILUTION ON HIGH FLUX
VAL3                           DILUTION VALVE SWITCHES FROM DILUTION CONFIGURATION
VALDW                          DWS VALVE CLOSES WHEN ACTUATED TO STOP DILUTION
OPP                            OPERATOR RESPONDS TO HIGH NEUTRON FLUX
RCPMP                          REACTOR COOLANT PUMPS CONTINUE TO OPERATE - SLOW DILUTION
```

Re: Shutdown PRA question from NRC letter dated December 22, 1995

Question 720.306 (#3010)

The PRA clearly states that containment integrity is maintained during modes 1 through 4. However, the status of containment during modes 5 and 6 is unclear in the PRA (Section 54.2.5). The PRA states that during midloop operation, containment "closure" is maintained. However, midloop operation is only a subset of shutdown operations in mode 5 with the RCS open. Also, the term "closure" is not defined. The staff assumes that "closure" is different from containment integrity. The staff is concerned that the results of the PRA do not include the risk impact of a potentially open containment given a core damage event during mode 5. The staff needs this information since events occurring during midloop/vessel flange operation account for over 90% of the shutdown core damage frequency. Therefore, Westinghouse is requested to provide the following information in the shutdown PRA:

a. Westinghouse is requested to document in the PRA how the requirement for containment integrity will be maintained during Modes 1-4 (i.e. Tech. Specs., admin. controls, etc.).

b. Westinghouse is requested to document in the shutdown PRA the status of containment during cold shutdown (mod [illegible] when the RCS is completely intact. This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary instrument and electrical penetrations. This explanation should also describe the operator's ability to close containment should a core damage event occur. Westinghouse is requested to document in the PRA how these assumptions will be met (i.e. Tech. Specs., admin. controls, etc.)

c. Westinghouse is requested to document in the shutdown PRA the status of containment during cold shutdown up to when the refueling cavity is flooded with an open RCS (midloop operation/vessel flange operation is a **subset** of this phase of shutdown). This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary electrical and instrument penetrations. This explanation should also describe the operator's ability to close containment before steaming through an open RCS makes containment conditions intolerable to the operator. Westinghouse is requested to document in the PRA how these assumptions will be met (i.e. Tech. Specs., admin. controls, etc.)

d. For both of the shutdown phases addressed above, Westinghouse is requested to identify in the shutdown PRA the probabilities assumed for containment isolation.

e. For both of the shutdown phases addressed above, Westinghouse is requested to report the fraction of core damage scenarios occurring with an open containment and their combined frequencies.

Response:

a. The AP600 Technical Specifications will specify the requirements for containment status during all modes of operation including shutdown. This information will be referenced in the shutdown PRA. During Modes 1-4, containment integrity is required. In Modes 5 & 6, during reduced inventory operations and when the upper internals are in place, containment closure capability is required. Containment closure capability is defined in the Technical Specifications as the capability to close the containment prior to core uncovery following a loss of the normal decay heat removal capability through the normal residual heat removal system. Details on the containment status during each operating mode are summarized in Table Q2-1 of the response to shutdown PRA question 2c (of NRC letter dated Nov. 9, 1995). This table will be provided in the AP600 Shutdown Evaluation Report and will be referenced in the shutdown PRA.

b. As shown in Table Q2-1 in the response to shutdown PRA question 2c (of NRC letter dated Nov. 9, 1995), there are no requirements for containment integrity or closure during Mode 5, when the RCS is intact.

c. As shown in Table Q2-1 in the response to shutdown PRA question 2c (of NRC letter dated Nov. 9, 1995), during Mode 5, with the RCS pressure boundary open and/or during reduced inventory operations, and during Mode 6 with the upper internals in place, containment closure is required. As described above, containment closure capability is defined as the capability to close the containment prior to core uncovery following a loss of the normal decay heat removal system. Equipment hatches and personnel hatches, penetrations for operating systems, and any temporary electrical and instrument penetrations may be open during these conditions, provided that there is the capability to close the various hatches and penetrations within prescribed time limits, corresponding to the minimum time to core uncovery following loss of decay heat removal capability. The actions taken to close the containment hatches must consider the potential for a steam environment inside containment within the time that the RCS could reach saturation.

d. ~~The next revision of the shutdown PRA will assess the probabilities of failure of containment isolation during shutdown modes where containment closure is required.~~

This RAI response provides an assessment of the failure probabilities for containment isolation during shutdown modes where containment closure is required. As stated in Section 54.2.4, in modes 5 & 6, during reduced inventory operations and when the upper internals are in place, containment closure capability is required. Containment closure capability is defined in the Technical Specifications as the capability to close the containment prior to core uncovery following a loss of the normal decay heat removal capability through the normal residual heat removal system.

Operator actions to close valves for isolating the respective systems have been accounted for in the shutdown PRA, and are therefore excluded from this evaluation.

Based on the shutdown PRA model, only events occurring in mode 5, during reduced inventory operations, are considered to require containment closure.

The following assumptions are made in this evaluation:

- Equipment hatches, personnel hatches, and temporary elecurical and instrument penetrations are open during the mid-loop scenarios modeled in the PRA.

- The openings include: one main equipment hatch, one maintenance hatch, two personnel hatches, and three spare penetrations.

- More than one temporary line or cable can fit through each spare penetration. Such lines are fitted with quick disconnect attachments.

- Each personnel hatch consists of two doors in series that are normally interlocked to maintain containment integrity. The interlock is defeated to allow both doors to be kept open .

- The openings are closed manually; the equipment hatch is closed from inside containment, and the other openings are closed from outside containment.

- The openings are manned by maintenance personnel with responsibilities as follows:
  - 2 persons for closing main equipment hatch
  - 2 persons for closing maintenance hatch
  - 2 persons for closing each personnel hatch
  - 2 persons for disconnecting the lines and closing the spare penetrations

  Each opening can be closed by one person with the second person serving as backup or assistant.

- Based on the existence of AP600 shutdown emergency response guidelines, it is assumed that detailed written procedures will be developed and used for closing the openings.

- Assuming reduced inventory is reached as early as 28 hours after reactor shutdown, the fastest the reactor coolant can heat up to boiling is about 17 minutes from the loss of RNS. It is estimated that the containment could heat up to 145°F in about 33 minutes after the reactor coolant begins to boil. Therefore, for this worst case scenario, the containment temperature could reach 145°F in 50 minutes from the loss of RNS.

- It is assumed that loss of RNS is the cue for initiating closure of these openings; therefore, there is a time window of approximately 50 minutes to complete these actions. It is further assumed the containment environment is habitable up to 145°F.

- Personnel are required to evacuate the containment before closing the personnel hatches; in that regard, the equipment hatch must be closed prior to closing the personnel hatches. It is assumed that it takes about 30 minutes to close the equipment hatch, and, during that time, personnel in the containment are evacuated.

- It is assumed the other openings, all of which are closed from outside containment, can be also closed within the actual time of 30 minutes discussed in the previous paragraph.

- Although the loss of RNS is expected to be diagnosed by the control room personnel, it is expected that an alarm would be annunciated in the containment to signify the need for containment closure. To be conservative, it is assumed that cognitive diagnosis for closing the hatches (by the maintenance crew) is required and this diagnosis must be completed within 15 minutes from the alarm. According to previous assumptions, a time window of about 35 minutes remains to physically close the openings.

- On closing each opening, one maintenance crew (MC) member is assigned a low dependency on the other crew member.
- An optimum stress level is assigned for this task according to THERP 20-16, item 1.
- It is assumed that the hatches and doors for the openings are exercised (when they are first opened) to ensure they can close on demand. Therefore, hardware failures of these openings are judged to be highly unlikely; (i.e., an estimated failure probability less than 1.0E-06 per demand for each opening). However, if 1.0E-05 per demand is conservatively applied for the failure probability of one of these openings to close, then a failure probability of 7.0E-05 per demand is assumed for hardware failure of these openings.

Quantification of the human error probability for this task is as follows:

(D_{HEP}) Diagnosis Error Calculation:

D1: Failure to diagnose need for closing containment hatches within 15 minutes = 4.0E-02 [THERP 20-3 & Figure 12-4]

$D2_{(MC1)}$: Failure to respond to 1 of 1 local alarm = 2.7E-04 [THERP 20-23 (1)]

$D2_{(MC2)}$: Low crew dependency assigned to the second crew member = 0.05 [THERP 20-4]

$D2 = D2_{(MC1)} \times D2_{(MC2)} = 2.7E\text{-}04 \times 0.05 = 1.35E\text{-}05$;

$(D_{HEP}) = D1 \times D2 < 1.0E\text{-}05$.

(A_{HEP}) Action Execution Calculation:

A1 a) Omit action to close assigned opening (omission error) = 1.3E-03 [THERP 20-7 (1)]

b) Stress multiplier = 2

$A1_{(MC1)}$ = a x b = 2.6E-03

$A1_{(MC2)}$ = 0.05 [THERP 20-18]

Therefore, action execution failure for one opening is estimated as:

$A1_{HEP}$ = [illegible] x $A1_{(MC2)}$ = 1.3E-04.

Since there are seven openings, the total action execution failure is:

A_{HEP} = $A1_{HEP}$ x 7 = 1.3E-04 x 7 = 9.1E-04.

Therefore, the HEP for closing the containment hatches and temporary penetrations is:

$D_{HEP} + A_{HEP}$ = 9.1E-04.

Result

The estimated failure probability of the openings for containment closure is the summation of the assumed hardware failure probability (7.0E-05) and the HEP (9.1E-04); that is a failure probability of 9.8E-04.

The failure probability of the fault tree for containment isolation (CIST) is estimated to be 1.71E-02. By including the failure probability of 9.8E-04 in the CIST fault tree, the estimated failure probability of containment isolation changes from 1.71E-02 to 1.81E-02; an increase of approximately 6 percent. This increase of 6% is judged to be insignificant and has no effect on the PRA results.

e. ~~The fraction of core damage frequency from events occurring with an open containment and their total frequency will be shown in the next revision of the shutdown PRA.~~

During the meeting between Westinghouse and the NRC PRA staff on January 18, 1996, the staff clarified that this RAI pertains to events, identified in the shutdown PRA, that could be initiated when the containment is open. Therefore, this RAI response provides an estimation of the fraction of core damage frequency from events occurring with an open containment and their total frequency. As discussed previously (in the response to part (b) of this RAI) the requirement for containment closure is limited to events occurring during mid-loop conditions.

Based on the results reported in Chapter 59 of the PRA, events occurring during mid-loop conditions contribute 85 percent of the level 1 shutdown core damage frequency. This contribution consists of the following:

• Loss of decay heat removal due to CCS/SWS initiated failures	54.13 percent
• Loss of offsite power	19.04 percent
• Loss of decay heat removal due to RNS initiated failures	10.41 percent
• LOCA due to inadvertent opening of valve RNS-V024	1.45 percent

The associated yearly frequencies of these events are:

• Loss of decay heat removal due to CCS/SWS initiated failures	2.98E-08
• Loss of offsite power	1.05E-08
• Loss of decay heat removal due to RNS initiated failures	5.73E-09
• LOCA due to inadvertent opening of valve RNS-V024	7.96E-10

Therefore, the total yearly frequency of these events is 4.7E-08.

Enclosure 3 to Westinghouse
Letter NSD-NRC-96-4739
June 6, 1996

Attachment 1

ASSESSMENT OF DESIGN CHANGES ON SHUTDOWN LEVEL 1 PRA

The design changes made subsequent to revision 6 of the PRA model do not significantly change the shutdown results. Furthermore, the major insights from the shutdown PRA are not changed by these design changes. The benefit and importance of the RNS and IRWST functions are not changed. Both of these functions are important to maintain plant safety during drained conditions.

The impact of each design change on the shutdown PRA results or insights is summarized below:

Assessment of Change Impact on Shutdown PRA Results or Insights

Design Change	Impact on Shutdown PRA Results or Insights
1. CCS valves to the RNS heat exchanger changed from manual to air-operated	Insignificant impact on results. No impact on insights; loss of RNS or its support systems is still expected to be among the dominant accident sequences
2. The capacity of the service water basin reduced; its duration changes from 24 hours to 12 hours	Insignificant impact on results. No impact on insights; loss of RNS or its support systems is still expected to be among the dominant accident sequences; loss of SWS causes the loss of RNS
3. Service water system (SWS) valves V037A & B changed from air-operated to motor-operated	Insignificant impact on results. No impact on insights; loss of RNS or its support systems is still expected to be among the dominant accident sequences; loss of SWS causes the loss of RNS
4. The number of PRHR heat exchangers changed from two to one	Insignificant impact on results. No impact on insights; PRHR is modeled in accident sequences during non-drained conditions. Non-drained condition sequences are not among the dominant accident sequences
5. RNS check valves V015A & B on the DVI lines changed to stop check valves	Check valve type has very little or no impact on the PRA results, since failure data is essentially the same for different types of check valves
6. IRWST recirculation paths changed from 10 inch and 4 inch lines to 6 inch lines in all paths	No impact; The recirculation lines are not applicable to the shutdown model
7. IRWST injection check valves maintaining the RCS pressure boundary changed to squib valves	Insignificant impact on results. No impact on insights; importance of the IRWST to maintaining plant safety is not affected by this change
8. IRWST motor-operated valves 118A & B and check valves 120A & B maintaining the IRWST water level changed to squib valves	Insignificant impact on results. No impact on insights; importance of the IRWST to maintaining plant safety is not affected by this change

Enclosure 1 to Westinghousc
Letter NSD-NRC-96-4739
June 6, 1996

CHAPTER 54

LOW-POWER AND SHUTDOWN RISK ASSESSMENT

54.1 Introduction

The low-power and shutdown assessment is conducted to address concerns about the risk from operations during shutdown conditions. The evaluation, which covers shutdown and low-power operation, encompasses operation when the reactor is in a subcritical state or is in transition between subcriticality and power operation up to 5 percent of rated power. The evaluation addresses conditions for which there is fuel in the reactor vessel and includes aspects of nuclear steam supply, the containment, and all systems that support the nuclear steam supply and containment. However, the evaluation does not address events involving fuel handling outside of the containment and fuel storage in the fuel storage building.

The scope of this shutdown assessment meets the requirement of Reference 54-1, which states:

> The limited scope PRA performed for shutdown conditions shall encompass evaluation of core damage frequency (only a simplified Level 1 PRA is required). A simplified evaluation of the release frequencies and magnitudes will be done. A simplified evaluation for shutdown conditions are required in order to demonstrate compliance with the overall requirements of the ALWR.

The shutdown assessment documented in this chapter covers internal events, except internal fire and internal flood; evaluations for floods and fires are provided in Chapters 56 and 57, respectively, for these types of internal events.

The shutdown assessment addresses ~~the six~~ five operating modes of AP600. These operating modes are carried out within the six major phases of shutdown. The applicability of the operating modes is discussed in subsection 54.2.3.

The activities performed during plant shutdown are divided into three categories: nondrained maintenance, drained maintenance, and refueling. A typical frequency for AP600 for these shutdown conditions is defined in this chapter and used to condense the frequencies of events that could lead to core damage at shutdown.

The shutdown categories are discussed in subsection 54.3.1, and the various activities conducted in these categories are delineated in subsection 54.3.2.

54.2 Initiating Events

This section describes the process by which initiating events considered during shutdown of AP600 are identified and evaluated. The initiating events used in the shutdown core damage frequency calculation are quantified in Section 54.4 and summarized in Table 54-6.

The consequences of events occurring during plant shutdown are sometimes bounded by the same events at power. This is based on the following differences that characterize shutdown operation:

- Lower decay heat levels and smaller inventory of radionuclides
- Longer allowable times for manual actuation of plant systems
- Increased effectiveness of available mitigating systems

During shutdown conditions, different plant configurations (for example, a partially drained reactor coolant system) and different configurations of the safeguards systems (actuation signals inhibited or safety systems secured or in maintenance) are possible, so that mitigation of events occurring during this plant status can sometimes be less effective.

54.2.1 Identification

Events initiated during plant shutdown are assumed to occur as a result of equipment failure or operator actions. Operator errors are assumed to be made while performing maintenance, testing, or system alignment.

The approach used to identify the possible and credible initiating events that could affect plant safety during shutdown includes the following considerations:

- Identification of the set of initiating events applicable to AP600 by reviewing the events reported in Reference 54-2 and previous PRA initiating events

- Analysis of the failure of specific AP600 auxiliary systems that might produce additional initiating events

- Analysis of the failures of AP600 passive systems that might produce new initiating events

54.2.2 Events Modeled

Plant shutdown refers to the operations that bring the reactor from safe shutdown temperature and pressure to cold (ambient) conditions. The following three types of plant shutdown are addressed:

- Nondrained maintenance shutdown – outages for maintenance or inservice inspections not requiring the reactor coolant system (RCS) to be drained (such as condenser cleaning).

- Drained maintenance shutdown – outages for maintenance or inservice inspections requiring the reactor coolant system to be partially drained (such as steam generator tube inspections). During this drained state, the plant is described to be at mid-loop/vessel-flange condition.

- Refueling shutdown – outages for refueling, during which maintenance may be performed with a drained refueling cavity.

The first two types of plant shutdown may include shutdowns that are required following transients or accidents initiated at power.

54.2.3 Shutdown Phases Summary Description

This subsection discusses the relation among the activities during the shutdown phases and the plant operating modes and identifies the operating modes that the shutdown evaluation focuses upon.

The six major phases in reactor shutdown are:

A	–	Cool down to cold shutdown
B	–	Drain down reactor coolant system
C	–	Fill refueling cavity
D	–	Post-refueling maintenance and drain refueling cavity
E	–	Reactor coolant system fill and gas evacuation
F	–	Heatup to hot standby

As shown in Table 54-1, phases A and F are applicable to shutdown conditions when the reactor coolant system is not drained; phases A, B, E, and F are applicable to shutdown conditions when the reactor coolant system is drained; and all six phases are applicable to refueling shutdown conditions.

The low-power and shutdown operations for AP600 are defined by the following ~~six~~ five operating modes:

~~Mode 1~~	~~–~~	~~Low power operation (up to 5 percent of rated power)~~
Mode 2	–	Startup and low power operation (up to 5 percent of rated power)
Mode 3	–	Hot standby
Mode 4	–	~~Hot~~Safe shutdown
Mode 5	–	Cold shutdown
Mode 6	–	Refueling

Based on the three types of plant shutdown, the relation among the shutdown phases, outage types, and operating modes is summarized in Table 54-1.

The shutdown PRA focuses on events occurring in modes 3 through 6. The treatment of events occurring during mode~~s 1 and~~ 2 is addressed in subsection 54.2.4.

54.2.4 Initiating Events for Operating Modes

~~Based on the results of the internal initiating events at-power PRA, events that do not contribute significantly to core damage and are judged to be less severe if they occur during shutdown conditions are not considered for detailed shutdown evaluation. Moreover, events that may be significant contributors to the internal initiating events at-power core damage frequency but are judged to be insignificant during shutdown because of the lower decay heat levels and longer times for operator response are also removed from detailed evaluation. Such events include steam generator tube ruptures (SGTR), core makeup tank (CMT) line break, safety injection (SI) line break, and anticipated transient without scram (ATWS).~~

A systematic examination is performed on potential initiating events that could occur during different operating modes. The objective of this examination is to identify the credible initiating events during shutdown for detailed analysis.

The matrix in Table 54-92 summarizes the screening process of the at-power initiating events for inclusion in the shutdown PRA evaluation. This matrix contains the 26 categories of initiating events from the at-power PRA. Each event is considered for the various RCS modes of operation. The events are then screened according to the following four categories:

1. These events are screened out because the plant response to these initiating events is bounded by the at-power event. The contribution to total core damage frequency for these events at shutdown, when compared with at-power conditions, is judged to be insignificant due to the relatively short amount of time in these plant conditions and the additional available time for operator intervention.

2. These events are screened out because RCS conditions have moderated significantly (i.e., reactor is tripped, pressure and temperature are reduced, decay heat is low) such that this event cannot occur during the shutdown mode. Events that are screened out for this reason include ATWS (reactor is already tripped) and most LOCAs (RCS pressure is significantly reduced). Small LOCA does not meet this criterion for most conditions because it is judged that operator errors or failures within the normal residual heat removal system can result in a small LOCA (stuck-open RNS low-temperature overpressure relief valve or other valve misalignment).

3. These events are screened out because specific system alignments during shutdown prevent them from occurring. These events include PRHR tube rupture during mode 4 (PRHR is isolated) and loss of main feedwater during mode 4 (MFW isolated, RCS cooling accomplished via the RNS).

4. These events are not screened out and are evaluated further in the shutdown PRA.

In addition to the screening analysis outlined above, a specific examination is performed on the passive systems to identify potential initiating events within these systems during shutdown conditions. This examination is discussed below for the following passive systems/subsystems:

- Core makeup tanks
- Accumulators
- Automatic depressurization system
- IRWST
- Passive residual heat removal
- Passive containment cooling

Core Makeup Tanks

The following failure mechanisms are evaluated for the core makeup tanks (CMTs):

- Spurious actuation - Spurious actuation of the CMTs is not considered a credible initiating event during power operation (modes 1 and 2). The CMTs are in the standby condition and are actuated by opening of the air-operated valves downstream in the lines connecting them to the safety injection lines. Failure of the valves to remain closed, or inadvertent opening by the operators, does not produce any change in the plant parameters, since no flow to the reactor coolant system can be initiated due to the continued reactor coolant pumps operation.

  During shutdown modes 3 and 4, the CMTs are in the standby condition, and the RCPs are operating. Similar to at-power operations, failure of the CMT discharge valves to remain closed, or inadvertent opening by the operator during modes 3 and 4 does not produce any change in the plant parameters; the CMTs do not inject.

  During modes 5 and 6, the CMTs are taken out for maintenance by isolating the inlet motor-operated isolation valves. Therefore, spurious opening of the CMT injection valves will not result in CMT operation. Furthermore, their operation during modes 5 or 6 will not cause a significant operational transient, since the RCS pressure is reduced and temperature is below 200°F.

- Pipe break - A break of the pipe connecting the CMT to the direct vessel injection (DVI) line or to the cold leg could result in a loss-of-coolant accident. However, this type of event is screened out from the shutdown quantification according to the criteria in Table 54-92.

Accumulators

The following failure mechanisms are evaluated for the accumulators during shutdown:

- Spurious actuation - Accumulators are in the standby condition during mode 3 above 1000 psig and are automatically actuated as the RCS pressure drops below accumulator pressure. Below 1000 psig, the accumulators are isolated to prevent their injection. Neither spurious actuation nor actuation by operator error is possible.

- Pipe break - A break of the pipe connecting the accumulators to the DVI line (from check valve V029A(B) to the DVI line) could result in LOCA conditions. However, this type of event is screened out from the shutdown quantification according to the criteria in Table 54-92.

Automatic Depressurization System (and Pressurizer Safety Valves)

The automatic depressurization system (ADS) consists of:

- Two identical depressurization trains on the pressurizer, each train having one 6-inch pressurizer safety valve and three stages of the ADS. Each stage has two normally closed valves in series. The first-stage valves are 4-inch motor-operated valves. The second- and third-stage valves are 8-inch motor-operated valves.

- Four depressurization lines (fourth stage of the ADS) on the hot legs, two lines for each hot leg. Each line consists of one 10-inch, normally open motor-operated valve in series with the 10-inch, normally closed squib valve.

The following potential failures are evaluated for shutdown:

- Spurious actuation of a pressurizer safety valve due to mechanical failure - During power operation, if the safety valve recloses before the loss of a large amount of coolant, the event is similar to a spurious reactor trip event; its contribution is included in the spurious reactor trip frequency. If the valve remains stuck open, the event proceeds like a medium LOCA. No operator action to close the pressurizer safety valve is possible (no operator action can contribute to the event frequency). For shutdown mode 3, failures of the safety valve are considered in the same manner as the at-power events. In mode 4 and below, the RCS pressure is significantly reduced such that the mechanical failure of a safety valve is not credible.

- Spurious actuation of the ADS - For power operations, this event is similar to a LOCA event. Depending on number of ADS lines spuriously opening, the spurious actuation frequency of the ADS is contributed to small, medium, or large LOCA.

  During shutdown mode 3, spurious ADS could occur similar to the at-power events. During shutdown mode 4, the spurious operation of the ADS valves is considered to be similar to a small LOCA, since the mass flow from the RCS will be lower than at-power due to the lower RCS pressure and temperature and lower decay heat associated with this mode. However, these types of LOCA events are screened out from the shutdown quantification according to the criteria in Table 54-92.

During mode 5, spurious operation of the ADS valves does not result in a significant operational transient because the RCS conditions are significantly reduced. Furthermore, the ADS valves are opened during a significant portion of mode 5 corresponding to reduced inventory operations.

IRWST Gravity Injection/Recirculation

The following failure mechanisms are evaluated for the IRWST:

- Spurious actuation - This system is normally in the standby condition and is automatically actuated by squib valves opening on low CMT water level, and by check valves opening when the reactor pressure drops below approximately 25 psia. During normal plant operation, spurious actuation of the gravity injection system (squib valves) will not result in an operational transient because of the high RCS pressure. During shutdown modes 3, 4 and the early part of mode 5, this is also the case. During mode 5 reduced inventory conditions, spurious actuation would cause an increase in RCS inventory, but would not lead to an accident event.

Passive Residual Heat Removal

The following failure mechanisms are evaluated for the passive residual heat removal system:

- Spurious actuation - During modes 3 and 4, this system is in the standby condition. Spurious actuation of the passive residual heat removal heat exchanger can be produced by the failure of one of the two air-operated valves (V108A or V108B) to remain closed, or by operator error. During shutdown mode 3, operation of the passive heat removal heat exchanger will reduce the RCS temperature. However, the plant will remain in a safe, stable condition, with the passive residual heat removal system removing decay heat. For the at-power events, spurious actuation of the passive residual heat removal system is classified as a transient (with main feedwater available) event. However, the contribution of this event to a transient (with main feedwater available) initiating event is negligible compared with the frequency related to the other generating causes (such as spurious reactor trip or turbine trip). Therefore, it is not analyzed for power operation, and is not analyzed in shutdown mode 3.

  In shutdown mode 4, the RCS temperature is reduced, and the effectiveness of the PRHR to remove heat is diminished. Therefore, its spurious operation will not cause a significant plant transient. In mode 5, the PRHR is isolated for maintenance, and spurious operation is not considered.

- Heat exchanger tube rupture - This event is similar to a small LOCA. However, this type of LOCA event is screened out from the shutdown quantification according to the criteria in Table 54-92.

Passive Containment Cooling System

The passive containment cooling system is in the standby condition and is automatically actuated when a high containment pressure signal is generated. Its spurious actuation does not produce any immediate plant consequence.

Thus, it is concluded from the examination that events that could potentially occur within the passive systems during shutdown and low-power conditions would not be significant contributors to the shutdown core damage frequency. Therefore, initiating events from failures in the passive systems are screened out from the shutdown quantification.

A comprehensive evaluation of the reactor coolant system and connected systems is performed to identify all potential drain paths that the operator could create during shutdown. This evaluation considers potential shutdown modes and configurations and the possibility that the RCS could be pressurized. The evaluation also considers if there are planned operations associated with each potential drain path, and determines if inadvertent opening of the drain path could cause overdraining of the RCS. Overdraining is defined as draining the RCS to a level below the minimum level necessary for continued normal residual heat removal system operation. If a drain path does not drain the RCS below this level, it is not considered further because decay heat removal would not be lost.

RCS draining can occur if the operators mistakenly open a normally closed valve in the reactor coolant system, or a valve in a connected system to the RCS. This could occur during shutdown modes, with the RCS pressurized or depressurized, where the consequences of such actions may not be intuitively obvious to the operators.

The following systems or subsystems are found to directly interface with the reactor coolant system, and could present a potential drain path from the reactor coolant system:

- Automatic depressurization system
- Reactor vessel head vent
- Chemical and volume control system (purification loop and letdown line)
- Normal residual heat removal system
- Passive residual heat removal system
- Core makeup tanks
- Primary sampling system

The possibility of draining the RCS by inadvertently opening valves in any of these systems is discussed in the paragraphs that follow.

Automatic Depressurization System

The first three stages of ADS valves are connected to the pressurizer and discharge to spargers located in the IRWST. These valves are manipulated by the operator during shutdown to perform in-service testing. Interlocks are provided to prevent the inadvertent opening of two ADS valves in series that would cause an inadvertent ADS actuation.

During shutdown modes, with the RCS pressurized, inadvertent opening of two ADS valves in series would cause a loss of RCS inventory similar to a loss-of-coolant event. This event is screened out from the shutdown quantification as discussed in subsection 54.2.4. In lower modes, with the RCS depressurized, inadvertent opening of these valves would not result in a loss of RCS inventory due to the elevation of the ADS valves (top of the pressurizer).

The fourth stage ADS valves are connected to the hot legs. These valves are squib valves, and no in-service testing of these valves is required. Opening these valves with the RCS pressurized would result in a loss of RCS inventory similar to a LOCA, which is also screened out from the shutdown quantification. During RCS depressurized conditions, opening these valves would drain the RCS down to the elevation where the valves discharge. This is above the hot legs and would not cause an overdraining of the RCS. Moreover, since there are no planned operations to stroke open the fourth stage ADS valves, and since two operators are needed to actuate the ADS valves, inadvertent opening of these valves is not considered credible.

Reactor Vessel Head Vent

The reactor vessel head vent valves are connected to the top of the reactor vessel head and discharge to the spargers in the IRWST. They may be opened during shutdown operations to vent the vessel head during draindown operations. Opening of these valves would cause overdraining of the RCS because the location of these valves and their discharge point are above the elevation of the RCS hot leg. Therefore, they are not considered further.

Chemical and Volume Control System

The normal drain path for the RCS is via the chemical and volume control system (CVS) letdown line which is connected to the CVS purification loop. This drain path is considered in the PRA quantification as shown in subsection 54.4.6. No other remotely operated valves exist in the CVS purification loop that could cause overdraining of the RCS. Small 1-in. manual valves are connected to the purification loop and are discussed below under "Manual Valves."

Normal Residual Heat Removal System

During shutdown modes, the normal residual heat removal system (RNS) is connected to the RCS hot leg. Inadvertent operation of two remotely operated valves could divert reactor coolant and drain the RCS. The RNS suction and discharge headers are connected to the IRWST and provide an IRWST recirculation loop that can be used to test the RNS pumps and to cool the contents of the IRWST. The RNS pump suction line to the IRWST contains a normally closed motor-operated valve (V023), while the RNS pump discharge line to the IRWST contains a normally closed motor-operated valve (V024). These valves are interlocked with the RNS valves connected to the RCS hot leg to preclude the operators aligning the RNS to the RCS if these valves are open, thus preventing an inadvertent diversion of reactor coolant to the IRWST.

During RNS operation, inadvertent opening of V024 could cause the RCS to be overdrained. This drain path is considered in the PRA quantification as shown in subsections 54.4.5 and 54.4.10. However, inadvertent opening of V023 would not result in overdraining of the RCS, because this line connects to the bottom of the IRWST. If V023 were inadvertently opened, the IRWST would increase the RCS inventory by injecting into the RCS via this line.

Passive Residual Heat Removal Heat Exchanger

The PRHR heat exchanger connects to the RCS via connections to a hot leg and a steam generator channel head. However, the elevation of the PRHR heat exchanger is above the RCS loops; therefore, the PRHR heat exchanger does not represent a potential drain path for the RCS. There are no manual drain valves, connected to the PRHR and piping, that are located below the RCS loop piping.

Core Makeup Tanks

The core makeup tanks are connected to the RCS via connections to the cold legs and the reactor vessel injection nozzles. However, the elevation of the core makeup tanks is above the RCS loops; therefore, the core makeup tanks do not represent a potential drain path for the RCS. There are no manual drain valves, connected to the core makeup tanks and piping, that are located below the RCS loop piping.

Primary Sampling System

The primary sampling system, consisting of very small lines (0.25-in.), connects to top of the RCS hot legs. Therefore, the primary sampling system cannot overdrain the RCS.

Manual Drains

The RCS, RNS, and CVS contain manual 1-in. drain lines that could potentially provide a drain path for the RCS. These drains are discussed further.

Reactor Coolant Pump Flushing Connection

Flushing connections are provided on each reactor coolant pump. These connections consist of a manual valve and a blind flange. These connections are only used during RCS decontamination operations (once every 10 to 20 years), during which the fuel is off-loaded. Therefore, these connections are not evaluated further.

Normal Residual Heat Removal System Test Valves and Equipment Drains

There are 1-in. manual drain lines in the RNS that, if opened, could drain the RCS. These valves may be opened to perform maintenance on the RNS equipment, or to perform containment isolation valve leak tests. These operations are performed prior to RNS operation during shutdown. It is highly unlikely that these valves would be open prior to RNS initiation for cooldown because the operability of the RNS is tested (via connections to the IRWST) immediately prior to alignment to the RCS. During this checkout of the RNS, the operator would be able to detect significant leakage from the system to the auxiliary building sump, and would also recognize the mispositioning of the valves. Even in the highly unlikely event that the valve were left open and the system aligned to the RCS, the operators would detect the pressurizer level decrease. The CVS makeup pumps would operate to maintain pressurizer water level, and the operators would isolate the RNS and perform a system checkout to verify all valves were correctly positioned.

Chemical and Volume Control System Drain Valves

There are 1-in. manual drain lines in the CVS purification loop that, if opened, could drain the RCS. These valves may be opened to perform maintenance on the CVS equipment, or to perform containment isolation valve leak tests. These operations are performed during mode 6, after the CVS purification is not required. During these operations, the CVS must be isolated from the RCS, and therefore, these valves could not drain the RCS.

After the screening process, the following types of events are retained for detailed analysis:

- Loss of decay heat removal following loss of the normal residual heat removal system (RNS) or loss of component cooling water system (CCS) or service water system (SWS)
- Loss of offsite power (LOOP)
- Loss-of-coolant accidents (LOCAs)
- Reactor coolant system drain events
- Reactivity accidents, including boron dilution events

The following paragraphs discuss the initiating events that could occur during the different shutdown modes.

- **Startup and ~~L~~low power ~~(mode 1~~ up to 5 percent power~~)~~, ~~startup (~~mode 2~~)~~, and hot standby (mode 3)**

  The plant response to a loss of core cooling (including loss-of-coolant accidents) at low power, startup, and hot standby is the same as during power operation, since the safety-related and nonsafety-related systems and actuation signals, both automatic and manual, are available. In addition, the contribution to total core damage frequency for events initiated at low power, startup, and hot standby, compared with at-power conditions, is judged to be insignifica ıt due to the relatively short amount of time in these plant conditions and the additi onal available time for operator intervention.

Thus, the consequences of initiating events occurring during modes ~~1 (low power),~~ 2~~,~~ and 3 are expected to be bounded by the analyses for events initiated during power operation and are removed from further consideration in this assessment.

Only boron dilution events are believed to be credible events that could impact plant risk if they occurred during hot standby, plant startup, or low power. These are retained for further evaluation.

- **~~Hot~~Safe shutdown/cold shutdown (modes 4 and 5)**

Events occurring during modes 4 and 5 with the reactor coolant system filled and pressurized are analyzed together. The grouping of events in these modes does not have a significant impact on the results, since events occurring at the lower end of cold shutdown are judged to be less risk significant than events occurring when the temperature and pressure are higher.

During the time at shutdown that the reactor is in these modes, most of the events normally analyzed for at-power conditions, such as turbine trip, loss of feedwater flow, and anticipated transient without scram, are not event initiators that could occur and are excluded from the shutdown quantification. However, loss of offsite power and loss-of-coolant accidents could lead to core damage with the plant in this condition.

The following initiating events not explicitly considered in the analysis for power operation are evaluated to determine the plant risk for these events during modes 4 and 5:

- Boron dilution
- Loss of decay heat removal due to failure of normal residual heat removal system
- Reactor pressure vessel drain events

When the plant is drained to mid-loop, additional or different considerations are taken into account in the shutdown evaluation to address the following issues:

- Different water inventory available in case of loss of decay heat removal.

- Different conditions of availability of mitigating systems. The passive residual heat removal heat exchanger (PRHR HX) is not effective because the reactor coolant system cannot be pressurized. The core makeup tanks must be actuated manually and in-containment refueling water storage tank (IRWST) injection is actuated either automatically or manually.

- Depressurization valves are open.

- **Refueling (mode 6)**

  During refueling mode, the reactor pressure vessel head is removed, the refueling cavity is flooded, and the normal residual heat removal system is used for decay heat removal. Operations performed during the refueling mode are addressed in the following discussion of the range of activities during shutdown.

Typical Range of Activities during Shutdown

The initial phase of all plant shutdowns consists of reactor boration, cooldown, and depressurization. Under normal conditions, boron from the boric acid tank is added to the reactor by the makeup pumps. Heat is transferred through the steam generators from the reactor coolant system to the steam system. Depressurization is accomplished by spraying reactor coolant into the pressurizer, which condenses the pressurizer steam bubble.

Before reaching the pressure limit for accumulator injection (about 700 psig), the accumulators must be isolated by closing motor-operated valves (MOVs) V027A and V027B.

The time windows for the various activities performed during a typical plant shutdown from ~~hot~~safe shutdown to refueling modes are based on the AP600 refueling outage plan (Reference 54-3). The selected time windows are summarized in Table 54-4.

When the reactor coolant temperature is reduced to about 350°F and the pressure is reduced to about 400 psig (about 4 hours after reactor shutdown), the cooldown continues using the normal residual heat removal system. With both trains available, this system is capable of cooling the reactor coolant system from:

- 350°F to 160°F within 24 hours

- 160°F to 130°F within 16 hours (during this phase, the draining of the reactor coolant system can be started)

- 130°F to 120°F within 39 hours (during this phase, the refueling cavity can be flooded)

The reactor coolant system temperature is typically below 160°F for plant operating mode 6 (refueling), in which the reactor coolant system may be opened for maintenance or refueling. The passive injection components (such as core makeup tank and in-containment refueling water storage tank injection) are isolated during the final stages of cooldown, prior to opening the reactor coolant system. If low hot leg water level is reached during shutdown operations, in-containment refueling water storage tank injection is automatically actuated by reopening the motor-operated valves in the injection lines.

To initiate the steam generator draining process, the hot legs are partially drained to about the 80-percent level, allowing air to be vented into the steam generator tubes from the pressurizer. This draining is performed through the normal residual heat removal, chemical and volume control (CVS), and liquid radwaste systems. The water is drained to mid-loop to install dams in the steam generator nozzles and to perform steam generator and/or reactor coolant pump inspections and maintenance. The drain rate is controlled by the low-pressure letdown path in the chemical and volume control system. The letdown flow control valves are remotely operated, and the hot leg level is measured with redundant instruments permanently installed on the hot legs. Therefore, the reactor coolant system level can be both monitored and controlled from the main control room throughout the brief period of mid-loop operation.

The operation for draining the reactor coolant system to mid-loop is typically performed during cooldown to 120°F. During this time, the nozzle dams are installed, and the water level can be raised to the vessel-head flange. The plant remains in this state until the reactor coolant system temperature reaches 120°F. A time window of 39 hours is assigned to the activities for completing phase B (drain down the reactor coolant system).

The refueling cavity is then flooded for refueling operations. Water is transferred from the in-containment refueling water storage tank to the refueling cavity by the spent fuel pool cooling system (SFS). This function has traditionally been performed by the normal residual heat removal system, and that capabiiity still exists if the need arises; however, no credit for normal residual heat removal function has been modeled.

If the normal residual heat removal system were to fail just after ~~flooding~~ the refueling cavity is flooded, the water would heat up to boiling in about 9 hours and boil down to the top of the fuel about 5 days later if the containment were not closed. Continued core cooling could easily be provided by several means. With the slow heatup of the refueling water, there is ample time to close the containment before the containment atmosphere begins to heat up. In addition, there are multiplc nonsafety-related systems (such as the chemical and volume control system, the spent fuel pool cooling system, the demineralized water transfer and storage (DWS) system and the fire water system) that can add water to the containment in this circumstance. Temporary water supplies, such as fire trucks, can also be used to add water to the containment. Based on these considerations, potential initiating events involving a loss of water inventory occurring during refueling mode are expected to have a negligible impact on the total core damage frequency and are not included in the models.

The activities conducted from (and including) flooding the refueling cavity to completion of the refueling task are expected to last about 100 hours. Phase C (fill refueling cavity) is completed within about 8 hours.

After completion of refueling and/or maintenance and inspections, the cavity is drained, the vessel head is set, and the steam generator dams are removed. At this point, the water temperature is very low (90°F or less) and the plant is in a stable maintenance state. A time window of 55 hours for draining the refueling cavity and for the maintenance activities (starting with setting the vessel head until the equipment hatch is replaced) is assumed.

After completion of this phase, the reactor coolant system has to be filled and the plant brought from cold shutdown to hot standby condition.

The AP600 Technical Specifications specify the requirements for containment status during all modes of operation including shutdown. During modes 1 to 4, containment integrity is required. There are no requirements for containment integrity or closure during mode 5, when the RCS is intact. In modes 5 and 6, during reduced inventory operations and when the upper internals are in place, containment closure capability is required. Containment closure capability is defined in the Technical Specifications as the capability to close the containment prior to core uncovery following a loss of the normal decay heat removal capability through the normal residual heat removal system. Equipment hatches and personnel hatches, penetrations for operating systems, and any temporary electrical and instrument penetrations may be open during these conditions, provided that there is the capability to close the various hatches and penetrations within prescribed time limits, corresponding to the minimum time to core uncovery following loss of decay heat removal capability. The actions taken to close the containment hatches consider the potential for a steam environment inside containment within the time that the RCS could reach saturation.

54.2.5 Actuating Signals and Systems Available

A list of safety-related and nonsafety-related systems available for operation during the different potential shutdown states is given in Table 54-2, which identifies the types of actuation for each system during the shutdown modes or conditions.

~~The following automatic actuation signals that are used during power operation are available during hot/cold shutdown conditions:~~

- ~~Signals that actuate a safeguards (S) signal:~~
  - ~~Low pressurizer level — through the protection and safety monitoring system (PMS) and diverse actuation system (DAS)~~
  - ~~High containment pressure — through the protection and safety monitoring system~~
  - ~~High containment temperature — through the diverse actuation system~~
- ~~Core makeup tank actuation signal and core makeup tank water level signal that actuate the automatic depressurization system (ADS)~~

~~The signals listed above do not function during mid-loop/vessel-flange and refueling shutdown conditions due to the draindown of the reactor coolant system. However, the low hot leg level~~

~~signal, used to monitor and control the reactor vessel water level during the draindown of the reactor coolant system for the mid-loop/vessel-flange shutdown phase, is available. This instrument automatically actuates the in-containment refueling water storage tank motor-operated valves on low level during the mid-loop/vessel-flange shutdown phase. This logic is part of the protection and safety monitoring system.~~

~~Containment integrity is maintained during modes 1 through 4. Only the containment penetrations of operating systems are open. During mid-loop operations in mode 5, containment closure is maintained, as described in the technical specifications. Otherwise, personnel or equipment hatches may be opened.~~

Both automatic and manual IRWST injection capabilities are available during all reduced inventory scenarios. However, conservatively, IRWST automatic actuation is not modeled in most reduced inventory cases, even though it would be expected to be available.

The PRA model reflects the following for events during drained conditions:

- Given loss of RNS, loss of RNS support systems, or LOOP with grid recovery, IRWST injection is required to actuate automatically or manually; both actuations are modeled in fault tree IW2A.

- Given LOOP without grid recovery, only manual IRWST injection is modeled; this is shown in fault tree IW2AP. Automatic injection is available, but not modeled.

- During draining of the RCS to mid-loop, only manual IRWST injection is modeled if overdraining occurs; this is shown in fault tree IW2AO. Automatic injection is available, but not modeled.

- For all of the above events during reduced inventory, if IRWST normal injection path fails, then injection through RNS pump suction line (V023) is manually actuated; this is shown in fault tree IWRNS.

54.2.6 Scenarios for Detailed Analysis

The following subsections describe initiating events that could occur during ~~hot~~safe/cold shutdown when the reactor coolant system is filled and pressurized or during mid-loop/vessel-flange condition when the reactor coolant system is drained and depressurized.

The AP600 has incorporated many design features that address mid-loop operations including features that reduce the probability of overdraining the RCS to a point where a loss of the normal residual heat removal system would be lost. These features are described in SSAR subsection 5.4.7.2.1 and are described below:

- **Loop piping offset** - As described in SSAR subsection 5.3.4.1, the RCS hot legs and cold legs are vertically offset. This permits draining of the steam generators for nozzle dam insertion with hot leg level much higher than traditional designs. The RCS must be drained to a level that is sufficient to provide a vent path from the pressurizer to the steam generators. This is nominally 80 percent level in the hot leg. This loop piping offset also allows a reactor coolant pump to be replaced without removing a full core.

- **Step-nozzle connection** - The normal residual heat removal system employs a step-nozzle connection to the reactor coolant system hot leg. The step-nozzle connection has two effects on mid-loop operation. One effect is to substantially lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

  Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction has been shown experimentally to be no greater than 5 percent. This level of air ingestion will make air binding of the pump much less likely.

- **No normal residual heat removal throttling during mid-loop** - The normal residual heat removal pumps are designed to minimize susceptibility to cavitation. The plant piping configuration, piping elevations and routing, and the pump net positive suction head characteristics allow the normal residual heat removal pumps to be started and operated at their full design flow rates with saturated conditions in the reactor coolant system. The normal residual heat removal system operates without the need for throttling a residual heat removal control valve when the level in the reactor coolant system is reduced to a mid-loop level. This eliminates the failure to throttle the residual heat removal pumps causing a loss of the residual heat removal system during mid-loop.

- **Hot leg level instrumentation** - The AP600 reactor coolant system contains independent level instrumentation in each hot leg with indication in the main control room. In addition, the wide-range pressurizer level instrumentation used during cold plant operations is available to measure to the bottom of the hot legs. There is continuous level indication in the main control room from the normal level in the pressurizer to the range of the two narrow-range hot leg level instruments. Alarms are provided to alert the operator when the reactor coolant system hot leg level is approaching a low level. The isolation valves in the line used to drain the reactor coolant system automatically close on a low reactor coolant system level during shutdown operations to preclude overdraining the RCS. Operations required during mid-loop are performed by the operator in the main control room. The level monitoring and control features significantly improve the reliability of the AP600 heat removal system during mid-loop operations.

These design features contribute to the reduction in the probability of overdraining the RCS for the AP600 as compared to current plants.

Other design features have been incorporated in the AP600 design to address the consequences of a loss of the normal residual heat removal system due to overdraining and/or excessive air ingestion into the residual heat removal pumps. These features, addressed in SSAR subsection 5.4.7.2.1, are described below:

- **Passive core cooling system** - The passive core cooling system in-containment refueling water storage tank (IRWST) injection lines are available in the event of a loss of the normal residual heat removal system during reduced inventory operations. Upon a loss of water level in the hot leg, the operator would take actions to restore the water level with the nonsafety-related chemical and volume control system makeup pumps. If the makeup pumps are not available and/or operable, the operator can actuate the safety-related IRWST injection valves to restore water level in the RCS and provide safety-related core cooling. In addition, the normal residual heat removal system contains a diverse means for gravity injection from the IRWST via the pump suction line to the IRWST. By opening valve RNS-V023, gravity injection can be provided to the RCS hot leg in the event of a loss of the normal residual heat removal system.

- **ADS valves** - The automatic depressurization system first-, second-, and third-stage valves, connected to the top of the pressurizer, are open whenever the core makeup tanks are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurization of the reactor coolant system during shutdown conditions when decay heat removal is lost. This also allows the IRWST to automatically provide injection flow if it is actuated on a loss of decay heat removal.

- **Reactor vessel outlet temperature** - Reactor coolant system hot leg wide-range temperature instruments are provided in each hot leg. The orientation of the wide-range thermowell-mounted resistance temperature detectors enable measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. In addition, at least two incore thermocouple channels are available to measure the core-exit temperature during mid-loop residual heat removal operation. These two thermocouple channels are associated with separate electrical divisions.

- **Self-venting suction line** - The residual heat removal pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This eliminates potential problems with refilling the pump suction line if a residual heat removal pump is stopped when cavitating due to excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

In addition, emergency response guidelines for shutdown operations will be used to implement shutdown emergency operating procedures. These procedures will guide the operator to recover from overdraining events.

54.2.6.1 Operating Modes 2 and 3

Reactivity accidents during modes 2 and 3, including boron dilution events, are analyzed. These events are discussed in subsection 54.4.11.

54.2.6.2 ~~Hot~~Safe/Cold Shutdown Events (Plant Operating Modes 4 and 5)

The following events during modes 4 and 5 are analyzed:

- Loss of decay heat removal
- Loss of offsite power
- Loss-of-coolant accident
- Reactor pressure vessel drain events
- Reactivity accidents

Loss of Decay Heat Removal in Modes 4 and 5

A loss of decay heat removal during ~~hot~~safe/cold shutdown conditions can be associated with:

- Failure in the normal residual heat removal system

- Failure of normal residual heat removal support systems (component cooling water or service water system)

- Improper operation of the normal residual heat removal system due to either of the following:

  - Drainage of the reactor coolant system below the level at which air ingestion by the normal residual heat removal pump occurs (only for drained maintenance shutdown)

  - Inadvertent opening of normal residual heat removal valve V024, allowing a flow diversion to the in-containment refueling water storage tank. Since a loss of reactor coolant system water inventory occurs as a result of this error, this event is considered in the loss-of-coolant accident analysis.

Loss of Offsite Power in Modes 4 and 5

For the loss-of-offsite-power event, the first level of defense is automatic restart of the normal residual heat removal pumps on the diesel generators. Details on mitigating the loss-of-offsite-power initiating event are provided in subsection 54.4.1.

Loss-of-Coolant Accident in Modes 4 and 5

With the normal residual heat removal system in the shutdown cooling mode, the mechanisms for causing a loss-of-coolant accident are the following:

- Operator error that inadvertently opens normal residual heat removal motor-operated valve V024 to allow flow diversion from the direct vessel injection (DVI) line to the in-containment refueling water storage tank, resulting in a loss of primary coolant.

- Pipe break in the normal residual heat removai system piping as a result of overpressurization due to loss of the decay heat removal system. This could occur, but is judged to be highly unlikely. Preliminary evaluations show that, following a normal residual heat removal system failure, thermal expansion and steaming cause an increase in pressure. The normal residual heat removal system relief valve V021 has sufficient capacity to prevent the reactor coolant system pressure to exceed the Appendix G limits (approximately 630 psig). The combined failure of the normal residual heat removal system and relief valve is judged to be significantly lower than the failure probability of the operator inadvertently opening RNS-V024; therefore, this mechanism of loss-of-coolant-accident generation is not represented in the loss-of-coolant-accident event trees.

- Sticking open of normal residual heat removal system relief valve V021 during nondrained maintenance, in ~~hot~~safe/cold shutdown conditions. This scenario is discussed in subsection 54.4.5.

- Pipe break within the normal residual heat removal system during ~~hot~~safe/cold shutdown conditions when the reactor coolant system is filled and pressurized.

Reactor Pressure Vessel Drain Events in Modes 4 and 5

The only AP600 system whose normal operation can cause draining of the reactor vessel is the normal residual heat removal system. However, only partial draining can occur because the normal residual heat removal suction line is connected to the reactor coolant system hot leg. If the water level goes below the minimum hot leg level, normal residual heat removal is lost due to pump air ingestion, which stops reactor pressure vessel draining. From this point, the scenario is bounded by the pipe break due to normal residual heat removal system overpressurization, described in the previous section.

Draining events can occur as a result of operator errors during the draindown of the reactor coolant system for steam generator or reactor coolant pump maintenance activities. This draindown is accomplished by using the flow path from the reactor coolant system hot leg through the normal residual heat removal pumps and heat exchangers, to the chemical and volume control system, and then to the liquid waste system. The drain rate is controlled by the low-pressure letdown path in the chemical and volume control system. The letdown flow control valves are remotely operated, and the hot leg level is measured with the permanently installed hot leg level instrumentation.

There are two safety-related RCS hot leg level channels, one located in each hot leg. These level indicators are provided primarily to monitor the RCS water level during mid-loop operation following shutdown operations. One level tap is located at the bottom of each hot leg and the other tap on the top of each hot leg as close to the steam generator as possible. These level instruments are independent, and do not share instrument lines.

During post-accident conditions, these instruments provide indication of the water level in the reactor vessel. They provide reactor vessel level indication for a range from the bottom of the hot leg to approximately the elevation of the reactor vessel flange mating surface.

Each hot leg level instrument reading is provided in the main control room and the remote shutdown workstation. This instrumentation provides an accurate readout of the RCS level in the control room. Alarms are provided to alert the operator when the RCS level is approaching a low level. These transmitters also provide input to the PMS to initiate in-containment refueling water storage injection on a low level during mid-loop operations.

In addition, the wide-range pressurizer level instrumentation used during cold plant operations is available to measure to the bottom of the hot legs. This provides a continuous level indication in the main control room from the normal level in the pressurizer to the range of the two narrow-range hot leg level instruments. Thus, the reactor coolant system level can be both monitored and controlled from the main control room. ~~An alarm is provided on low hot leg level, allowing the operator sufficient time to isolate letdown.~~ Furthermore, letdown flow is automatically isolated on a low-low reactor coolant system hot leg level signal.

Overdraining the reactor coolant system during draining of the system to mid-loop is evaluated as an initiating event in subsection 54.4.6. The pressurizer wide-range level instrument~~, although not redundant to the hot leg level instruments in the strictest sense,~~ serves an alternative way of monitoring the level of the vessel and can help in identifying inconsistency in the level indications. If the hot leg level instruments malfunction, the operator must recognize the condition and stop the normal residual heat removal system pump(s) to preclude draining of the reactor coolant system beyond mid-loop. Unlike normal residual heat removal pump operation at operating plants that require local actions for venting if the plant is drained beyond mid-loop, operation of AP600 only requires refilling the vessel to the appropriate level and restarting the normal residual heat removal system pump.

54.2.6.3 Mid-Loop/Vessel-Flange Events

The most limiting AP600 shutdown maintenance condition during which an accident could occur is when the reactor coolant level is reduced to the mid-loop/vessel-flange level, the reactor coolant system pressure boundary is opened, the vessel head is on, and the depressurization valves are maintained in the open position. It is normal practice to drain the reactor coolant system to mid-loop level to install the hot leg and cold leg nozzle dams. The water level is then raised to the vessel flange. This mid-loop status is expected to last about 8 hours. After these operations, steam generator inspection and maintenance is performed. In this situation, the normal residual heat removal system is used to cool the reactor coolant system. Therefore, the initiating events identified in subsection 54.2.6.2, with the exception of normal residual heat removal system pipe rupture, are considered as initiating events when the plant is at mid-loop/vessel-flange level.

~~However, w~~When the plant is at mid-loop/vessel-flange level, the passive residual heat removal heat exchanger cannot effectively operate.~~ because the reactor coolant system cannot be pressurized due to the open depressurization valves.~~ Therefore, in case of loss of the normal residual heat removal system~~s~~during mid-loop operation, core cooling must be provided by manual or automatic actuation of gravity injection from the in-containment refueling water storage tank via one of the two injection lines or the normal residual heat removal system pump suction line. If necessary after 72 hours, this can be followed by passive recirculation through the recirculation lines.

54.2.7 Summary of Initiating Events Analyzed

The following is a summary of the events analyzed in the shutdown assessment, based on the preceding discussion.

- ~~Hot~~Safe/cold shutdown condition with the reactor coolant system filled and intact:

  a) Loss of offsite power

  b) Loss of decay heat removal capability, initiated from failure of normal residual heat removal system, including normal residual heat removal valve V021 sticking open during nondrained maintenance

  c) Loss of decay heat removal capability, initiated from failure of component cooling water or service water system

  d) Loss-of-coolant accident due to rupture of the normal residual heat removal system piping

  e) Loss-of-coolant accident due to inadvertent or spurious opening of normal residual heat removal system motor-operated valve RNS-V024

- Transition from filled and depressurized reactor coolant system to mid-loop conditions:

  a) Overdraining of the reactor coolant system during draindown to mid-loop

- Mid-loop/vessel-flange condition with the reactor coolant system drained and depressurized:

  a) Loss of offsite power

b) Loss of decay heat removal capability, initiated from failure of normal residual heat removal system

c) Loss of decay heat removal capability, initiated from failure of component cooling water or service water system

d) Loss-of-coolant accident due to inadvertent or spurious opening of normal residual heat removal system motor-operated valve RNS-V024

- Several boron dilution events during shutdown conditions, as defined and discussed in subsection 54.4.11

54.3 Data

Data are developed for the frequencies and mission times of three types of plant shutdown events. The initiating frequencies for the various shutdown events are described in Section 54.4. The data are described in the following subsections.

54.3.1 Shutdown Frequency

The trip frequencies used in the shutdown assessment for AP600 are provided in Table 54-3. These are the same conservatively high estimates as used in the Level 1 at-power PRA.

The breakdown of the accident types contributing to this initiating event frequency is shown in Table 54-3. The total frequency of reactor trip due to transients, loss of normal residual heat removal support systems, and loss of offsite power, is estimated to be 2.1 events per year.

The estimated frequency of controlled shutdown other than refueling outages is shown in Table 54-3.

It is assumed that a refueling shutdown is scheduled every 24 months. Therefore, the frequency of refueling outages is 0.5 events per year.

For nondrained and drained maintenance shutdowns, the plant may be brought to cold shutdown condition following transients or accident-initiating events from high power. It is assumed that, for those events not further affected by additional component failures (with successful reactor trip and core cooling systems operation), it is assumed that 20 percent of the cases require bringing the plant to cold shutdown. It is further assumed that only 10 percent of the cold shutdown events require drained maintenance.

Based on the shutdown frequencies outlined above and the percentages of forced outages that could take the plant to cold shutdown and drained conditions, the frequencies of the plant in cold shutdown conditions (i.e., reactor coolant system nondrained and drained conditions) are calculated as follows:

- Reactor Coolant System Forced Outage Frequency for Nondrained Maintenance

  This frequency is calculated as the product of the trip frequency (2.1 events per year) and the percentage of shutdowns that takes the plant to cold shutdown with the reactor coolant system remaining filled (20 x 90 percent). This frequency is:

  (2.1 x 0.20 x 0.90) = 0.38 events/year (A)

- Reactor Coolant System Forced Outage Frequency for Drained Maintenance

  This frequency is calculated as the product of the trip frequency (2.1 events per year) and the percentage of shutdowns that takes the plant to cold shutdown with the reactor coolant system drained (20 x 10 percent). This frequency is:

  (2.1 x 0.20 x 0.10) = 0.042 events/year (B)

Based on operating experience of Westinghouse plants in the US, the average number of controlled shutdowns, excluding refueling shutdown, is assumed to be 1.8 events per year. It is assumed that 80 percent of those cases require nondrained maintenance, 19 percent require drained maintenance without fuel removal, and 1 percent require drained maintenance with fuel removal.

Based on the controlled shutdown frequencies outlined above and the percentages of these outages that could take the plant to cold shutdown and drained conditions, the frequencies of the plant in cold shutdown conditions (i.e., reactor coolant system nondrained and drained conditions) are calculated as follows:

- Reactor Coolant System Controlled Shutdown Frequency for Nondrained Maintenance

  This frequency is calculated as the product of the controlled shutdown frequency (1.8 events per year), and the percentage of shutdowns that takes the plant to cold shutdown with the reactor coolant system kept filled (80 percent). This frequency is:

  (1.8 x 0.80) = 1.4 events/year (C)

- Reactor Coolant System Controlled Shutdown Frequency for Drained Maintenance

  This frequency is calculated as the product of the controlled shutdown frequency (1.8 events per year) and the percentage of controlled shutdowns that takes the plant to cold shutdown with the reactor coolant system drained (19 percent). This frequency is:

  (1.8 x 0.19) = 0.34 events/year (D)

- Shutdown Frequency for Fuel Removal Maintenance

  This frequency is calculated as the product of the controlled shutdown frequency (1.8 events per year) and the percentage of controlled shutdowns that takes the plant to refueling mode (1 percent), plus the refueling outage frequency (0.5 events per year). This frequency is:

$$[0.5 + (1.8 \times 0.01)] = 0.52 \text{ events/year} \qquad \text{(E)}$$

Based on the calculations above, the yearly frequencies of the three types of plant shutdown events are calculated as follows:

Nondrained maintenance frequency is:

Sum of the forced and controlled shutdown frequencies, (A + C) = 0.38 + 1.4 = 1.8 events/year.

Drained maintenance frequency is:

Sum of the forced and controlled shutdown frequencies, (B + D) = 0.042 + 0.34 = 0.38 events/year.

Refueling outages frequency is:

Controlled shutdown frequency, (E) = 0.52 events/year.

Based on shutdown frequencies calculated above of the three maintenance activities, the frequencies of the plant in the different shutdown phases are formulated as follows:

- Yearly frequency of the plant at ~~hot~~safe shutdown and~~/~~cold shutdown conditions is:

  1.8 + 0.38 + 0.52 = 2.7 events/year

- Yearly frequency of the plant at mid-loop condition is:

  0.38 + 0.52 = 0.90 events/year

54.3.2 Mission Times

The times in each phase are summarized in Table 54-4. These durations are based on the AP600 integrated refueling outage schedules from Reference 54-3. The mission times used for the initiating event frequencies for the mitigating systems are estimated by combining the times for the various operations conducted during the relevant shutdown modes. These mission times are evaluated in this section and summarized in Table 54-5.

No event tree is constructed fcr the first part of the cooldown (~~hot~~safe shutdown to 350°F and 400 psig), given the very limited duration of this part of the event. During this period, the yearly frequency of the three types of plant shutdowns is 2.7, and the duration is 8 hours. Therefore, this mode would occur only 22 hours per year, during which all the mitigating systems, except accumulators, are normally available. Therefore, transients that could occur in the shutdown period prior to ~~hot~~safe shutdown conditions are judged to be much less significant contributors to core damage than events evaluated during ~~hot~~safe and cold shutdown and mid-loop conditions and are not included in the quantitative shutdown evaluation.

Times are grouped in accordance with two main categories of plant states for which event trees are constructed, namely: ~~hot~~safe/cold shutdown condition with the reactor coolant system filled and intact; and mid-loop/vessel-flange condition with the reactor coolant system drained and depressurized.

A weighted average of the time spent in a ~~hot~~safe/cold shutdown condition for both categories of events (i.e., those ending in ~~hot~~safe/cold shutdown with reactor coolant system filled and intact and those ending in mid-loop/vessel-flange conditions) is used to calculate the frequencies of events for which that plant condition applies. Likewise, a weighted average of the time spent in mid-loop/vessel-flange condition for refueling and drained maintenance events is used to calculate the frequencies of events initiated when the plant is drained to mid-loop.

The ~~hot~~safe/cold shutdown calculation is as follows. From Table 54-4, the applicable times are:

- 24 hours for cooldown from 350°F to 160°F – phase A
- 16 hours for cooldown from 160°F to 130°F – phase A
- 24 hours for portion of return to power – phase F

This duration (24+16+24 = 64 hours) applies to the 1.8 events per year ending in nondrained ~~hot~~safe/cold shutdown and to the 0.9 events per year ending in mid-loop. Note that including the 24 hours for the beginning of the heatup/return to power is very conservative, based on the initiating events discussion provided earlier.

An allowance is also made for a nondrained maintenance time, which is assumed to be 200 hours per event. This 200-hour duration is believed to be conservative when used as an average maintenance period for each nondrained shutdown. This nondrained maintenance time applies to only the 1.8 nondrained events per year.

The ~~hot~~safe/cold shutdown (i.e., nondrained maintenance) mission time is the weighted average of these durations:

$$\frac{[\,1.8\text{ events/year} \times (64+200)\text{ hours/event}\,] + [\,0.9\text{ events/year} \times 64\text{ hours/event}\,]}{(1.8+0.9)\text{ events/year}} = 197\text{ hours/event}$$

or approximately 200 hours per event during ~~hot~~safe/cold shutdown.

The drained maintenance calculations are as follows.

For drained maintenance other than refueling, the applicable times from Table 54-4 are:

- 100 hours for drained maintenance, including getting into and out of mid-loop (phase B)
- 24 hours for refilling the reactor coolant system (phase E)

The 100-hour duration for drained maintenance is also believed to be conservatively long, based on experience at current plants and considering that AP600 has fewer components that could require drained maintenance than current plants. The resulting duration (100+24 = 124 hours) applies to the 0.38 drained maintenance events per year.

For refueling, the applicable times from Table 54-4 are:

- 39 hours for mid-loop operation (phase B)
- 55 hours for post-refueling operations/maintenance (phase D)
- 24 hours for refilling the reactor coolant system (phase E)

This duration (39+55+24 = 118 hours) applies to the 0.52 refueling events per year.

Then the total drained maintenance mission time is the weighted average of these times:

$$\frac{[\,0.38 \text{ events/year} \times 124 \text{ hours/event}\,] + [\,0.52 \text{ events/year} \times 118 \text{ hours/event}\,]}{(0.38 + 0.52) \text{ events/year}} = 197 \text{ hours/event}$$

Therefore, the time period to use in calculation of initiating event frequencies at drained conditions is 120 hours. For initiating events at nondrained conditions, the 200-hour time period is appropriate; however, the calculations for nondrained conditions include an additional factor of 10 percent as a conservatism, so that 220 hours has been used.

~~Hot~~Safe/Cold Shutdown Condition with Reactor Coolant System Filled and Intact

Phase A – Cooldown to Cold Shutdown

As discussed above, this phase is assigned a conservatively long mission time of 220 hours. The calculations in subsection 54.3.1 show that the frequency of being in ~~hot~~safe/cold shutdown conditions is 2.7 times per year. The mission time and frequency are reflected in the calculations of initiating event frequencies during the ~~hot~~safe/cold shutdown phase.

Mid-Loop/Vessel-Flange Condition with Reactor Coolant System Drained and Depressurized

Drained conditions encompass the activities described below. The activities of most significance to plant risk while drained are draining to mid-loop, drained maintenance, and post-refueling maintenance (phases B, D, and E).

As discussed earlier, activities for mid-loop/vessel-flange are assigned a mission time of 120 hours. The calculations in subsection 54.3.1 show that the frequency of being in mid-loop condition is 0.90 times per year. This mission time and frequency are reflected in the calculations of initiating event frequencies when the plant is at mid-loop.

Phase B – Reactor Coolant System Draindown

The reactor coolant system draindown (Phase B) is referred to as mid-loop or vessel-flange operation. This activity is carried out with the vessel head unbolted and the reactor coolant system temperature below 130°F. The operation has a duration of 39 hours and an estimated occurrence of 0.90 events per year.

Phase C – Refueling Cavity Fill

The plant is assumed to remain in the refueling mode (flooded cavity) for about 100 hours. However, no event tree is constructed for this plant condition because the core and cavity are flooded during this period.

Phase D – Post-Refueling Maintenance and Drain Refueling Cavity

During plant shutdown for refueling operations, it is estimated that post-refueling maintenance and inspection activities would take about 55 hours; the frequency for this activity is 0.52 events per year.

Phase E – Reactor Coolant System Fill and Gas Evacuation

The reactor coolant system fill and vent activity (phase E) lasts for about 24 hours. The shutdown frequency for this activity is estimated to be 0.90 events per year. Note that this activity is performed with the system closed. The contribution of this period could have been assigned to the nondrained events; however, it has been assigned with the drained events. This phase is included in the drained events because it would follow such events, and because previous shutdown evaluation results indicate that it is conservative to include the additional time in the drained cases.

Phase F – Cold ~~Startup~~Shutdown to Hot Standby

It is estimated that returning to power from refueling and drained outages requires about 121 hours and about 24 hours for nondrained outages. The initiating event frequency calculations for all of the shutdown events include an estimate of 24 hours to cover the period during the return to power operations prior to achieving mode 3.

The times for all of the phases discussed above are included in the total time used to calculate the failure rates for motor-operated valves in the systems analyzed for 'boron dilution accidents, described in subsection 54.4.12.

Table 54-4 summarizes the mission times and frequencies.

54.4 Event Tree Development

The event tree analysis for the AP600 shutdown assessment identifies the initiating events that are potentially significant contributors to core damage. Event trees are developed for the following initiating events occurring during the specified shutdown conditions:

- ~~Hot~~Safe/cold shutdown condition with the reactor coolant system filled and intact:
  - Loss of offsite power – LOSP-ND
  - Loss of decay heat removal capability, initiated from failure of normal residual heat removal system – RNS-ND
  - Loss of decay heat removal capability, initiated from failure of component cooling water or service water system – CCW-ND
  - Loss-of-coolant accident due to rupture of the normal residual heat removal system piping – LOCA-PR-ND
  - Loss-of-coolant accident due to inadvertent or spurious opening of the normal residual heat removal system motor-operated valve RNS-V024 – LOCA-V24-ND
- Transition from filled and depressurized reactor coolant system to mid-loop conditions:
  - Overdraining of the reactor coolant system during draindown to mid-loop – RCS-OD
- Mid-loop/vessel-flange condition with the reactor coolant system drained and depressurized:
  - Loss of offsite power – LOSP-D
  - Loss of decay heat removal capability, initiated from failure of normal residual heat removal system – RNS-D

  - Loss of decay heat removal capability, initiated from failure of component cooling water or service water system – CCW-D

  - Loss-of-coolant accident due to inadvertent or spurious opening of the normal residual heat removal system motor-operated valve RNS-V024 – LOCA-V24-D

- Boron dilution events during various shutdown conditions:

  - Diluted accumulator water injection – AIRCS

  - Reactor startup with chemical and volume control system in dilution mode following a loss of offsite power – STPCD

The initiating event frequencies for the accident scenarios that are quantified in the AP600 shutdown assessment are calculated in the following subsections and summarized in Table 54-6.

To evaluate the significance of these initiating events occurring during the different shutdown conditions, loss of offsite power, loss of normal residual heat removal, and loss of component cooling water or service water are modeled in separate event trees. Based on the operating configuration of the service water system and its total heat load during shutdown conditions, loss of the compressed and instrument air system (CAS) has been determined not to fail the service water system, and its failure is not considered to be an initiating event.

The fault trees used to calculate the normal residual heat removal system initiating event frequency do not include the component cooling water or service water system fault trees. As a result, the loss of normal residual heat removal system initiator only includes faults in the normal residual heat removal system. The loss of RNS support (component cooling water or service water) system is segregated into a separate initiating event that combines these two support systems; this initiating event frequency is calculated with the component cooling water or service water system fault trees.

Where the normal residual heat removal system is used in an event tree as a mitigating system, the event tree node is represented by the component cooling water and service water system fault trees linked to the normal residual heat removal system fault tree. Therefore, the required support provided to the normal residual heat removal system by the component cooling water and service water systems is modeled in the event trees.

Unless stated otherwise, component failure rates used to calculate initiating event frequencies in this section are derived from Chapter 32.

54.4.1 Event Tree LOSP-ND

The assumptions made in developing the event tree LOSP-ND are as follows:

- As documented in subsection 54.3.1, the frequency of plant shutdown is 2.7 events per year. The mission time of mitigating systems during the ~~hot~~safe/cold shutdown phase is 220 hours.

- LOSP-ND represents the initiating event for loss of offsite power during the cooldown phase of plant shutdown -- failure of the function means that loss of offsite power has occurred. The frequency of a loss of offsite power is 0.12 events per year (Reference 54-1). The duration of this shutdown phase is 220 hours. Therefore, the probability of loss of offsite power during this phase is: [(0.12 / 8760) x 220] = 3.01E-3.

  Therefore, initiating event LOSP-ND = 2.7 x 3.01E-03 = 8.1E-03 events/year.

- Diesel generator power source available (DGEN) -- the diesel generators are expected to operate if a loss of offsite power occurs. Failure of this function means that the diesel generator fails to start automatically and manually.

- Normal residual heat removal system automatic restart on diesel generators (ANR) -- in case of a loss of offsite power, the normal residual heat removal pumps trip, but an automatic restart of the pumps is provided, after diesel generators start and the electrical busses are sequenced. Failure of the function means that automatic restart of the normal residual heat removal pumps on the diesel generators has not occurred, or that the normal residual heat removal system or the diesel generators fail to operate during the mission time.

- Power recovery within 2 hours (GR2) -- the probability of recovering the grid within 2 hours is evaluated to determine the possibility of normal residual heat removal function recovery through the grid, in time to avoid core damage.

  After 2 hours, the vessel water level is estimated to go below the minimum hot leg level, resulting in the loss of normal residual heat removal pump suction. Therefore, water makeup and decay heat removal functions must be provided to prevent core damage.

  The 2 hours of allowable time is estimated based on the thermal-hydraulic analysis results performed for the Seabrook plant (Reference 54-4). This was used as a reference for the AP600 since the ratio of power to vessel water inventory for the two plants is similar. The thermal-hydraulic analyses performed for the Seabrook plant show the following:

- Initial reactor coolant system temperature of 140°F.

- Vessel full and closed with steam generator secondary side dry at 1 day after shutdown.

- Core uncovered in about 3.5 hours if residual heat removal is not isolated. Residual heat removal relief valves open at about 2.7 hours and water inventory loss starts.

- Core uncovered in about 6 hours if the residual heat removal system is isolated.

The results shown above indicate that the core will be uncovered in 3.5 hours if it is assumed that the operator does not isolate normal residual heat removal. It is assumed that the reactor coolant system temperature for AP600 could be around 200°F when offsite power is lost, which is 60°F higher than the temperature in the example cited above. Therefore, for AP600, it is estimated that the core will be uncovered in 2 hours if normal residual heat removal is not isolated. For manual actuation of systems required later in the sequence, a 1-hour time window is conservatively assumed in evaluating human error.

Success in recovering the grid within 2 hours eliminates the need for relying on diesel generators for mission completion. The effect on the event tree model is that the fault trees called for after the grid is recovered are the same as those used in the loss of decay heat removal cases, in which loss of offsite power has not occurred. The probability of recovering the grid within 2 hours is estimated to be 0.24~~ events per year~~ in Reference 54-1.

- Normal residual heat removal system manual restart after grid recovery (MRAGR) -- this event tree node represents the probability of failing to manually restart the normal residual heat removal pumps after grid recovery given the failure of the pumps to restart automatically on the diesel generators. Failure of this function is the failure to manually recover decay heat removal.

- Passive residual heat removal system (PMA) -- following a loss of the normal residual heat removal system, heat removal by manual actuation of the safety-related passive residual heat removal heat exchanger is required. It is expected that the operator will recognize the failure of normal residual heat removal system and the need for passive residual heat removal operation and actuate the passive residual heat removal system before automatic actuation through the low pressurizer level signal. For the case where the diesel generators fail, it is assumed that control power and instrument air also fail; in which case the passive residual heat removal air-operated valves fail open, and the system is expected to operate without an initiating signal or operator intervention. Failure of this function is failure of the passive residual heat removal heat exchanger to remove decay heat from the reactor coolant system. Where operator action is required, manual actuation of the passive residual heat removal heat exchanger must be performed in time to prevent an increase in the reactor coolant system pressure, which could cause the normal residual heat removal relief valve to open.

Opening of the normal residual heat removal relief valve results in the loss of water inventory similar to a loss-of-coolant accident for which passive residual heat removal is not useful. This same event (reactor coolant system pressure increase and opening of the relief valve) can also occur if passive residual heat removal fails, but this scenario does not change the event tree model because depressurization is always needed after this failure occurs.

- Core makeup tanks (CMT) -- as a result of loss of both safety-related and nonsafety-related decay heat removal systems, automatic safety-related cooling is provided by actuation of the core makeup tank on a low pressurizer level (through the protection and safety monitoring system or the diverse actuation system) as the reactor coolant is boiled off. Failure of this function is the failure to actuate both core makeup tanks, either automatically or manually.

- Reactor coolant system depressurization (RD) -- to meet long-term core cooling requirements, the depressurization system should be actuated to permit in-containment refueling water storage tank gravity injection. This actuation can be obtained either manually by the operator or automatically on core makeup tank low water level signals. Failure of this function is failure to actuate the minimum configuration of valves required for full reactor depressurization.

- Gravity injection (GI) -- after full depressurization of the reactor coolant system, in-containment refueling water storage tank gravity injection can be established~~ because the gravity injection lines are not isolated in this mode~~. This permits water from the in-containment refueling water storage tank to flow through the gravity injection lines into the safety injection lines. Failure of this function is the failure of both gravity injection lines to open. As stated in Section 54.6, water recirculation is not required prior to 72 hours and, therefore, is not reflected in the event tree logic.

The LOSP-ND event tree is shown in Figure 54-1.

54.4.2 Event Tree RNS-ND

RNS-ND represents the initiating event for the loss of decay heat removal capability due to failure of the normal residual heat removal system during the cooldown phase of plant shutdown. If one pump fails, it is assumed that an equilibrium temperature of about 150°F is reached, but core uncovery does not occur. Therefore, failure of this function is the failure of both normal residual heat removal pumps to continue to run for 220 hours. RNS-ND is evaluated as follows:

- Frequency of plant shutdown is 2.7 events per year, as discussed previously.

- Failure of normal residual heat removal system to operate during ~~hot~~safe/cold shutdown is evaluated in the RNC2 fault tree. The failure probability obtained from quantifying this fault tree is 3.56E-04.

Therefore, initiating event RNS-ND = 2.7 x 3.56E-04 = 9.6E-04 events/year

The frontline systems used in this event tree are the same as described previously in subsection 54.4.1. The RNS-ND event tree is shown in Figure 54-2.

54.4.3 Event Tree CCW-ND

CCW-ND represents the initiating event for the loss of decay heat removal capability due to failure of the component cooling water or service water system during the cooldown phase of plant shutdown. Fai'ııe of this function is the failure of both trains of component cooling or service water systems ιo operate for the mission time of 220 hours. CCW-ND is evaluated as follows:

- Frequency of plant shutdown is 2.7 events per year, as discussed previously.
- Failure of component cooling water or service water system to operate during ~~hot~~safe/cold shutdown is evaluated in the CSWF2 fault tree. The failure probability obtained from quantifying this fault tree is 1.2E-03.

Therefore, initiating event CCW-ND = 2.7 x 1.2E-03 = 3.2E-03 events/year

The functions of frontline systems used in this event tree are the same as described previously in subsection 54.4.1. The CCW-ND event tree is shown in Figure 54-3.

54.4.4 Event Tree LOCA-PR-ND

LOCA-PR-ND represents the initiating event for a loss-of-coolant accident during the cooldown phase of plant shutdown because of rupture of the piping within the normal residual heat removal system. This event is important because, if the operator does not isolate the normal residual heat removal system, it causes passive residual heat removal to be ineffective in mitigating the event.

- The initiating event frequency is calculated using two basic assumptions:

  a. The piping is assumed to have the same failure rate as at-power.

  b. The normal residual heat removal system consists of approximately 60 pipe sections, which include the piping in the containment that is not considered in the at-power case. The resulting frequency of 1.5E-05 events per year is calculated considering the following inputs:

- Pipe rupture failure rate: 4.25E-10 per section, per hour
- Number of pipe sections: 60
- Frequency of being in ~~hot~~safe/cold shutdown = 2.7 per year
- Mission time = 220 hours

Therefore, the normal residual heat removal system pipe rupture frequency is: 4.3E-10 x 60 x 2.7 x 220 = 1.5E-05 events/year.

- Manual isolation of the normal residual heat removal system given normal residual heat removal system pipe rupture (RHN-MAN04) -- if a break in the normal residual heat removal system piping occurs, it is assumed that the leak will have a relatively low flow rate; similar to the flow rate for a small loss-of-coolant accident (SLOCA). For this scenario, the operator is required to isolate the normal residual heat removal system in time to allow the passive residual heat removal heat exchanger to be placed in service. It is assumed that the time window to isolate the normal residual heat removal system is about 10 minutes. MAAP4 analysis discussed in Section 54.6 indicates that the time window for this operator action is longer than 10 minutes because the core makeup tanks would actuate automatically when the loss-of-coolant accident occurs; however, 10 minutes is selected as a conservative time window. This operator action is evaluated in Section 54.8; the human error probability (HEP) is 5.3E-02.

  The hardware failure probability of the motor-operated valves to isolate the normal residual heat removal system is estimated to be about an order of magnitude lower than the human error probability~~ of 5.2E-02~~. Therefore, hardware failures of these valves are not modeled for this scenario in the shutdown evaluation.

The frontline systems used in this event tree are the same as described previously, in subsection 54.4.1. The LOCA-PR-ND event tree is shown in Figure 54-4.

54.4.5 Event Tree LOCA-V24-ND

LOCA-V24-ND represents the initiating event for a loss-of-coolant accident during the cooldown phase of plant shutdown because of an inadvertent or spurious opening of normal residual heat removal system motor-operated valve RNS-V024. This event causes the reactor coolant to drain into the in-containment refueling water storage tank. For this scenario, the passive residual heat removal heat exchanger is ineffective in mitigating the event.

This initiating event is postulated as occurring because of any of the following failures:

- The operator inadvertently opens the normal residual heat removal valve RNS-V024 and fails to detect and reclose the valve. This operator action includes pre-accident system misalignment and post-accident operator recovery actions. This human error is identified as RHN-MANDIV and evaluated in Chapter 30. The human error probability (HEP) for this action is 1.0E-05. The failure probability of RHN-MANDIV is used only in the frequency of overdraining the reactor coolant system.

- Valve RNS-V024 spuriously opens due to erroneous signal from the protection and safety monitoring system-related instrumentation and control. The frequency is estimated to be 5.5E-05 events per year; this frequency is supported by data provided in Chapter 26. Therefore, the failure probability of this failure occurring during ~~hot~~safe/cold shutdown is: [2.7 x (5.5E-05 / 8760) x 220] = 3.7E-06 events/year.

- Catastrophic failure of the motor-operated valve has a failure rate of 5.0E-09 events/hour; this gives a failure frequency of: (2.7 x 5.0E-09 x 220) = 3.07E-06 events/year.

Additionally, normal residual heat removal system relief valve V021 sticking open is evaluated as a potential cause of loss of coolant. The shutdown scenario leading to this failure requires occurrence of both of the following:

1) The operator inadvertently starts the chemical and volume control system makeup pump, with failure to recognize the error and stop the pump. The time window for performing this task is assumed to be approximately 25 minutes. The diagnosis cues for recognizing this error are increasing system pressure and water level, with associated alarms annunciation. The human error evaluation for this operator action is assumed to be similar to that performed for RHN-MANDIV, discussed in a previous paragraph. Therefore, a human error probability of 1.0E-05 is estimated for this action.

2) If the operator fails to stop the chemical and volume control system makeup pump, valve V021 is expected to open in about 30 minutes to relieve the pressure and then reclose. However, in this case, valve V021 may fail to reclose due to mechanical failure. The component failure rate for valve V021 failing to reclose is 5.0E-03 failures per demand (Chapter 32).

Therefore, the scenario that could result in valve V021 being a potential source for loss-of-coolant generation has a failure probability of: (2.7 x 1.0E-05 x 5.0E-03) = 1.4E-07 events/year.

The frequency of initiating event LOCA-V24-ND is the summation of the four failures described above: (1.0E-05 + 3.7E-06 + 3.0E-06 + 1.4E-07) = 1.7E-05 events/year.

The frontline systems used in this event tree are the same as described previously, in subsection 54.4.1. The LOCA-V24-ND event tree is shown in Figure 54-5.

54.4.6 Event Tree RCS-OD

RCS-OD represents the initiating event for overdraining the reactor coolant system during operations for draining down the system to the required level for mid-loop conditions.

Two scenarios are postulated whereby overdraining of the reactor coolant system could occur. These are described and estimated as follows:

Scenario 1:

The hot-leg level (HL) instruments may fail and their failure go undetected during the 2-year fuel cycle. During draining of the reactor coolant system, the operator initially monitors the coolant level using the pressurizer wide-range level (PZR WRL) instrumentation, which are verified to operate correctly prior to draining down the reactor coolant system to the hot leg level. The hot leg instruments are designed to pick up the reactor coolant system level with readings that are consistent with the pressurizer wide-range level reading. The operator is required to observe inconsistency among the readings from the reactor coolant system level instruments and close the air-operated valves (AOVs) CVS-V045 or -V047 to prevent overdraining of the reactor coolant system. It is assumed that the operators have more than 3 hours to detect the hot leg instruments failure and close the required valves; the time window for draining from the hot leg level instrumentation readings to mid-loop condition is estimated to be more than one day.

The failure probability for this scenario is estimated as follows:

a) Random failure of both hot leg instruments is:

$(6.0E\text{-}07 \times 8760)^2 = 2.8E\text{-}05$

b) Common cause failure of hot leg instruments is:

$(6.0E\text{-}07 \times 8760 \times .05) = 2.6E\text{-}04$

Therefore, the failure probability of the hot leg instruments is: 2.8E-05 + 2.6E-04 = 2.9E-04.

c) Failure of the operator to recognize hot leg instruments failure and stop reactor coolant system draining is identified by RCS-MANOD1S. This operator action is evaluated in Section 54.8. The human error probability is 4.04E-04.

Therefore, the failure probability for scenario 1 is estimated to be 2.9E-04 x 4.0E-04 = 1.2E-07.

Scenario 2:

All level instruments are assumed to be operating correctly. The operator initiates draining through the chemical and volume control system and stops monitoring the reactor coolant system level. The reactor coolant system drains down to low hot leg level. Air-operator valves CVS-V045 and -V047 (arranged in series) are required to close automatically upon receipt of low hot leg level signals. These air-operated valves are assigned a mission time of 39 hours as the time for mid-loop operation. If automatic closure of the valves does not occur, the operators are required to close them. It is assumed that the operators have a short time window (approximately 5 minutes) to close the valves.

The failure probability for this scenario is estimated as follows:

a) Random failure of CVS-V045 and -V047 is: $(1.0E\text{-}06 \times 39)^2 = 1.5E\text{-}09$

b) Common cause failure of air-operated valves is: (1.0E-06 x 39 x .088) = 3.4E-06

From (a) and (b), the failure probability of the air-operated valves is: 1.5E-09 + 3.4E-06 = 3.4E-06.

c) Failure of air-operated valve automatic actuation signal is assigned a probability of 1.0E-04/demand. This failure probability is based on data provided in Chapter 26.

d) Failure of the operator to respond to low hot leg alarm and stop reactor coolant system draining is identified by RCS-MANOD2S. This operator action is evaluated in Section 54.8. The human error probability for this action is 1.39E-02. Credit for this operator action assumes that there is a hot leg alarm independent of the air-operated valve actuation signal.

From (c) and (d), failure of air-operated valves to close automatically and manually is: 1.0E-04 x 1.4E-02 = 1.4E-06.

Therefore, the failure probability for scenario 2 is estimated to be 3.4E-06 + 1.4E-06 = 4.8E-06.

Based on the estimates shown above, the initiating event frequency for RCS-OD is the sum of the failure probabilities for scenarios 1 and 2 multiplied by the yearly frequency of 0.9 for this event. That is, (1.2E-07 + 4.8E-06) x 0.9 = 4.4E-06 events/year.

Given the initiating event, the following top events are modeled in the event tree RCS-OD:

- Manually isolate normal residual heat removal system leak (MIRL) -- it is assumed that if overdraining of the reactor coolant system occurs, the operator will isolate the normal residual heat removal system (RHN-MAN04). Although the scenario for the operator action in this case is different from the scenario in subsection 54.4.5, the same human error probability is assigned for both cases. This operator action is evaluated in Section 54.8; the human error probability is 5.3E-02.

- Gravity injection (GI) -- the in-containment refueling water storage tank gravity injection lines are isolated in this phase of shutdown. Therefore, the operator must manually establish injection from the in-containment refueling water storage tank. This permits water from the in-containment refueling water storage tank to flow through one of the two gravity injection lines into the safety injection lines. Failure of this function is the failure to manually open the motor-operated valves in both gravity injection lines.

- Gravity injection from the in-containment refueling water storage tank via normal residual heat removal system suction line (GIRNS) -- the suction line of the normal residual heat removal system pumps is isolated durinr this phase of shutdown. Therefore, if in-containment refueling water storage tan! gravity injection fails, the operator must manually open motor-operated valve RNS-V023 to establish an alternative injection path from the in-containment refueling water storage tank. This permits water from the in-containment refueling water storage tank to flow through the normal residual heat removal system suction line into the reactor coolant system. Failure of this function is the failure to manually open the motor-operated valve in the suction line for the normal residual heat removal system pumps.

The RCS-OD event tree is shown in Figure 54-6.

54.4.7 Event Tree LOSP-D

The assumptions made in developing the event tree LOSP-D are as follows:

- As documented in subsection 54.3.1, the frequency of plant being at mid-loop is estimated to be 0.9 events per year. The mission time of mitigating systems during the ~~hot~~safe/cold shutdown phase is 120 hours.

- LOSP-D represents the initiating event for the loss of offsite power while the plant is at mid-loop. Failure of the function means that loss of offsite power has occurred. The frequency of a loss of offsite power when full-load rejection capability is unavailable is 0.12 events per year (Reference 54-1). The duration of this shutdown phase is 120 hours. Therefore, the failure probability is: [(0.12 / 8760) x 120] = 1.6E-03.

  Therefore, initiating event LOSP-D = 0.9 x 1.6E-03 = 1.5E-03 events/year.

Note that for the headings already used for the ~~hot~~safe/cold shutdown conditions, the same description and the same considerations are applicable when the plant is at mid-loop, with the following exceptions:

- The passive residual heat removal heat exchanger is not considered as a mitigating feature because it cannot function; the reactor coolant system is not pressurized when the plant is at mid-loop.

- During this shutdown condition, motor-operated valves V0121A and V0121B on the in-containment refueling water storage tank gravity injection lines and motor-operated valve V023 on the normal residual heat removal system pump suction line are closed to avoid draining the in-containment refueling water storage tank water due to reactor coolant system depressurization. Gravity injection requires manual or automatic opening of these motor-operated valves.

- Automatic depressurization system valves are open.

- Grid recovery within 1 hour (GR1) -- This event tree node represents the probability of recovering the grid within 1 hour. This scenario considers the possibility of normal residual heat removal system operation using offsite power sources without the need for diesel generator operation. After 1 hour, the vessel water level is estimated to go below the minimum hot leg level, resulting in loss of normal residual heat removal pump suction. The 1 hour of allowable time is estimated by considering the following:

  - Time to heat up the vessel water inventory during drained maintenance from 130°F to 212°F

  - Time to boil off the water inventory during drained maintenance conditions

  Using the plant thermal-hydraulic data and the conservative hypothesis that boiling occurs at atmospheric pressure, the following values are obtained:

  Time for heat up = 0.4 hour
  Time for boil off = 0.8 hour

  Therefore, a total time of 1.2 hours is assumed as the allowable time for normal residual heat removal function recovery during drained maintenance conditions. However, the time window for evaluating operator error to actuate the systems required in the event tree model is assumed equal to 1 hour, the same as for the ~~hot~~safe/cold shutdown condition.

  The probability of failing to recover the grid within 1 hour is estimated to be 0.42 (Reference 54-1).

The LOSP-D event tree is shown in Figure 54-7.

54.4.8 Event Tree RNS-D

RNS-D represents the initiating event for the loss of decay heat removal capability due to failure of the normal residual heat removal system when the plant is at mid-loop condition. If one pump fails, it is assumed that core uncovery does not occur. Therefore, failure of this function is the failure of both normal residual heat removal pumps to continue to run for 120 hours. RNS-D is evaluated as follows:

- Frequency of plant being at mid-loop is 0.9 events per year.

- Failure of normal residual heat removal system to operate during mid-loop condition is evaluated in the RNS2D fault tree file. The failure probability obtained from quantifying this fault tree file is 9.1E-05.

Therefore, initiating event RNS-D = 0.9 x 9.1E-05 = 8.2E-05 events/year.

The frontline systems used in this event tree are the same as described previously, in subsections 54.4.6 and 54.4.7. The RNS-D event tree is shown in Figure 54-8.

54.4.9 Event Tree CCW-D

CCW-D represents the initiating event for the loss of decay heat removal capability due to failure of the component cooling water or service water system when the plant is at mid-loop condition. Failure of this function is the failure of both trains of component cooling or service water systems to operate for the mission time of 120 hours. CCW-D is evaluated as follows:

- Frequency of plant being at mid-loop is 0.9 events per year.

- Failure of component cooling water or service water system to operate during mid-loop condition is evaluated in the CSWF2D fault tree file. The failure probability obtained from quantifying this fault tree file is 4.7E-04.

Therefore, initiating event CCW-D = 0.9 x 4.7E-04 = 4.2E-04 events/year.

The frontline systems used in this event tree are the same as described previously, in subsections 54.4.6 and 54.4.7. The CCW-D event tree is shown in Figure 54-9.

54.4.10 Event Tree LOCA-V24-D

LOCA-V24-D represents the initiating event for loss-of-coolant accident when the plant is at mid-loop condition because of inadvertent or spurious opening of normal residual heat removal system motor-operated valve RNS-V024. This event causes the reactor coolant to drain into the in-containment refueling water storage tank.

This initiating event is postulated as occurring because of any of the following failures:

- The operator inadvertently opens the normal residual heat removal valve RNS-V024 and fails to detect and reclose the valve. This human error is identified as RHN-MANDIV and evaluated in Chapter 30. The human error probability for this action is 1.0E-05.

- Valve RNS-V024 spuriously opens due to erroneous signal from the protection and safety monitoring system-related instrumentation and control. The frequency is estimated to be 5.5E-05 events per year; this frequency is supported by data (probability of spurious automatic depressurization system actuation) provided in Chapter 26. Therefore, the failure probability of this failure occurring during drained conditions is: [0.9 x (5.5E-05 / 8760) x 120] = 6.8E-07 events/year.

- Catastrophic failure of the motor-operated valve has a failure rate of 5.0E-09 events/hour; this gives a failure probability of: (0.9 x 5.0E-09 x 120) = 5.4E-07 events/year.

Additionally, the scenario that could result in valve V021 being a potential cause of loss of coolant is the same as that described in subsection 54.4.6. For mid-loop conditions, this scenario has a failure probability of: (0.9 x 1.0E-05 x 5.0E-03) = 4.5E-08 events/year.

The frequency of initiating event LOCA-V24-D is the summation of the failures described above; that is: (1.0E-05 + 6.8E-07 + 5.4E-07 + 4.5E-08) = 1.1E-05 events/year.

The frontline systems used in this event tree are the same as described previously, in subsections 54.4.6 and 54.4.7. The LOCA-V24-D event tree is shown in Figure 54-10.

Note that during drained conditions, a loss-of-coolant accident due to normal residual heat removal system pipe break is not considered to be a credible failure mode because the reactor coolant system is depressurized. Therefore, loss-of-coolant accident resulting from pipe break when the plant is drained to mid-loop is not considered in the shutdown assessment.

54.4.11 Boron Dilution Events (Reactivity Events)

The following list of potential boron dilution events has been identified for AP600:

- Addition of diluted accumulator water during refueling
- Addition of diluted core makeup tanks water during shutdown conditions
- Addition of diluted in-containment refueling water storage tank water during shutdown conditions
- Boron dilution events due to chemical and volume control system operation

The possibility of diluting the primary coolant as a consequence of other events is investigated to evaluate the potential for creating a situation where the reactor does not remain subcritical.

This possibility exists for loss-of-coolant accidents because water from various sources, with various boron concentrations, can replenish the primary circuit water inventory and change its average boron concentration. During a loss-of-coolant accident, water from the core makeup tanks, accumulators, the in-containment refueling water storage tank, and the chemical and volume control system can be injected into the primary circuit. The potential for primary circuit water dilution and reactor criticality being a concern depends on the boron concentration of the various water sources and the boron concentration required to keep the reactor subcritical. Because of the controls on boron concentration of the various water sources and the fact that dilution is of concern only during the beginning of a fuel cycle, the core damage frequency associated with dilution events during loss-of-coolant accidents is negligible.

Another aspect of the potential for boron dilution is the transfer of water to and from the primary circuit during a steam generator tube rupture event. Several scenarios regarding the timing, magnitude, and direction of mass transfer through the ruptured tube are possible. These scenarios are a function of the operation of plant systems (such as the passive residual heat removal system, the automatic depressurization system, and core makeup tanks) and the size of the tube rupture. The frequency of boron dilution as a consequence of a steam generator tube rupture event causing core damage is judged to be negligible and is not analyzed for shutdown.

Analysis of the potential boron dilution events is performed to identify the cases that require more detailed analyses (event tree construction). The cases for evaluation are discussed in the subsections that follow.

Accumulator Dilution, Followed by Injection During Shutdown Conditions (Event Tree: AIRCS)

These scenarios involve adding diluted water from the accumulators to the core when the vessel is depressurized below the setpoint of accumulator injection. During shutdown, the motor-operated valves provided on the injection lines are closed prior to depressurization to isolate the accumulators and to prevent flow from the accumulators into the vessel. If it is assumed that the water in one of the accumulators is diluted to a sufficiently low boron concentration, then it is possible to have potentially significant reactivity events.

Sequences 1A and 1B (shown in Figure 54-11) model catastrophic rupture and spurious opening of the accumulator motor-operated valves, resulting in accumulator water flowing into the vessel. The accumulator boron concentration, the degree of mixing, and the flow rate into the core determines whether a slug of diluted water can add reactivity rapidly enough to cause a serious power excursion.

Another possible scenario of injection of accumulator water into the vessel is that the operator fails to follow shutdown procedures, missing the procedural step of closing the motor-operated valves in the accumulator injection lines. An alarm is provided in the main control room to alert the operator to this error. When the reactor coolant system pressure falls below the accumulator internal pressure, water slowly makes its way from the accumulator into the vessel. This scenario is assumed to occur during shutdown conditions when the reactor coolant system is closed; if the reactor coolant system is open, the operator should be aware of the injection of accumulator water. However, with the reactor coolant system closed, there is insufficient free volume to allow accumulator injection, so the reactor coolant system is re-pressurized. When the reactor coolant system pressure increases above the accumulator internal pressure, accumulator water injection stops. This scenario is judged to be highly unlikely based on the expected performance of the accumulator, the unlikely operator error for this scenario, and the fact that a low boron concentration in the accumulator is not expected. Therefore, no event tree is constructed for it.

As indicated earlier, the event tree depicting the sequences 1A and 1B is shown in Figure 54-11.

The failure probabilities for headings in these event trees are calculated as follows:

- The frequency of the shutdown conditions equal to 2.7 events per year is obtained from subsection 54.3.1.

- AMD -- for the accumulator motor-operated valves de-energized event, a value equal to 0.001 is assigned for the human-error probability of failure to follow procedures that require the accumulator isolation valves to be closed when reactor coolant system pressure falls below 700 psig. Power lockout of motor-operated valves is also provided to prevent accidental opening of these valves on a spurious signal.

- NSOM -- an estimate of the probability that a motor-operated valve would spuriously open due to failure of the valve controls is obtained by assuming that the mean failure rate for motor-operated valves to remain closed is equivalent to that for remaining open. The failure rate of 1.4E-07 events per hour is obtained from Chapter 32. Assuming a mean outage time equal to 800 hours and taking into account that two accumulators are provided for the plant, the probability of the motor-operated valves spuriously opening is calculated to be 2.2E-04.

- NCFOM -- an estimate of the probability that a motor-operated valve would open suddenly (catastrophic failure) is obtained using the failure rate from Chapter 32, equal to 5.0E-09 events per hour. Assuming a mean outage time equal to 800 hours and taking into account that two accumulators are provided for the plant, the probability of the motor-operated valves suddenly opening is calculated to be 8.0E-06.

- ABCO -- the probability of accumulator dilution to a critically low boron concentration (conservatively assumed to be 1000 ppm) is from Reference 54-5 and is calculated to be 9.7E-05.

The resulting core power excursion frequencies of these sequences (1A and 1B) are estimated to be: 2.1E-09 events per year for 1A and 5.8E-11 events per year for 1B. Because these initiating event frequencies are sufficiently small and plant mitigating features exist, these events are not further evaluated.

Core Makeup Tank Dilution, Followed by Injection during Shutdown Conditions

No detailed analyses are performed based on the following considerations:

- The core makeup tank boron concentration (3500 ppm) is higher than the accumulator and in-containment refueling water storage tank boron concentration (2500 ppm)

- Weekly tests are provided for core makeup tank boron concentration

The assumed low probability of a critically low core makeup tank boron concentration coincident with either spurious automatic actuation of the core makeup tanks or spurious manual actuation due to operator error, leads to the conclusion that reactivity events due to core makeup tank boron dilution are highly unlikely.

In-Containment Refueling Water Storage Tank Dilution, Followed by Injection During Shutdown Conditions

These scenarios involve adding diluted water from the in-containment refueling water storage tank during one of the shutdown modes of operation. Two sequences are of concern: inadvertent actuation of safety injection and leakage of in-containment refueling water storage tank water into the vessel.

No detailed analyses are performed based on the following considerations:

- During shutdown, the differential pressure across the motor-operated valves in the in-containment refueling water storage tank injection lines is very low. Therefore, the probability of catastrophic failure of these valves is considered to be negligible.

- The probability of having a low boron concentration in the in-containment refueling water storage tank is much lower than the accumulators because of the significantly larger volume of water that must be diluted. Weekly tests for in-containment refueling water storage tank boron concentration are provided.

- The consequences of the motor-operated valves in the injection lines spuriously opening or leaking are less severe than for the accumulator injection case because the flow rate is much lower.

54.4.12 Boron Dilution Events Due to Chemical and Volume Control System Operation

Scenarios for boron dilution due to chemical and volume control system operation are identified considering the following plant conditions:

- ~~Hot~~Safe shutdown
- Cold shutdown
- Startup

The analysis of the boron dilution events due to chemical and volume control system operation takes into account the following specific design features provided for AP600:

- Two motor-operated valves are provided on the chemical and volume control system makeup pump suction line from the demineralized water storage tank. These valves close on the following signals:

  - Reactor trip signal

- Source range flux doubling signal
- Loss of offsite power
- Safeguards signal

- The chemical and volume control system three-way valve (V115) aligns to the boric acid tank on these same signals.

- Following a loss of ac power, the chemical and volume control system makeup pumps are loaded onto the nonsafety-related diesel generators but are not started automatically.

~~Hot~~Safe Shutdown

While the reactor is maintained in the ~~hot~~safe shutdown condition, xenon buildup occurs, increasing the degree of shutdown. It reaches a maximum of about 3 percent $\Delta K/K$ about 9 hours following shutdown. If rapid restart of the plant is required, dilution of the reactor coolant is performed to counteract this buildup. The reactor makeup subsystem mode switch is set in the DILUTE position, and makeup is initiated for a specified dilution volume.

A boron dilution event can occur if the operator fails to switch from the DILUTE position to the AUTO position when the plant is performing a reactor startup. However, frequent checks are carried out during this phase, and rod position is closely monitored. Therefore, this event is considered to be bounded by those events analyzed for normal operation. Also, since the reactor coolant pumps are running during this time, the unborated water mixes with the primary coolant water and localized slugs of unborated water do not occur. Therefore, the dilution event is very slow and could be mitigated by the operator. Therefore, this event is not evaluated any further.

Cold Shutdown

The reactor coolant system boron concentration is increased to the cold shutdown value before cooldown and depressurization of the reactor is initiated. To perform this boration, the operator sets the reactor makeup subsystem control switch to the BORATE position and selects the volume of boric acid solution to be added. This amount is predetermined to be sufficient to make the required change in boron concentration. A deviation alarm is provided within the chemical and volume control system. The final concentration is verified by reactor coolant sampling.

On a boron dilution protection signal, the chemical and volume control system makeup pump suction header is aligned to the boric acid tank by positioning three-way valve V115. In addition, dilution sources are isolated by the automatic closure of motor-operated valves V136A and V136B in the suction line from demineralized water storage tank.

The following events must occur for an inadvertent boron dilution to be caused by the chemical and volume control system:

- The two motor-operated valves in the chemical and volume control system line from demineralized water storage tank do not close either because of logic or hardware failure.

- The chemical and volume control system boric acid blending valve (V115) is in the DILUTE position because of logic or hardware failure.

- The operator must fail to stop the reactor coolant system dilution following the receipt of source range flux doubling signal alarms. The operator can stop the dilution by stopping the chemical and volume control system makeup pumps or by closing a discharge isolation valve.

Based on these considerations, the failure probability of this event is considered to be negligible. Further, the potential consequences of this event are not considered to be significant, because the flow rate of unborated water that makes its way into the vessel is low enough to allow mixing. The increase in reactor power is slow and could be mitigated by the operator. Thus, this event is not evaluated further.

Plant Startup

Plant startup is defined as the operations that bring the reactor from cold shutdown conditions to normal, no-load operating temperature and pressure, and subsequently to full-power operation. During filling and pressurization of the reactor coolant system, makeup water is drawn from the demineralized water storage tank and blended with boric acid from the boric acid tank to provide makeup at the correct boron concentration to maintain cold shutdown conditions. Reactor coolant system pressurization (through operation of letdown and charging control valves) and heating (through to reactor coolant pump and pressurizer heater input) are then performed.

Heatup is continued until a temperature of 250°F is achieved. At this point, the operator initiates dilution of the reactor coolant to the concentration required for criticality by placing the chemical and volume control system makeup subsystem in the DILUTE mode. The makeup pumps run automatically to supply demineralized water. This phase lasts about 2 to 4 hours.

Two different types of boron dilution events are identified for plant startup operations:

- A boron dilution due to adding more demineralized water than required. Since the reactor coolant pumps are running, sufficient mixing with primary coolant water occurs such that dilution is slow. No rapid power excursion occurs, indication is available to the operators, and this event has no significant consequences. This event is not further analyzed since it is bounded by the events considered in the previous sections.

- A boron dilution due to restart of reactor coolant pumps following a loss of offsite power. If the reactor coolant pumps are tripped and the operator fails to stop the dilution and then restarts the reactor coolant pumps, there is the possibility of a slug of diluted water entering the core with a consequential rapid power excursion. For the case where reactor coolant pumps stop during dilution operation, the following events must occur:

  - Loss of offsite power with consequential trip of reactor coolant pumps and chemical and volume control system makeup pumps.

  - Failure of the loss of offsite power automatic signal to close motor-operated valves on the chemical and volume control system line connected to the demineralized water storage tank, and mechanical failure of the motor-operated valves that prevent their closure.

  - Regulating valve V115 fails to align to the boric acid tank on a loss of offsite power signal.

  - The operator manually starts the chemical and volume control system makeup pumps. These pumps may be loaded onto the diesels following a loss of offsite power, but only manually. This allows a continued dilution of the reactor coolant system.

  - After grid recovery, the operator continues startup procedures and operates the reactor coolant pumps. This causes a slug of diluted water to enter the core.

  The combined probability of these events, even though some commonality could exist among them, is judged to be sufficiently low that it would not have a significant impact on the core damage frequency.

54.4.13 Endstates Summary

The sequences from the event trees quantified in the shutdown assessment are identified by the endstates LP-3BE, LP-ADS, and LPCBP in the event trees. LP-3BE is an intermediate state defined as low power, depressurized core damage; LP-ADS is an intermediate state defined as low power, not depressurized core damage; and LPCBP is used to define containment bypass sequences. The endstates designated OK are not core damage conditions. Endstates designated with other identifiers (e.g., 1A, FAIL) have been discussed as insignificant contributors and are not retained in the quantification.

As further described in Section 54.11, the low-power event core damage sequences (LP-3BE and LP-ADS sequences) are further split into substates using the plant damage state event trees discussed in that section.

54.5 Fault Tree Models for Shutdown and Low-Power Events

The fault trees for the shutdown and low-power events are listed in Table 54-7, which shows the fault tree names, the description of each tree, and the system or subsystem to which each tree belongs. These fault trees are used on the event trees where they are applicable. Fault trees that are used for both at-power and shutdown conditions are indicated by "Note 1" in Table 54-7.

The fault tree models reflect the system operations and basic assumptions documented in the corresponding system notebooks for the at-power PRA. Modeling assumptions for the shutdown assessment that are different from, or additions to, the assumptions reflected in the at-power PRA system analyses (Chapters 8 through 28 of the PRA) are documented in the notes for Table 54-7 or in the success criteria summary tables.

The test or maintenance unavailability status of systems assumed in the shutdown assessment for the different shutdown conditions is shown in Table 54-8.

54.5.1 Instrumentation and Control Modeling for Shutdown (Level 1)

This section presents the analysis of the instrumentation and control (I&C) support needed for the shutdown assessment. All three instrumentation and control systems that provide support, the protection and safety monitoring system, the diverse actuation system (DAS), and the plant control system (PLS), are included in this section. The basic techniques used in modeling the instrumentation and control subtrees, basic assumptions, and methods used in data development and quantification for shutdown are the same as those used in modeling the instrumentation and control support subtrees for the at-power PRA. Chapters 26, 27, and 28 provide a discussion of the techniques used to model, quantify, and link the instrumentation and control trees. This section lists the instrumentation and control subtrees needed to perform the shutdown assessment and evaluates specific instrumentation and control models when differences from the at-power case exist.

PMS/DAS Instrumentation and Control Modeling and Assumptions

The following frontline systems require instrumentation and control support from the protection and safety monitoring system and/or diverse actuation system in the shutdown models:

ADS	Automatic depressurization system
CIS	Containment isolation system
CMT	Core makeup tank
IRW	IRWST injection
PCS	Passive containment cooling system
PRHR	Passive residual heat removal

The following paragraphs discuss the instrumentation and control modeling, assumptions, data development, and quantification methods for protection and safety monitoring system and diverse actuation system.

Table 54-9 lists the protection and safety monitoring system and diverse actuation system fault trees needed for the shutdown assessment. Included in the table is the name of the frontline system fault tree that calls the instrumentation and control subtree for reference to the appropriate frontline system success configuration table. In most cases, the shutdown instrumentation and control fault tree is identical to an at-power instrumentation and control fault tree, exceptions include the support power model and the operator action assignments. Table 54-10 includes a list of the shutdown instrumentation and control models with an equivalent at-power model. Where the shutdown fault tree name differs from the at-power fault tree name only by ending in S, the power support model is changed to its equivalent S case, which removes the logic of the main generator breaker in the power trees. Table 54-13 lists all operator action assignments for the protection and safety monitoring system and diverse actuation system shutdown instrumentation and control fault trees.

Table 54-11 presents the success configuration summaries for the protection and safety monitoring system and diverse actuation system fault tree models that were either new models or present a significant difference from an equivalent at-power model. Reference is provided in the table to the frontline system tree success configuration table for further detail on the model.

PMS/DAS Instrumentation and Control Data Development and Quantification Methods

The data development techniques and quantification methods used in analyzing the protection and safety monitoring system and diverse actuation system instrumentation and control are the same as those used in the at-power analysis. This section documents only the new data used in the shutdown assessment.

New mission times are required for equipment modeled in instrumentation and control support trees used in modeling the mid-loop condition. The following fault trees require the new mission time:

IRW-IC1S IRW-IC2S IRW-IC3S IRW-IC4S
IRWIC1PS IRWIC2PS

The normal mission time assigned to the equipment of the protection and safety monitoring system and diverse actuation system is based upon a quarterly test interval. However, since the above trees are modeled for mid-loop operation, the output channels are assumed to be functionally tested prior to draining the primary system. System inputs are assumed to be either functionally tested or, in the case of the hot leg level transmitters, tested by operation during the primary system draindown. Therefore, the mission time assigned to the equipment covered by these tests is the amount of time that the plant is in the mid-loop condition. Table 54-12 documents data points calculated for the protection and safety monitoring system and diverse actuation system instrumentation and control models. Included in the table is a description of the data point and data value assigned.

Plant Control System Instrumentation and Control Modeling and Assumptions

The following frontline systems and support systems require instrumentation and control support from the plant control system in the shutdown models:

CCS	Component cooling water system
ECS	Main ac power system
RNS	Normal residual heat removal system
SWS	Service water system
VLH	Hydrogen control system

The following paragraphs discuss the instrumentation and control modeling, assumptions, data development, and quantification methods for the plant control system.

Table 54-14 lists the plant control system fault trees needed for the shutdown assessment. Included in the table is the name of the frontline or support system fault tree that calls the instrumentation and control subtree for reference to the appropriate success configuration table. In most cases, the shutdown instrumentation and control fault tree is identical to an at-power instrumentation and control fault tree; exceptions include the support power model and the operator action assignments. Table 54-15 includes a list of the shutdown instrumentation and control models with an equivalent at-power model. Where the shutdown fault tree name differs from the at-power fault tree name only by ending in S, the power support model is changed to its equivalent S case, which removes the logic of the main generator breaker in the power trees. Table 54-18 lists operator action assignments for the plant control system shutdown fault trees.

Table 54-16 presents the success configuration summaries for the plant control system fault tree models that were either new models or present a significant difference from an equivalent at-power model. Reference is provided in the table to the frontline system tree success configuration table for further detail on the model.

Plant Control System Data Development and Quantification Methods

The data development techniques and quantification methods used in analyzing the plant control system are the same as those used in the at-power analysis. This section documents only the new data used in the shutdown assessment.

New mission times are required for equipment modeled in plant control system support tree SWS-IC1X used in the initiating event frequency for loss of the component cooling water system/service water system. The normal mission time assigned to the equipment of the plant control system is based upon a quarterly test interval. In the case of the shutdown initiating event tree, the mission time is assigned to be 220 hours, which is the average amount of time spent in the shutdown condition. Table 54-17 documents all data points calculated for the plant control system models. Included in the table is a description of the data point and data value assigned.

54.5.2 Instrumentation and Control Modeling for Shutdown (Level 2)

The shutdown assessment requires additional instrumentation and control subtrees for quantifying the bridge event trees used to evaluate plant damage substates for use in the Level 2 study. Tables 54-19 through 54-21 list the instrumentation and control subtrees used for the plant damage state quantification, their equivalent at-power model, and the operator actions modeled in the subtrees. Refer to Chapters 26 and 27 of the PRA report for details on these models.

54.6 Success Criteria

There are some differences between the shutdown and at-power success criteria for some plant safety functions. The differences are mainly due to a much lower decay heat level applicable to the shutdown cases. In general, success is achieved with fewer systems and components at shutdown. The success criteria modeled for the core cooling function during shutdown conditions are included in Tables 54-22a through 54-49. Tables 54-50 and 54-51 present the automatic depressurization system success criteria that are used for the plant damage state event trees, as discussed in subsection 54.11.

The success criteria differences include:

- To meet the core cooling function requirements in the long term for the shutdown case, the success of in-containment refueling water storage tank gravity injection is sufficient; engineering design evaluations show that for shutdown, recirculation of water in the reactor pressure vessel is not necessary prior to 72 hours, as it is in the at-power case.
- During mid-loop/vessel-flange operation, the automatic depressurization system valves for stages 1, 2, and 3 are open and, therefore, the reactor coolant system is already depressurized for effective gravity injection.
- Although the chemical and volume control system makeup function is available during shutdown, it is not credited to mitigate an overdraining of the reactor coolant system during draindown to mid-loop initiating event.
- The mission times used in the fault tree analyses are included in the tables provided in Section 54.5 and in this section for the respective systems.
- The electrical power fault trees used for the at-power assessment were modified as necessary to exclude the plant generator as a source of ac power during shutdown conditions.

Timing of Events

Only the amount of time required to recognize loss of the decay heat removal function plays an important role in the progression of the events evaluated during shutdown conditions. This time period is determined (Section 54.4) to be 2 hours for the nondrained cases and 1.2 hours for the mid-loop/vessel-flange operation cases.

54.6.1 MAAP4 Code Analysis for Shutdown Success Criteria

MAAP4 analyses were performed to define the automatic depressurization system success criteria for AP600 at shutdown conditions. These analyses constitute an addendum to the analyses performed for the at-power PRA that are documented in Appendix A. The shutdown event trees are simplified; therefore, there are fewer MAAP4 cases to consider. In addition, the plant starts from different initial conditions, and there are some differences in system alignments and protection signals available. The specifics of these differences are given in subsections 54.6.2 and 54.6.3.

54.6.2 MAAP4 Parameter File

The MAAP4 parameter file was modified for shutdown conditions, as noted in the following subsections.

Initial Conditions

The assumed shutdown conditions for AP600 are defined in Table 54-52.

The MAAP4 analyses address the shutdown conditions where reactor coolant system cooling is provided by the normal residual heat removal system and the reactor coolant system is intact. These conditions are in bold type on Table 54-52. The base set of MAAP4 analyses are run with the highest initial temperature and pressure. In addition, the initial steam generator pressure and core power are modified, as appropriate.

The initial steam generator level is the same at shutdown conditions as at power, but the density of the water is higher; therefore, the initial mass is higher at shutdown.

The initial core power is chosen to be 1 percent of the full-power condition. This core power level is reached 1 to 2 hours after shutdown. Although the shutdown cases being analyzed are more likely to have been shut down for a longer period, 1 percent initial power was chosen because it is bounding. The core power is further reduced as the transient progresses.

Core Makeup Tank Actuation

When the plant is shut down, the following signals are blocked:

- Low-1 pressurizer pressure

- Low steamline pressure
- Low-3 cold leg temperature

These blocked signals are safety injection signals. The only remaining safety injection signal that can actuate the core makeup tank is high-1 containment pressure. Although this is not expected to be reached during the shutdown cases (since the containment may be open), the high containment pressure is left in the core makeup tank actuation logic. Other core makeup tank actuation signals available for shutdown conditions are:

- Low-2 pressurizer level
- Low steam generator level (wide-range) coincident with high hot leg temperature

Normal Residual Heat Removal System

In success criteria cases for the at-power PRA, the normal residual heat removal system is modeled in injection mode, providing water inventory to the reactor coolant system in an open-system mode where water is drawn from the in-containment refueling water storage tank. In the shutdown cases, the normal residual heat removal system operates with the reactor coolant system as a closed-system, where water is recirculated and heat is removed through normal residual heat removal heat exchangers. One effect of the different operating modes is the shutoff head of the normal residual heat removal system pumps. In the cases starting from full power, the normal residual heat removal system is not able to inject until the system pressure is below approximately 175 psia. In the shutdown cases, the normal residual heat removal system normally operates at about 325 psia.

In the shutdown cases, it is assumed that the reactor coolant system has been on normal residual heat removal system when the accident starts. However, as explained later, normal residual heat removal system is not explicitly modeled in the shutdown cases.

54.6.3 MAAP4 Input Changes

There are several changes that were made due to shutdown conditions.

1) The containment may be open during the shutdown modes being represented in the analyses. Because this is limiting for in-containment refueling water storage tank injection, all of the MAAP4 analyses assume that the containment is open and that there is no containment pressurization from any release from the reactor coolant system.

2) In full power cases, non-loss-of-coolant accident loss-of-heat-removal events result in the reactor coolant system pressure increasing to approximately 2500 psia, the pressurizer safety valve setpoint. However, in the shutdown modes, when the reactor coolant system is connected to the normal residual heat removal system, the pressure is limited by a relief valve in the normal residual heat removal system. It is assumed in the loss of normal residual heat removal system events that the normal residual heat removal system remains connected to the reactor coolant system, and this relief valve

will limit the reactor coolant system pressure. The relief valve opens when the pressure reaches ~580 psia. It will relieve approximately 550 gpm. Although the actual valve has not been selected, most relief valves close within 5 to 15 percent of the opening pressure. In tne MAAP4 model, the closing pressure was selected at 536 ρsia, which is 7.5 percent below the opening pressure.

To simulate the normal residual heat removal system relief valve in MAAP4, a break on the hot leg is opened as the reactor coolant system pressure exceeds the open set pressure, and the break is closed as the reactor coolant system drops below the close set pressure. The effect of this model on the reactor coolant system pressure is shown in Figure 54-12. The mass flow rate through the relief valve is shown in Figure 54-13. The relief flow rate is assumed to be approximately 550 gpm. This translates to approximately 30 kg/sec.

In this example, the reactor coolant system pressure exceeds the set pressure of 580 psia at about 7500 seconds, although the relief valve is open. This is when the void fraction of the reactor coolant system starts to increase, and the mass release through the relief valve (hot leg break) is reduced. It is not known whether this prediction is consistent with the actual system response, since the MAAP4 model on the hot leg is only a rough approximation of the relief valve within the normal residual heat removal system. However, the only impact of the valve relief rate is on the timing of the event. The MAAP4 model just described is sufficient for the purposes of defining the automatic depressurization system success criteria. This normal residual heat removal system relief model is used in all loss of decay heat removal events. It is not a factor in the MAAP4 cases that model a break in the normal residual heat removal system.

3) One of the initiating events is a break in the normal residual heat removal system. In this scenario, the break size is unknown, and the amount of water that is returned to the reactor coolant system is unknown. It is assumed that the normal residual heat removal system pumps continue to actively pump water from the reactor coolant system until the normal residual heat removal system pumps trip due to voiding in the hot leg. The flow rate of the normal residual heat removal system pumps is approximately 3500 gpm. If the break size or location allows some of the normal residual heat removal system flow to return to the reactor coolant system, the net loss of reactor coolant system inventory could be less.

A method could not be found to directly model a forced flow rate being pumped from the reactor coolant system hot leg. Options that were tried include the use of the letdown flow model in MAAP4; however, the suction does not come from the hot leg, and flow was terminated prior to the desired time. Another option was to try to force a break flow rate based on the hot leg water level. However, re-setting an output variable such as break flow only resets the output value and does not result in any differences in the related systems calculations. Therefore, the method used to simulate the inventory lost through the reactor coolant system is to model a break on the hot leg, with a break area that changes based on the hot leg water level. This allows a large break size to simulate a high forced flow rate from the reactor coolant system. When the outlet from the reactor coolant system to the normal residual heat removal system uncovers and the normal residual heat removal system pumps trip, the pathway is assumed to remain open for any steaming of the reactor coolant system coolant. This is modeled by reducing the break area.

Cases are run with net values of 3500 gpm, 2000 gpm, and 1000 gpm being lost from the reactor coolant system due to the normal residual heat removal system pumps and a break within the normal residual heat removal system. MAAP4 runs were done to find the break area that would approximate these flow rates. With a given break area, the break flow rate changes as the event progresses. Therefore, an average break flow rate is calculated by integrating the break flow, then dividing it by the time to determine the average flow rate that has been lost when the top of the hot leg uncovers. The results of this task are illustrated in Figures 54-14, 54-15, and 54-16 for the 3500, 2000, and 1000 gpm cases, respectively.

54.6.4 Definition of MAAP4 Cases from Event Trees

There are four event trees that credit automatic depressurization system actuation within some of the success paths (paths that include successful injection from the in-containment refueling water storage tank). These are RNS-ND, CCW-ND, LOSP-ND, and LOCA-PR-ND.

For the MAAP4 analyses, the first three event trees are very similar. They are initiating events that can be summarized as a loss of decay heat removal capability. The loss-of-offsite power case includes a reactor coolant pump (RCP) trip at the beginning of the event; the reactor coolant pump is assumed to operate in the other events until a core makeup tank actuation signal is reached.

In the loss-of-decay-heat-removal cases, the reactor coolant system pressurizes until coolant inventory is lost through the normal residual heat removal system relief valve. The loss of inventory causes a core makeup tank actuation signal on low pressurizer level. If a core makeup tank is successfully actuated, an automatic depressurization system actuation signal will be generated by a low core makeup tank level signal (MAAP4 cases sd1 and sd2). If both core makeup tanks fail, then the automatic depressurization system must be manually actuated. The cue for operator action is assumed to be low normal residual heat removal system flow (or low component cooling water/service water flow), which occurs at the beginning of the event. Therefore, operator action times for manual automatic depressurization system (MAAP4 cases sd4 and sd5) are measured from the beginning of the event.

The fourth event tree is an normal residual heat removal system pipe rupture. If the operator is able to isolate the break, the event will progress as a loss of decay heat removal case. If the normal residual heat removal system break is not isolated, the event is a loss-of-coolant accident, with the loss of inventory being pumped from the reactor coolant system hot leg by the normal residual heat removal system pumps. The return rate of normal residual heat removal system water to the reactor coolant system is unknown for this scenario; therefore, three sets of cases were done with the net loss from the reactor coolant system being 3500 gpm, 2000 gpm, and 1000 gpm. When the connection to the normal residual heat removal system uncovers, the normal residual heat removal system pumps trip. It is assumed that the pathway to the normal residual heat removal system remains open and that ıeactor coolant system inventory continues to be lost, although not pumped. The successful actuation of the core makeup tank and thus, automatic depressurization system, are modeled in MAAP4 case sd3. The failure of core makeup tanks, and thus, manual automatic depressurization system, are modeled in MAAP4 case sd6. The operator cues for initiating automatic depressurization system are:

- Decreasing reactor coolant system coolant
- Low pressurizeı level
- Low normal residual heat removal system flow
- High normal residual heat removal system water sump level

Although these cues could occur at different times, depending on the break size and location, the MAAP4 operator action times are measured from the beginning of the event. Operator action times of 30 minutes, 60 minutes, and 2 hours were analyzed.

Details of the MAAP4 models for these events were presented in subsection 54.6.3. The naming of each MAAP4 case is further identified in subsection 54.6.5.

54.6.5 Results From MAAP4 Analyses

Table 54-53 summarizes the MAAP4 cases that were analyzed. This table contains information on the success criteria case, the initiating event, the core makeup tank assumption, the automatic depressurization system assumption, the MAAP4 case name, and a summary of the peak core temperature. The definition for each automatic depressurization system success criterion is shown to be:

Three out of four lines of automatic depressurization system stages 2 and 3 open
OR
One out of four lines of automatic depressurization system stage 4 open.

For the MAAP4 cases that show success with the automatic depressurization system success criterion above, the timing of major events in the transient is summarized in Tables 54-54a through 54-54e. Note that if a case led to core uncovery, then the peak core temperature listed is the peak after core uncovery.

Generally, the system response is not challenged and the peak core temperatures remain low. This is primarily attributed to the low decay heat. However, note that the decay heat assumption made for these analyses starts at 1 percent of full power which is a higher level than would be anticipated during these shutdown modes of operation. Therefore, the decay heat assumption in these analyses is quite conservative.

54.7 Common Cause Analysis

In general, equipment and software common cause failures occurring during plant shutdown conditions are assumed to be similar to the common cause failures considered in the at-power evaluation. These common cause failures are documented in Chapter 29.

Common cause failures evaluated specifically for the equipment operated during plant shutdown conditions are documented in Table 54-55.

54.8 Human Reliability Analysis

This section documents the operator actions that are evaluated and used in the shutdown assessment. These operator actions are selected on the basis that, if the actions are performed inadvertently or, if required, and not performed correctly, plant support systems could be disabled or an accident could be initiated.

Operator actions for the AP600 PRA are documented in Chapter 30, which includes operator actions used for the at-power and/or shutdown plant conditions.

Additional operator actions used in the shutdown assessment are described in subsection 54.8.1; these operator actions are evaluated using the methodology and basic assumptions outlined in Chapter 30. All operator actions used in the shutdown evaluation are summarized in Table 54-56.

54.8.1 Operator Actions Calculated

CAN-MAN0S (Locally Close Manual Valve CAS-V204 to Isolate Containment)

The CAN-MAN0S operator action evaluates the probability of failure to recognize the need and failure to close manual valve V204 in the instrument air system for containment isolation given core damage as a result of an event initiated during shutdown conditions. For this scenario, the control room operators are required to recognize the need for containment isolation, and notify the auxiliary operators to close valve V204 locally.

The performance shaping factors used in the evaluating CIT-MAN0S are applied to the CAN-MAN0S operator action. Therefore, the following assumptions are used as input to the quantification of CAN-MAN0S:

- Procedure (LONG/SHORT): SHORT
- Time Window: 2 hours
- Estimated Actual Time: approximately 40 minutes
- Cues: Primary; high containment radiation; high containment pressure; high containment temperature; (It is assumed that response to three alarms is required)

- Stress Level: HIGH; (multiplier of 5 is applied)
- Recovery by: Shift technical advisor (STA) and senior reactor operator (SRO) for recovery of control room detection; auxiliary operator for recovery of local action

CAN-MAN0S is quantified as follows:

Item No.	Subtask Description for CAN-MAN0S	Mean HEP	Stress Level	Source (HRA Guidebook); Table 31A-4 (Item)	Recovery	Modified HEP
1	Failure to respond to one of three alarms	2.7E-03	5	(48)	2.19E-02	2.96E-04
2	Select wrong local valve to isolate CAS containment penetration (V204)	3.7E-03	5	(27)	4.32E-01	7.99E-03
3	Omit action to provide suction from SFP	3.8E-03	5	(9)	4.32E-01	8.21E-03
	TOTAL HEP = Item 1 + Item 2 + Item 3					1.65E-02

Note:

1. Recovery for control room actions is evaluated by: "Item 40 in HRA data table" x "stress level" x "0.1" x "0.54"; where, Item 40 represents recovery by STA, equated to 8.1E-02; 0.1 is recovery by SRO; and 0.54 is credit for slack time beyond 1 hour.
2. Recovery for local actions is evaluated by: "Item 38 in HRA data table (1.6E-01)" x "stress level" x "0.54."
3. "Modified HEP" = "Mean HEP" x "stress level" x "recovery factor."

RHN-MAN04 (Isolate the Normal Residual Heat Removal System during Shutdown Conditions)

The RHN-MAN04 operator action evaluates the probability of failure to recognize the need and failure to isolate the normal residual heat removal system, given rupture of the normal residual heat removal system piping during ~~hot~~safe/cold shutdown conditions.

For this scenario, the control room operators are required to detect the occurrence of normal residual heat removal system pipe rupture and isolate the normal residual heat removal system to allow passive residual heat removal to be placed in service.

The configuration of the normal residual heat removal system valve allows the operators to isolate the normal residual heat removal system by closing only RNS-V022 or by closing combinations of (RNS-V001A and -V002A) or (RNS-V001B and -V002B). This model considers closure of RNS-V022 only; modeling the other valves is considered to be a recovery option in case the operator has not successfully closed RNS-V022. In that regard, this evaluation is believed to be conservative.

The following assumptions are used as input to the quantification of RHN-MAN04:

- Procedure (LONG/SHORT): SHORT
- Time Window: 10 minutes
- Estimated Actual Time: approximately 6 minutes
- Cues: Primary-decreasing reactor coolant system coolant, low pressurizer level, low hot leg level, low normal residual heat removal system flow, high normal residual heat removal system sump water level

  Secondary-low reactor coolant system pressure (if reactor coolant pump running), high core exit temp, high radiation level in sump building, containment temp./ press./ radiation not increasing; (It is assumed that response to at least five alarms is required; only the primary cues listed above are considered)
- Stress Level: HIGH, (multiplier of 5 is applied)
- Recovery by: No recovery is applied to this task

RHN-MAN04 is quantified as follows:

Item No.	Subtask Description for RHN-MAN04	Mean HEP	Stress Level	Source (HRA Guidebook); Table 31A-4 (Item)	Recovery	Modified HEP
1	Failure to respond to one of five alarms	8.0E-03	5	(50)	N/A	4.00E-02
2	Select wrong control for RNS-V022	1.3E-03	5	(29)	N/A	6.50E-03
3	Omit action to close RNS-V022	1.3E-03	5	(8)	N/A	6.50E-03
	TOTAL HEP = Item 1 + Item 2 + Item 3					5.30E-02

Note:
1. "Modified HEP" = "Mean HEP" x "stress level."

RCS-MANODS1 (Close AOVs CVS-V045 or -V047, Given Failure of HL Instruments)

The RCS-MANODS1 operator action evaluates the probability of failure to observe failure of the hot leg level instruments and failure to close the air-operated valves CVS-V045 and V047 to preclude initial overdraining of the reactor coolant system, during draining of the system to mid-loop.

For this scenario, the operators initially monitor the coolant level using the pressurizer wide-range level (PZR WRL) instrumentation, which is assumed to be reading accurately. Subsequently, the hot leg level instruments are designed to pickup the reactor coolant system level with readings that are consistent with the pressurizer wide-range level reading. The operator is required to observe such inconsistency among the readings from the reactor coolant system level instruments and close the air-operated valves CVS-V045 or -V047 to prevent overdraining of the reactor coolant system.

The following assumptions are used as input to the quantification of RCS-MANODS1:

- Procedure (LONG/SHORT): SHORT
- Time Window: > 3 hours
- Estimated Actual Time: ~ 5 minutes
- Cues: Inconsistency among reactor coolant system level readings from pressurizer wide-range level instrument and hot leg level instruments
- Stress Level: HIGH; (multiplier of 5 is applied)
- Recovery by: Shift technical advisor and senior reactor operator

RCS-MANODS1 is quantified as follows:

Item No.	Subtask Description for RCS-MANODS1	Mean HEP	Stress Level	Source (HRA Guidebook); Table 31A-4 (Item)	Recovery	Modified HEP
1	Failure to detect inconsistency between level instruments	1.2E-03	5	(18)	2.19E-02	1.31E-04
2	Select wrong controls for CVS-V045 & -47; (total dependency is assumed)	1.2E-03	5	(28)	2.19E-02	1.31E-04
3	Omit action to close VS-V045 & -47; (total dependency is assumed)	1.3E-03	5	(8)	2.19E-02	1.42E-04
	TOTAL HEP = Item 1 + Item 2 + Item 3					4.04E-04

Note:

1. Recovery for control room actions is evaluated by: "Item 40 in HRA data table" x "stress level" x "0.1" x "0.54"; where, Item 40 represents recovery by STA, equated to 8.1E-02; 0.1 is recovery by SRO; and 0.54 is credit for slack time beyond 1 hour.
2. "Modified HEP" = "Mean HEP" x "stress level" x "recovery factor."

RCS-MANODS2 (Close Air-Operated Valves CVS-V045 or -V047, Given Failure of Valves to Close Automatically)

The RCS-MANODS2 operator action evaluates the probability of failure to detect failure of automatic closure of air-operated valves CVS-V045 and -V047, and failure to manually close the valves, when low hot leg level is reached during draining of the system to mid-loop.

For this scenario, the operator initiates draining through the chemical and volume control system and stops monitoring the reactor coolant system level. The reactor coolant system drains down to low hot leg level. Air-operator valves CVS-V045 and -V047 are required to close automatically upon receipt of low hot leg level signals. If automatic closure of the valves does not occur, the operators are required to close them.

The following assumptions are used as input to the quantification of RCS-MANODS2:

- Procedure (LONG/SHORT): SHORT
- Time window: 5 minutes
- Estimated actual time: 1 minute
- Cues: Low hot leg level alarm; AOVs in open position (It is assumed that when the alarm is annunciated the operator is required to manipulate the controls for closing the valves even though automatic closure may have been successful)
- Stress level: HIGH; (multiplier of 5 is applied)
- Recovery by: No recovery is applied to this task

RCS-MANODS2 is quantified as follows:

Item No.	Subtask Description for RCS-MANODS2	Mean HEP	Stress Level	Source (HRA Guidebook); Table 31A-4 (Item)	Recovery	Modified HEP
1	Failure to respond to one alarm	2.7E-04	5	(46)	N/A	1.35E-03
2	Select wrong controls for CVS-V045 & -47; (total dependency is assumed)	1.2E-03	5	(28)	N/A	6.00E-03
3	Omit action to close VS-V045 & -47; (total dependency is assumed)	1.3E-03	5	(8)	N/A	6.50E-03
	TOTAL HEP = Item 1 + Item 2 + Item 3					1.39E-02

Note:

1. "Modified HEP" = "Mean HEP" x "stress level."

RHN-MAN05 (Initiate Gravity Injection from IRWST via Normal Residual Heat Removal System Suction Line)

The RHN-MAN05 operator action evaluates the probability of failure to recognize the need and failure to initiate gravity injection via the normal residual heat removal system hot leg connection by using the normal residual heat removal system line from the in-containment refueling water storage tank to the normal residual heat removal system pumps suction header.

For this scenario, the control room operators are required to detect the gravity injection through the in-containment refueling water storage tank injection lines has failed due to failure of the motor-operated valves on the injection lines. The time window used for operator action IWN-MAN00 is also applicable to operator action RHN-MAN05; this time window is assumed to be greater than 60 minutes.

The following assumptions are used as input to the quantification of RHN-MAN05:

- Procedure (LONG/SHORT): SHORT
- Time window: > 60 minutes
- Estimated actual time: approximately 10 minutes
- Cues: Primary - high core exit temperature, check valves on injection lines remain closed, hot leg level instruments do not show increase in reactor coolant system level; (It is assumed that response to one alarm related to high core exit temperature is required)
- Stress level: HIGH (multiplier of 5 is applied)
- Recovery by: shift technical advisor and senior reactor operator. Slack time beyond one hour is not credited to this operator action.

RHN-MAN05 is quantified as follows:

Item No.	Subtask Description for RHN-MAN05	Mean HEP	Stress Level	(HRA Guidebook); Table 31A-4 (Item)	Recovery	Modified HEP
1	Failure to respond to one of one alarm for high core exit temperature	2.7E-04	5	(50)	4.05E-02	5.47E-05
2	Omit action to check status of check valves	1.3E-03	5	(8)	4.05E-02	2.63E-04
3	Misread status of check valves	1.2E-03	5	(22)	4.05E-02	2.43E-04
4	Omit action to check RCS level	1.3E-03	5	(8)	4.05E-02	2.63E-04
5	Misread RCS level	1.2E-03	5	(17)	4.05E-02	2.43E-04
6	Omit action to open MOV RNS-V023	1.3E-03	5	(8)	4.05E-02	2.63E-04
7	Select wrong control for MOV RNS-V023	1.3E-03	5	(29)	4.05E-02	2.63E-04
	TOTAL HEP = Item 1 + Item 2 + Item 3 + Item 4 + Item 5 + Item 6 + Item 7					1.60E-03

<u>Note</u>:

1. Recovery for control room actions is evaluated by: "Item 40 in HRA data table" x "stress level" x "0.1"; where, Item 40 represents recovery by STA, equated to 8.1E-02; and 0.1 is recovery by SRO.
2. "Modified HEP" = "Mean HEP" x "stress level" x "recovery factor."

54.8.2 Conditional Human Error Probabilities

The conditional human error probabilities calculated for shutdown evaluation are presented in Table 54-57. The conditional probabilities were calculated in the same manner as described in Section 30.7.

54.9 Fault Tree Quantification

The fault trees used in the shutdown assessment are listed in Table 54-7. The fault trees are quantified using the same method that was followed in quantifying the at-power PRA. The quantification method is documented in Chapter 33. The quantification of these fault trees yield the following failure probabilities, as well as the cutsets that are used as inputs to the quantification of the event trees.

- ADAS -- 3.25E-06. The automatic depressurization system is automatically actuated and fails to achieve full reactor coolant system depressurization for transients during ~~hot~~safe/cold shutdown conditions.

- ADTS -- 3.00E-05. The automatic depressurization system is manually actuated following failure of the core makeup tanks and fails to achieve full reactor coolant system depressurization during ~~hot~~safe/cold shutdown conditions.

- ADALS -- 3.88E-06. The automatic depressurization system is automatically actuated and fails to achieve full reactor coolant system depressurization following a loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- ADLS -- 3.11E-05. The automatic depressurization system is manually actuated following failure of the core makeup tanks and fails to achieve full reactor coolant system depressurization following a loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- CIST -- 1.71E-02. Containment isolation failure following transient or loss of offsite power starting from shutdown conditions.

- CM2AM -- 5.91E-04. Failure of two out of two core makeup tank lines, automatically or manually actuated.

- CM2AMP -- 5.91E-04. Failure of two out of two core makeup tank lines, automatically or manually actuated, during a loss of offsite power.

- IW2AB -- 1.62E-04. Failure of in-containment refueling water storage tank gravity injection lines to deliver water from the in-containment refueling water storage tank to the reactor coolant system following a transient or loss-of-coolant accident or loss of offsite power during shutdown conditions; (same fault tree is used in the at-power PRA).

- IW2A -- 3.15E-04. Failure of gravity injection, automatically or manually actuated, to inject water into the reactor vessel following a transient or loss-of-coolant accident during mid-loop conditions

- IW2A0 -- 1.53E-03. Failure of gravity injection, manually actuated, to inject water into the reactor vessel during draining to mid-loop.

- IW2AP -- 7.25E-04. Failure of gravity injection, automatically or manually actuated, to inject water into the reactor vessel following loss of offsite power during mid-loop condition.

- IWFS -- 8.55E-03. Failure of recirculation motor-operated flow paths to deliver water from the in-containment refueling water storage tank to the refueling cavity following core damage.

- IWRNS -- 4.67E-03. Failure of normal residual heat removal system pump suction line to inject water from the in-containment refueling water storage tank to the reactor coolant system when the plant is at mid-loop following failure of in-containment refueling water storage tank injection.

- PCTS -- 9.87E-05. Failure of the passive containment cooling system to operate.

- PRM -- 6.63E-05. Failure of passive residual heat removal, manually actuated, to remove decay heat from the reactor coolant system following loss of normal residual heat removal, following a transient event during ~~hot~~safe/cold shutdown conditions.

- PRMP -- 6.67E-05. Failure of passive residual heat removal, manually actuated, to remove decay heat from the reactor coolant system following loss of normal residual heat removal, following a loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- PRW -- 6.61E-05. Failure of passive residual heat removal, manually actuated, to remove decay heat from the reactor coolant system following a station blackout and loss of compressed air events (same fault tree is used in the at-power PRA).

- RNC2 -- 3.56E-04. Failure of both normal residual heat removal trains, aligned in reactor coolant system cooldown mode to continue to run for 220 hours (mission time) during ~~hot~~safe/cold shutdown conditions.

- RNC2D -- 9.06E-05. Failure of both normal residual heat removal trains, aligned in reactor coolant system cooldown mode, to continue to run for 120 hours during mid-loop conditions.

- RNT2 -- 5.19E-02. Failure of both normal residual heat removal trains to manually restart and run in time to avoid the drain of the reactor level below the normal residual heat removal suction, after they stop following a loss of offsite power and power is restored within two hours during ~~hot~~safe/cold shutdown conditions.

- RNT2D -- 3.49E-02. Failure of both normal residual heat removal trains to manually restart and run in time to avoid the drain of the reactor level below the normal residual heat removal suction, after they stop following a loss of offsite power and power is restored within one hour during mid-loop condition.

- RNP2 -- 2.13E-01. Failure of both normal residual heat removal trains to automatically or manually restart on the diesel generators and run in time to avoid the drain of the reactor level below the normal residual heat removal suction, after they stop following loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- RNP2D -- 1.18E-01. Failure of both normal residual heat removal trains to automatically or manually restart on the diesel generators and run in time to avoid the drain of the reactor level below the normal residual heat removal suction, after they stop following loss of offsite power during mid-loop condition.

- CSWF2 -- 1.19E-03. Failure of component cooling water and service water to support the normal residual heat removal system decay heat removal for 220 hours during ~~hot~~safe/cold shutdown conditions.

- CSWF2D -- 4.70E-04. Failure of component cooling water and service water to support the normal residual heat removal system decay heat removal for 120 hours during mid-loop condition.

- CCTS -- 2.57E-04. Failure of component cooling water system to support the normal residual heat removal system decay heat removal during a transient or loss-of-coolant accident during ~~hot~~safe/cold shutdown conditions.

- CCPS -- 2.28E-02. Failure of component cooling water system to support the normal residual heat removal system decay heat removal during loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- SWTS -- 1.88E-04. Failure of service water system to support the normal residual heat removal system decay heat removal during a transient or loss-of-coolant accident during ~~hot~~safe/cold shutdown conditions.

- SWPS -- 2.05E-02. Failure of service water system to support the normal residual heat removal system decay heat removal during loss of offsite power during ~~hot~~safe/cold shutdown conditions.

- VLHS -- 9.16E-04. Failure of hydrogen control system to control containment hydrogen during and after a severe accident event with degraded core.

54.10 Level 1 Core Damage Frequency Quantification

The shutdown assessment is quantified using the same method that was followed in quantifying the at-power PRA. With respect to file manipulation, the quantification process is documented in Chapter 33. The basic analysis process and the Level 1 quantification results are summarized in the following subsections.

54.10.1 Core Damage Quantification Method

The AP600 shutdown core damage frequency is derived from the quantification of events initiated during shutdown. The input to this analysis includes the initiating event frequencies, an event tree model for each initiator, and system and operator failure models. These inputs are documented in Sections 54.3 through 54.8. In the plant core damage analysis, the core damage accident sequences defined in the event trees are quantified by using the fault tree linking method to obtain the following results:

- Plant core damage frequency for shutdown initiating events
- Frequency of each core damage accident sequence
- Dominant component level cutsets leading to core damage
- Dominant cutsets for each initiating event category
- Importance ranking of initiating events
- Importance ranking of fault tree basic events

The fault tree linking is performed by using the Westinghouse GRAFTER and WLINK code systems (References 54-6 and 54-7). The GRAFTER code system is used to create the frontline and support system fault tree models and to quantify these models to obtain minimal cutsets. The frontline system fault trees contain support system basic events labeled SUB-XXX, where XXX represents the fault tree name of the support system. These basic events are replaced by their equivalent cutsets during the linking process. The linking is performed using the WLINK code system. The WLINK code uses accident sequence descriptions (expressed in terms of fault trees and scaler quantities) to calculate the core damage component-level cutsets and the core damage frequency.

Inputs to the Core Damage Model

The inputs to the core damage model include the following:

- List of initiating event categories and their frequencies

- Event sequences (as shown on the event tree diagrams) for all initiating event categories

- Either a fault tree model or a scaler for each event tree top node

- Fault tree models for each support system (defined as SUB-XXX basic event in the fault trees)

- AP600 PRA master data base

A list of core damage accident sequences is generated from each event tree diagram. This list contains minimal accident sequence cutsets ordered by the timing of events. In general, failed systems are shown in these accident sequence cutsets. The fault tree quantification is done in two steps. First, each fault tree basic event probability is calculated using the AP600 PRA master data base. Second, each fault tree is quantified to obtain its minimal cutsets. The WLINK code is then used to link the fault tree cutsets and scalers appearing in each of the accident sequence cutset lists. Accident sequences that do not lead to core damage are not analyzed.

54.10.2 Quantification Inputs

In quantifying the shutdown events, the following four classes of input data are utilized. These inputs are discussed in the paragraphs that follow:

- Initiating event input
- Accident sequence input
- Fault tree input
- Other input (scalar)

Initiating Event Input

The initiating events and their frequencies are discussed in subsections 54.2.6 and 54.4, respectively.

Accident Sequence Input

Each event tree model generated in Section 54.4 for shutdown events is examined to identify accident sequences leading to core damage. For each initiating event, a list of core damage accident sequences is generated. The rules used to generate these lists are as describe.l in Chapter 33.

Fault Tree Input

Fault tree models are developed for the event tree top events and their support systems. The inputs used in these fault tree models are included in the respective tables provided in Sections 54.5 and 54.6.

Fault tree input to the core damage quantifica ion process consists of cutset files representing the fault tree models, and a master data bas: that provides the input to calculate fault tree basic event probabilities. The master dat? base is provided in Table 54-58. The fault tree basic event identifiers are provided in Table 54-59.

Other Input

Some of the event tree top nodes are not fault trees, but are scalars. These scalars are identified in each event tree and are assigned basic event identifiers and probabilities.

Test & Maintenance Unavailabilities

As shown in Table 54-8, component unavailabilities due to test and unscheduled maintenance of systems are modeled and included in the quantification of events during ~~hot~~safe/cold shutdown conditions.

For the Level 1 quantification, component unavailabilities due to test and/or unscheduled maintenance are not included in the quantification for events during mid-loop condition. The rationale for excluding system unavailabilities due to test and maintenance when the plant is at mid-loop is provided in the notes for Table 54-8.

The fault tree modeling uses, in some cases, the same trees to calculate the frequencies of initiating events at ~~hot~~safe/cold shutdown and mid-loop conditions; these have the unavailabilities due to test and maintenance of electrical and instrumentation and control components modeled in their subtrees. In order to avoid constructing separate fault trees for events at mid-loop, component test and maintenance unavailabilities for events at mid-loop were excluded by requantifying the appropriate ~~hot~~safe/cold shutdown fault trees with test and maintenance removed.

54.10.3 Level 1 Shutdown Core Damage Frequency Results

The shutdown core damage frequency is 5.5E-08 per year. The results indicate that the dominant contributors to core damage at shutdown are accidents postulated with the reactor coolant system drained and operations performed with the plant at mid-loop or vessel-flange condition.

The Level 1/accident sequence quantification results for the shutdown assessment are presented in Table 54-60. The core damage sequences for the shutdown assessment are shown in Table 54-61. The top 100 component level failure combinations (cutsets) associated with these sequences are shown in Table 54-62. These results show a total shutdown core damage frequency of 5.5E-08 events per reactor year.

Table 54-63 presents the results of importance (risk decrease) calculations for the initiating events analyzed in the shutdown assessment. These results indicate that events occurring during reactor coolant system drained conditions contribute over 90 percent of the total shutdown core damage frequency. Events resulting in loss of normal residual heat removal system function while drained (e.g., loss of component cooling water, failure of normal residual heat removal system, loss of offsite power) have the largest impact on core damage frequency at shutdown (over 85 percent of the total). Loss-of-coolant events (with the reactor coolant system drained or undrained) account for about 9 percent of the total.

Tables 54-64 and 54-65 present the risk decrease and risk increase rankings, respectively, for the basic events (including the initiating events) modeled in the shutdown assessment.

54.11 Shutdown and Low-Power Release Category Quantification

~~This section describes the quantification of the containment event trees and calculation of the large release frequency for the AP600 shutdown conditions. The development of the containment event tree structure and release category definitions are described in Chapter 35. Table 54-66 presents the containment event tree top events and their definitions. Table 54-67 presents the release categories and their definitions. For the shutdown conditions, the same containment event tree structure as used for at-power is employed to quantify the large release frequency.~~

The release category quantification is being updated and will be provided to the NRC in the June 28, 1996 submittal.

~~54.11.1 Level 1/Level 2 PRA Interface~~

~~To limit the number of quantifications of the containment event tree that must be performed, similar core damage accident sequences from the Level 1 low power analysis are grouped into bins called accident classes. The accident classes are the end points to the Level 1 event trees and are presented graphically on the tree diagrams in Section 54.4. The shutdown accident classes are similar to at-power accident classes presented in Chapter 35 and the definitions are summarized in Table 54-68.~~

~~The quantification of the containment event tree is performed by linking fault trees to the system nodes on the tree and by using scalar values which were calculated with the decomposition event trees (Chapters 36 through 41) for the severe accident phenomenological nodes. To facilitate this combination of fault tree linking and scalar quantification on event trees with hundreds of paths, the acciden: classes frequencies are run through plant damage state (PDS) event trees which model only the availability of the plant systems credited on the containment event tree. The plant damage state event trees have only fifteen paths. The plant damage state event trees for the low power accident classes are presented in Figures 54-67 through 54-70. The fault trees are linked to the plant damage state trees, and the 15 end-states (called plant damage state substates) describe the accident class as well as the availability of the systems credited on the containment event tree. These systems are:~~

- ~~Containment isolation (node IS)~~
- ~~Passive containment cooling (PCS) water (node PC)~~
- ~~Hydrogen control system (node IG)~~
- ~~Cavity flooding (node IR)~~
- ~~Water recirculation to the cavity for debris coolir g (node RW)~~

~~The plant damage state event trees are quantified using the WLINK code (Reference 54-7). Each plant damage state substate is then quantified with the entire containment event tree (including the phenomenological nodes) and with the system nodes failure probabilities set to either 0 or 1, depending on the plant damage state substate definition. The scalar~~

~~quantification of the containment event tree is accomplished using the WESCADET/WESQT codes (Reference 54-9).~~

~~Tables 54-69 and 54-70 summarize the plant damage state substate frequencies and conditional probabilities, respectively, derived from the dominant Level 1 event sequences for each of the accident classes. The accident classes and their plant damage state event trees are discussed below.~~

~~Accident Class LP-ADS~~

~~Accident class LP-ADS bins together low-power accident sequences that are not sufficiently depressurized to allow gravity injection of the in-containment refueling water storage tank water into the reactor vessel through the direct vessel injection lines. LP-ADS includes accident sequences that are not depressurized as well as sequences that are partially depressurized, but not enough for gravity injection. Since this distinction in reactor coolant system pressurization is required for the Level 2 quantification, an interfacing event tree presented in Figure 54-66 is used to separate LP-ADS into the other accident classes (LP-1A, LP-3D, and LP-3BR) that distinguish degree of depressurization presented in the section below. The tree asks two questions regarding the reactor coolant system pressure:~~

~~Node ADP — Is the reactor coolant system partially depressurized?~~
~~Node DP — Does the operator recover full depressurization after core damage?~~

~~The tree quantification conservatively assumes that none of the sequences are partially depressurized (the failure probability at node ADP is set to 1.0). This treatment results in all sequences being treated as either fully pressurized to the reactor coolant system or normal residual heat removal system safety valve setpoint (accident class LP-1A), or fully depressurized after core uncovery (accident class LP-3BR).~~

~~Accident Class LP-1A~~

~~Accident class LP-1A bins together accident sequences that are fully pressurized to the safety valve setpoint of either the reactor coolant system or the normal residual heat removal system depending on the initial conditions of the plant at the time of the accident initiation. If the reactor coolant system is initially closed and cooling is provided through the startup feedwater system, the reactor coolant system will pressurize to the setpoint of the pressurizer safety valve (2500 psia) if the cooling is lost. If the reactor coolant system is being cooled by the normal residual heat removal system when cooling is lost, the system will pressurize to the normal residual heat removal system safety valve setpoint (580 psia). All of the sequences in accident class LP-1A are treated as though the reactor coolant system pressurizes to the higher pressurizer safety valve setpoint in the quantification of the containment event tree.~~

~~The plant damage state event tree for accident class LP-1A is presented in Figure 54-67. The availability of containment isolation, passive containment cooling water and hydrogen control systems is considered. Sufficient cavity flooding to prevent vessel failure is only credited if~~

~~the operator action to flood the cavity is successful. In the event of vessel failure, sufficient water to recirculate to the reactor cavity is credited if the in-containment refueling water storage tank can inject through the direct vessel injection (DVI) lines or if sufficient core makeup tank and accumulator water is available. Table 54-69 and 54-70 summarize the plant damage state substate frequencies and conditional probabilities, respectively, for accident class LP-1A.~~

~~Accident Class LP-3D~~

~~Accident class LP-3D bins together accident sequences that are partially depressurized through the automatic depressurization system. Partial depressurization reduces the reactor coolant system pressure significantly, but not enough to allow the gravity injection of in-containment refueling water storage tank water. Because of the conservative treatment on the plant damage state event tree for LP-ADS at node ADP, no sequences are binned into LP-3D.~~

~~The plant damage state event tree for accident class LP-3D is presented in Figure 54-68. The availability of containment isolation, passive containment cooling water, and hydrogen control systems is considered. Sufficient cavity flooding to prevent vessel failure is only credited if the operator action to flood the cavity is successful. In the event of vessel failure, sufficient water to recirculate to the reactor cavity is only credited if the in-containment refueling water storage tank can inject through the direct vessel injection lines, since in shutdown mode the accumulators are considered to be isolated. Core makeup tank and reactor coolant system water alone does not provide sufficient water to recirculate water back to the cavity for debris cooling.~~

~~Accident Class LP-3BR~~

~~Accident class LP-3BR bins together accident sequences that are fully depressurized after core damage at node DP. Accident class LP-ADS results in LP-3BR if full depressurization is recovered at node DP on the LP-ADS plant damage state event tree. Full depressurization will allow the in-containment refueling water storage tank water to inject into the vessel and reflood the core if the gravity injection flowpath is opened and not plugged.~~

~~The plant damage state event tree for accident class LP-3BR is presented in Figure 54-64. The availability of containment isolation, passive containment cooling water and hydrogen control systems is considered. Sufficient cavity flooding to prevent vessel failure is credited if the direct vessel injection lines are available to flood the vessel and spill from the break or the automatic depressurization system or if the operator action to flood the cavity is successful. In the event of vessel failure, sufficient water to recirculate to the reactor cavity can be credited if the in-containment refueling water storage tank injection is successful at node IR since the accumulators are considered to be isolated in shutdown mode. Core makeup tank and reactor coolant system water alone does not provide sufficient water to recirculate water back to the cavity for debris cooling. Tables 54-69 and 54-70 summarize the plant damage state substate frequencies and conditionel probabilities, respectively, for accident class LP-3BR.~~

~~Accident Class LP-3BE~~

~~Accident class LP-3BE bins together accident sequences that are fully depressurized prior to core damage. Core damage occurs as the result of the failure of in-containment refueling water storage tank gravity injection due to either valve failure or line plugging.~~

~~The plant damage state event tree for accident class LP-3BE is presented in Figure 54-70. The availability of containment isolation, passive containment cooling water, and hydrogen control systems is considered. Sufficient cavity flooding to prevent vessel failure is credited if the operator action to flood the cavity is successful. In the event of vessel failure, sufficient water to recirculate to the reactor cavity can be credited if the in-containment refueling water storage tank flooding is successful at node IR since the accumulators are considered to be isolated in shutdown mode. Core makeup tank and reactor coolant system water alone does not provide sufficient water to recirculate water back to the cavity for debris cooling. Tables 54-69 and 54-70 summarize the plant damage state substate frequencies and conditional probabilities, respectively, for accident class LP-3BE.~~

~~Accident Class LPCBP~~

~~Accident class LPCBP bins together core damage accident sequences that bypass the containment. Containment bypass may occur if a steam generator tube rupture with an unisolated secondary system releases fission products to the outside environment, or if a break outside the containment in a system which interfaces with the reactor coolant system results in a fission product release to the outside environment. There is no plant damage state event tree or containment event tree treatment for accident class LPCBP since the containment is bypassed and provides no attenuation of the fission product releases.~~

~~54.11.2 Containment Event Tree Quantification~~

~~The containment event trees are quantified for each plant damage state substate with the WESCADET/WESQT code (Reference 54-8). The conditionals and probabilities for each of the containment event tree phenomena nodes are presented in Chapter 43. The probabilities for the system nodes are obtained from the quantification of the fault trees that are linked to the node in the plant damage state event trees in Figures 54-66 through 54-70. The results of the quantification are expressed as the frequency and conditional probability of each of the release categories and are presented in Table 54-71. Tables 54-72 through 54-77 present the dominant sequences for each of the 11 release categories.~~

~~Accident Class LP-1A~~

~~The sequences in accident class LP-1A have elevated reactor coolant system pressure and temperature, resulting from inability to recover reactor coolant system depressurization in class LP-ADS. These sequences challenge the reactor coolant system pressure boundary. The core makeup tanks and accumulators are available to provide water to the containment in this~~

~~accident class. The following is a summary of the results for this accident class. Percentages refer to percent of the total accident class frequency.~~

- ~~3.3 percent fail the steam generator tubes and result in a large release to the environment (BP)~~
- ~~1 percent result in high-pressure melt ejection (HPME) and early containment failure induced by high-pressure melt ejection~~
- ~~95.7 percent fail the reactor coolant system pressure boundary at the hot leg nozzles or at the reactor vessel wall above the core debris~~
- ~~1.4 percent have failure of containment isolation~~
- ~~91.8 percent fail to flood the reactor cavity and have vessel failure~~
- ~~23.4 percent have failure of the hydrogen control system~~
- ~~11.7 percent have early hydrogen combustion~~
- ~~0.12 percent fail containment early due to hydrogen combustion~~
- ~~14.7 percent have short term core concrete interaction during debris quench~~
- ~~0.8 percent do not quench the debris in the cavity~~
- ~~<0.1 percent do not have enough water in the cavity to cool the core debris~~
- ~~5.2 percent have hydrogen combustion before 24 hours (intermediate)~~
- ~~0.2 percent fail containment before 24 hours due to hydrogen combustion (intermediate failure)~~
- ~~1.1 percent have hydrogen combustion after 24 hours (late)~~
- ~~<0.1 percent fail containment after 24 hours due to hydrogen combustion (late failure)~~
- ~~0.7 percent have basemat melt-through (very late containment failure)~~
- ~~0.8 percent have excessive containment leakage~~

~~Accident Class LP-3BR~~

~~The sequences in accident class LP-3BR are those with recovered reactor coolant system depressurization from the LP-ADS accident class. The core makeup tanks and accumulator are generally not available to provide water to the containment. Recovery of depressurization leads to injection of the in-containment refueling water storage tank water through the direct vessel injection lines and floods the reactor cavity. The core is reflooded in LP-3BR. The following is a summary of the results for this accident class. Percentages refer to percent of the total accident class frequency.~~

- ~~1.7 percent have failure of containment isolation~~
- ~~<0.1 percent fail to flood the reactor cavity~~
- ~~<0.1 percent fail the reactor vessel~~
- ~~0.1 percent have failure of the hydrogen control system~~
- ~~0.05 percent have early hydrogen combustion~~
- ~~<0.1 percent have containment failures due to hydrogen combustion~~
- ~~<0.1 percent have basemat melt-through~~
- ~~0.8 percent have excessive containment leakage~~

~~Accident Class LP-3BE~~

~~The sequences in accident class LP-3BE are fully depressurized with failure of the gravity injection of water from the in-containment refueling water storage tank. Most of these sequences are initiated at mid-loop in which accumulators and core makeup tanks are valved off and unavailable for injection. In a significant percentage of sequences, the failure mode for gravity injection is plugging of the screens in the in-containment refueling water storage tank, which results in a common cause failure of cavity flooding to prevent reactor vessel failure. Therefore, there is a significant percentage of sequences which result in vessel failure into a dry cavity and extended core concrete interaction. The following is a summary of the results for this accident class. Percentages refer to percent of the total accident class frequency.~~

- ~~1.4 percent of the sequences have failure of the containment isolation~~
- ~~22.2 percent fail to flood the reactor vessel and have vessel failure~~
- ~~22.2 percent fail to quench debris in the reactor cavity~~
- ~~0.1 percent have failure of the hydrogen control system~~
- ~~<0.1 percent have containment failures induced by hydrogen combustion~~
- ~~22.2 percent have basemat melt-through~~
- ~~0.8 percent have excessive containment leakage~~

~~Accident Class LPCBP~~

~~The sequences in accident class LPCBP bypass the containment and are not addressed with the containment event tree. All of the frequency of accident class LPCBP is binned into release category BP.~~

~~54.11.3 Shutdown and Low-Power Containment Event Tree Quantification Results Summary~~

~~The following items summarize the results of the release frequency essessment for shutdown and low-power operation for the AP600:~~

- ~~The overall shutdown large release frequency for AP600 is $1.4\text{x}10^{-8}$ events per reactor-year. This frequency includes the containment bypass, containment isolation failure, excessive containment leakage, and containment failures/release modes.~~

- ~~The frequency of compromised containment integrity resulting from the accident initiator is $3.2\text{x}10^{-9}$ events per reactor-year. This impaired containment frequency includes containment bypass, containment isolation failure, and excessive containment leakage. It accounts for 22.5 percent of the overall shutdown large release frequency.~~

- ~~The frequency of containment failure within 24 hours of core damage is $2.1\text{x}10^{-11}$ events per reactor-year. This frequency includes early and intermediate containment failures. It accounts for 0.15 percent of the overall large release frequency.~~

- ~~Approximately 63 percent of the initially impaired containment frequency consists of initiating events that bypass containment. Approximately 1.4 percent of the initially impaired containment frequency is attributed to induced steam generator tube ruptures.~~

- ~~Early containment failure contributes 0.1 percent to the large release frequency.~~

- ~~Approximately 88 percent of the early containment failure frequency is due to high pressure melt ejection cases. The frequency of high pressure melt ejection cases ($1.3x10^{-11}$ events per reactor year) is less than 0.02 percent of the core damage frequency and contributes less than 0.1 percent of the large release frequency. Given the insignificant fraction of the core damage frequency involved, no further analyses of the associated phenomena have been performed and no decomposition event trees were developed to demonstrate containment integrity for melt ejection phenomena, despite the fact that both AP600 design features and the emerging consensus on direct containment heating for existing pressurized water reactors afford considerable promise that integrity would be maintained. High pressure melt ejection cases are included with the early containment failure release category CFE-C.~~

- ~~The frequency of containment failure after 24 hours of core damage due to basemat failure is $1.1x10^{-8}$ events per reactor year. Basemat failure occurs more than 72 hours after the onset of core damage. The frequency accounts for 77.4 percent of the overall large release frequency. Late containment failure due to hydrogen combustion is negligible with respect to basemat failure.~~

- ~~Because many of the water sources to the containment are valved off during shutdown conditions, a significant percentage of the severe accidents at shutdown result in dry reactor cavities in which the debris cannot be cooled. (No credit was taken in the models for actions by the operators outside the control room to re-open valves to these water sources.)~~

- ~~The following are the estimated frequencies of the shutdown containment challenges from severe accident high energy events:~~

  - ~~the frequency of core damage combined with failure of passive containment cooling water is $3.8x10^{-10}$ events per reactor year~~

  - ~~the frequency of global combustion is $2.7x10^{-10}$ events per reactor year~~

  - ~~the frequency of unmitigated core concrete interaction is $1.1x10^{-8}$ events per reactor year~~

  - ~~the frequency of ex-vessel fuel coolant interaction is $4.4x10^{-10}$ events per reactor year~~

- ~~the frequency of high pressure melt ejection is 1.3x10^{-11} events per reactor-year~~

- ~~the frequency of in-vessel fuel coolant interactions that threaten containment integrity is approximately 0.0 events per reactor-year~~

54.12 Shutdown Assessment Importance and Sensitivity Analyses

A number of importance and sensitivity analyses was performed for the shutdown assessment Level 1 results. The importance and sensitivity studies were performed to gain additional insights from the shutdown results.

The following are presented:

- Importance analyses of shutdown PRA base case core damage quantification (cases 1 – 4)

- In-containment refueling water storage tank failure sensitivity (case 5)

- Normal heat removal system failure sensitivity (case 6)

- Sensitivity to operator actions with all human error probabilities set to 0 (case 7)

- Sensitivity to minimized credit for operator actions, with all human error probabilities set to 0.5 (case 8)

- Sensitivity to allow test and maintenance during drained condition (case 9)

- Sensitivity to allow unscheduled maintenance of normal residual heat removal system components during drained conditions (case 10)

- Sensitivity to allow unscheduled maintenance of component cooling water system components during drained conditions (case 11)

- Sensitivity to allow unscheduled maintenance of service water system components during drained conditions (case 12)

Two measures of risk are defined for, and used, in the analyses: risk decrease and risk increase importances. Risk decrease is a measure of the contribution of a basic event to the core damage frequency when its failure probability is set to 0.0; risk increase is defined as the contribution of a basic event to the core damage frequency when its failure probability is set to 1.0. Risk decrease is a useful measure of the benefit that might be obtained as a result of improved component maintenance or testing, better procedures or operator training. Risk increase is a useful measure of which components or actions would most adversely affect the core damage frequency if actual operating practices resulted in higher failure probabilities than assumed in the core damage assessment.

54.12.1 Importance Analyses for Core Damage at Shutdown

The core damage results for internal initiating events at shutdown include 365 basic events (including initiating events, component failures, human errors, and common cause failures) in over 9000 core damage cutsets. The importance analysis of the core damage results for events initiated during shutdown is discussed in terms of four categories of basic events, as follows:

- Initiating events
- Common cause
- Human errors
- Component failures

Initiating Event Importance (Case 1)

The AP600 core damage frequency for internal initiating events during plant shutdown was calculated to be 5.50E-08 events per year.

Core damage frequency of 5.50E-08 is small; it indicates that one core damage event (from events initiated during plant shutdown) is expected in about eighteen million plant-years of operation.

Ten separate initiating events were defined to accurately represent the AP600 design during shutdown conditions. The initiating events occur during the following three conditions:

- Nondrained (~~hot~~safe/cold shutdown) conditions with the reactor coolant system filled and pressurized
- Drained (mid-loop) conditions when the reactor coolant system is depressurized
- Conditions during which the reactor coolant system is being drained to mid-loop

Five of the initiating events are defined for nondrained conditions; four initiating events are defined for drained conditions; and one initiating event is defined as occurring during drainage of the reactor coolant system to mid-loop.

The initiating events during plant shutdown are listed in Tables 54-83 and 54-84. The contribution of the initiating events to the total core damage frequency is shown in Table 54-83 in terms of the risk decrease importance of the initiating events. The risk increase importance of the initiating events is shown in Table 54-84.

The results listed in Table 54-83 show the following:

- Initiating events during reactor coolant system drained conditions comprise approximately 85 percent of the total shutdown core damage frequency.

- Initiating events during reactor coolant system nondrained conditions comprise approximately 10 percent of the total shutdown core damage frequency.

- Overdraining of the reactor coolant system during drainage to mid-loop conditions comprises approximately 5 percent of the total shutdown core damage frequency.

When the risk decrease results are examined according to initiating event types, the following observations are made:

- The loss of decay heat due to component cooling water system or service water system failure initiating event accounts for approximately 57 percent of the total core damage frequency.

- The loss of decay heat removal due to random normal residual heat removal system failure initiating event accounts for approximately 11 percent of the total shutdown core damage frequency.

- Loss of offsite power initiating events account for approximately 20 percent of the total shutdown core damage frequency.

- Loss-of-coolant accident initiating events account for approximately 7 percent of the total shutdown core damage frequency.

- The reactor coolant system overdrain initiating event accounts for approximately 5 percent of the total shutdown core damage frequency.

Common Cause Failure Importances (Case 2)

The common cause failures reflected in the core damage frequency for events initiated during plant shutdown are described in Tables 54-85 and 54-86. The contribution of the common cause failures to the total shutdown core damage frequency is shown in Table 54-85 in terms of their risk decrease importances. Table 54-85 includes all common cause events with risk decrease importance greater than 1 percent of the baseline shutdown core damage frequency. The risk importance of the common cause failures is shown in Table 54-86, which includes all common cause events with risk increase importance greater than 300 percent.

The results in Table 54-85 indicate that the most significant common cause failures are those within the in-containment refueling water storage tank. These common cause failures, comprising about 83 percent of the shutdown core damage frequency for internal events at shutdown, are as follows:

- Common cause failure of the in-containment refueling water storage tank motor-operated valves (MOVs) comprises approximately 63 percent of the total shutdown core damage frequency.

- Common cause failure (plugging) of the strainers in the in-containment refueling water storage tank comprises 14 percent of the total shutdown core damage frequency.

- Common cause failure of the in-containment refueling water storage tank gravity injection check valves comprises approximately 6 percent of the total shutdown core damage frequency.

These results indicate the importance of maintaining high reliability of the in-containment refueling water storage tank during shutdown.

The results from Table 54-86 indicate that the common cause failures that have the highest risk increase worth are:

- Software common cause failure of all logic cards in the protection and safety monitoring system, plant control system, and diverse actuation system. The results indicate that if this software common cause failure were assumed to occur and go undetected, the core damage frequency from shutdown internal events would increase substantially, from 5.50E-08 to 2.27E-03.

- Common cause failure of the strainers in the in-containment refueling water storage. The results indicate that if this common cause failure were assumed to occur and go undetected, the core damage frequency from shutdown internal events would increase from 5.50E-08 to 6.45E-04.

- Common cause failure of the motor-operated valves in the in-containment refueling water storage tank injection lines. The results indicate that if this common cause failure were assumed to occur and go undetected, the core damage frequency from shutdown internal events would increase from 5.50E-08 to 6.27E-04.

- Common cause failure of the power interface output boards in the protection and safety monitoring system. The results indicate that if this common cause failure were assumed to occur and go undetected, the core damage frequency from shutdown internal events would increase substantially. from 5.50E-08 to 1.87E-04.

- Common cause failure of the check valves in the in-containment refueling water storage tank injection lines. The results indicate that if this common cause failure were assumed to occur and go undetected, the core damage frequency from shutdown internal events would increase from 5.50E-08 to 2.08E-05.

The common cause importance evaluation shows that failures of the in-containment refueling water storage tank components are significant contributors to both the risk decrease and risk increase worths. Maintaining a high reliability of the in-containment refueling water storage tank valves and strainers is important to maintaining the current very low level of core damage frequency at shutdown.

Maintaining a high reliability for the instrumentation and control (the logic cards and protection and safety monitoring system power interface output boards) is similarly important, as shown by the risk increase results. In general, safety-related common cause failures appear with the highest risk increase (and risk decrease) importances. This is an indication of the protection afforded by the safety systems at shutdown.

Human Error Importances (Case 3)

The human error importance discussed here pertains to the operator actions as they appear in the dominant core damage cutsets of the base case shutdown core damage quantification. The risk-important human errors are identified in Tables 54-87 and 54-88.

Tables 54-87 and 54-88, show the relative importance for human error basic events. Table 54-87 lists human error basic event importances, using the risk decrease method, for those events with importance greater than 1 percent of the baseline core damage frequency. Table 54-88 shows human error basic event importance, using the risk increase method, for events with importance greater than 100 percent of the baseline total.

Table 54-87 shows that there are only seven operator actions with importance greater than 1 percent, and that none of those events is a dominant contributor to core damage frequency at shutdown. This indicates that there would be no significant benefit from additional refinement of the actions modeled. The results from Table 54-87 also indicate that the total risk reduction worth of the operator actions is no more than 18 percent. The three human errors with the highest risk reduction worths are as follows:

- Operator fails to recognize the need to open the normal residual heat removal system pump suction line motor-operated valve V023 (to inject water from the in-containment refueling water storage tank following failure of the in-containment refueling water storage tank injection when the plant is at mid-loop). This operator action is identified as RHN-MAN05C and has a 5 percent risk reduction worth. The contribution of this operator action is in part the result of dependence on a preceding action, whereby, a human error probability of 0.15 is assigned to RHN-MAN05C.

- Operator fails to isolate normal residual heat removal system pipe rupture during shutdown conditions. This operator action is identified as RHN-MAN04 and has a 4 percent risk reduction worth.

- Operator fails to open the in-containment refueling water storage tank motor-operated isolation valves V121A and B (to inject water from the in-containment refueling water storage tank when the plant is at drained conditions). This operator action is identified as IWN-MAN00C and has a 3.4 percent risk reduction worth. The contribution of this operator action is in part the result of dependence on a preceding action, whereby an human error probability of 0.15 is assigned to IWN-MAN00C.

The human error risk increase worths, shown in Table 54-88, indicate that there are few operator actions with the potential to significantly increase shutdown core damage frequency. The three human errors with the highest risk increase worths are as follows:

- Operator fails to recognize the need for reactor coolant system depressurization during ~~hot~~safe/cold shutdown conditions. This operator action is identified as LPM-MAN05; guaranteed failure of this operator action would increase the core damage frequency from 5.50E-08 to 1.49E-06.

- Operator fails to open the in-containment refueling water storage tank motor-operated isolation valves V121A and B to inject water from the in-containment refueling water storage tank when the plant is at drained conditions. Guaranteed failure of this operator action would increase the core damage frequency from 5.50E-08 to 7.39E-07.

- Operator fails to recognize the need for and failure to open the normal residual heat removal system pump suction line motor-operated valve V023 (to inject water from the in-containment refueling water storage tank following failure of the in-containment refueling water storage tank injection when the plant is at mid-loop). Guaranteed failure of this operator action would increase the core damage frequency from 5.50E-08 to 2.99E-07.

If it were assumed that the operators always fail to perform all actions credited in the base shutdown assessment, the internal events core damage frequency would increase from 5.50E-08 to approximately 2.50E-06.

The results of the human error importance evaluation lead to the conclusion that the shutdown core damage frequency is not sensitive to human actions, but that operator ability to diagnose and respond to events at shutdown is important to maintaining a low shutdown core damage frequency.

Component Importances (Case 4)

The component importances discussed in this section pertain to the components as they appear in the dominant core damage cutsets of the base case shutdown core damage quantification. The risk-important components are identified in Tables 54-89 and 54-90.

Tables 54-89 and 54-90, show the relative importance for component basic events. Table 54-89 outlines component basic event importance, using the risk decrease method, for those events having an importance greater than 1 percent of the baseline core damage frequency. Table 54-90 shows component basic event importance, using the risk increase method, for events with importance greater than 300 percent of the baseline total.

Table 54-89 shows that there are only eight components with a risk decrease importance greater than 1 percent. The results from Table 54-89 indicates that the highest risk reduction worth from any single component is about 3 percent, and the total risk reduction worth of the components is about 15 percent. This shows that single component failures are not important contributors to core damage frequency at shutdown, and indicates the benefit derived from the AP600 defense-in-depth design. The components with the highest risk reduction worths are as follows:

- Failure of normal residual heat removal system pump A has a risk reduction worth of approximately 3 percent. Similarly, failure of normal residual heat removal system pump B has a risk reduction worth of approximately 3 percent. Note that these failures include failures of associated equipment (circuit breakers, relays).

- Failure of either of the diesel generators to start and run (or failure of associated breakers to close) has a combined total risk reduction worth of approximately 4 percent.

The component risk increase worths are shown in Table 54-90. The results indicate that there are only eight components with risk increase worth greater than 300 percent. These components and their risk increase worths are as follows:

- Guaranteed failure of the in-containment refueling water storage tank resulting in failure of passive residual heat removal during ~~hot~~safe/cold shutdown conditions would increase the core damage frequency from 5.50E-08 to 8.20E-07.

- Guaranteed failure of any of the other seven components would increase the core damage frequency from 5.50E-08 to approximately 3.10E-07.

The results of the component importance evaluation lead to the conclusion that single independent component failures are not overly important to the shutdown core damage frequency. The redundancy and diversity of AP600 systems ensures that shutdown core damage frequency remains low even if single component failures occur.

54.12.2 Other Sensitivity Analyses for Shutdown Core Damage

This section documents the evaluation of five sensitivity cases performed on the Level 1 shutdown core damage frequency.

These sensitivity cases are as follows:

- In-containment refueling water storage tank failure sensitivity (case 5)

- Normal residual heat removal system failure sensitivity (case 6)

- Sensitivity to perfect operator actions with all human error probabilities set to 0 (case 7)

- Sensitivity to minimized credit for operator actions, with all human error probabilities set to 0.5 (case 8)

- Sensitivity allowing test and maintenance during drained condition (case 9)

Sensitivity cases 5, 6, and 8 were selected in order to measure the relative importances of the primary means of protection during shutdown. Case 7 measures the impact of having perfect operators. Case 9 measures the significance of allowing test and maintenance during drained conditions.

In-Containment Refueling Water Storage Tank Failure (Case 5)

This sensitivity study evaluates the impact of failure of the in-containment refueling water storage tank on the core damage frequency during plant shutdown conditions. The in-containment refueling water storage tank is modeled as a mitigating system in all accident conditions during shutdown.

The sensitivity case produced a core damage frequency of 6.44E-04. This increase over the base core damage frequency confirms that the in-containment refueling water storage tank is an important mitigating system during shutdown events. Given the redundancy inherent in the in-containment refueling water storage tank, these results are not realistic, but they do show the benefit derived from the in-containment refueling water storage tank.

Normal Residual Heat Removal System System Failure (Case 6)

This sensitivity study evaluates the impact of failure of the normal residual heat removal system on the core damage frequency during plant shutdown conditions. The normal residual heat removal system is the main frontline system for decay heat removal during the shutdown conditions modeled in the PRA.

This sensitivity produces a core damage frequency of 3.16E-04. This increase over the base core damage frequency is significant and confirms that the normal residual heat removal system is an important operating system during shutdown conditions.

Set all Human Error Probabilities to 0.0 (Case 7)

This sensitivity study evaluates the impact of having perfect operators (i.e., setting all human error probabilities to 0.0 in the baseline shutdown core damage quantification). The operator actions used in this sensitivity study are listed in Table 54-91, and are those that appear in the baseline quantification results.

This sensitivity produces a core damage frequency of 4.99E-08, which is a decrease of approximately 9 percent in the base core damage frequency. This indicates that the operator actions are not risk important at the level of plant risk obtained from the base case study. The results of this sensitivity differ somewhat from the risk decrease importance results due to the effects of multiple actions in some sequences. The risk decrease results, which are not cumulative, showed a higher impact, but the conclusions do not change.

Set all Human Error Probabilities to 0.5 (Case 8)

This sensitivity study evaluates the impact of setting all human error probabilities to 0.5 in the baseline shutdown core damage quantification. The operator actions used in this sensitivity study are listed in Table 54-91. The value of 0.5 was chosen for the shutdown sensitivity for the following reasons:

- The operator has longer time frames in which to complete tasks during shutdown conditions than at-power; therefore, failure may be less likely.

- The highest human error probability used in the PRA quantification is about 0.5, which is assigned to operator actions having a high dependency on a previously failed action.

The sensitivity produces a core damage frequency of 2.99E-06. This increase over the base case core damage frequency indicates that the operators play a significant role in maintaining a very low core damage frequency for internal events at shutdown, but also shows that even with very little credit for operator actions, the AP600 shutdown core damage frequency is very low.

Allow Test and Maintenance during Drained Conditions (Case 9)

In the base case shutdown quantification, electrical components are modeled in the drained condition fault trees without test and maintenance unavailability, and in the ~~hot~~safe/cold shutdown conditions with test and maintenance unavailability. (The test and maintenance assumptions for the systems used in the shutdown assessment are documented in Table 54-8.) That is, the base case assumes that these electrical components will not have planned maintenance or be tested during drained conditions.

This sensitivity study evaluates the impact of allowing test and maintenance of electrical components during reactor coolant system drained conditions. In this sensitivity, unavailabilities due to test and maintenance are modeled for the electrical components in the drained condition event trees. This sensitivity is designed to assess the impact on the base case shutdown core damage frequency, if electrical equipment is allowed to be unavailable due to test and maintenance when the reactor coolant system is drained.

This sensitivity produces a core damage frequency of 1.07E-07, which is twice the base case core damage frequency of 5.50E-08.

Allowing Unscheduled Maintenance of Normal Residual Heat Removal System Components during Drained Conditions (Case 10)

This sensitivity evaluates the impact of allowing unscheduled maintenance of the normal residual heat removal system components during drained conditions. The test and maintenance assumptions for the RNS are provided in Table 54-8. As stated in Table 54-8, test and maintenance of the RNS are performed at power and the availability and operability of the RNS are verified prior to draining the RCS to mid-loop. It is expected that if failure of one train of the RNS occurs while the plant is at mid-loop, the plant will be taken to filled and depressurized conditions for unscheduled maintenance.

This sensitivity study changes the core damage frequency from 4.72E-08 to 5.59E-08; an increase of 18 percent. This increase of 18 percent is not significant and indicates that performing unscheduled maintenance on one loop of the RNS is not risk-important relative to the risk obtained from the base case shutdown study.

Allowing Unscheduled Maintenance of Component Cooling Water System Components during Drained Conditions (Case 11)

This sensitivity evaluates the impact of allowing unscheduled maintenance of the component cooling water system components during drained conditions. The test and maintenance assumptions for the CCS are provided in Table 54-8. As stated in Table 54-8, test and maintenance of the RNS support systems are performed at power and the availability and operability of these systems are verified prior to draining the RCS to mid-loop. It is expected that if failure of one train of component cooling water occurs while the plant is at mid-loop, the plant will be taken to filled and depressurized conditions for unscheduled maintenance.

This sensitivity study changes the core damage frequency from 4.72E-08 to 5.47E-08; an increase of 16 percent. This increase of 16 percent is not significant and indicates that performing unscheduled maintenance on one loop of the component cooling water system is not risk-important relative to the risk obtained from the base case shutdown study.

Allowing Unscheduled Maintenance of Service Water System Components during Drained Conditions (Case 12)

This sensitivity evaluates the impact of allowing unscheduled maintenance of the service water system components during drained conditions. The test and maintenance assumptions for the SWS are provided in Table 54-8. As stated in Table 54-8, test and maintenance of the RNS support systems are performed at power and the availability and operability of these systems are verified prior to draining the RCS to mid-loop. It is expected that if failure of one train of service water occurs while the plant is at mid-loop, the plant will be taken to filled and depressurized conditions for unscheduled maintenance.

This sensitivity study changes the core damage frequency from 4.72E-08 to 6.00E-08; an increase of 27 percent. This increase of 27 percent is not significant and indicates that performing unscheduled maintenance on one loop of the service water system is not risk-important relative to the risk obtained from the base case shutdown study.

54.13 Summary of Shutdown Level 1 Results

The top six accident sequences contribute 92 percent of the Level 1 shutdown core damage frequency. These dominant sequences are as follows:

1. Loss of component cooling or service water system initiating event during drained conditions, which contributes 54.1 percent of the core damage frequency

2. Loss of offsite power initiating event during drained conditions, with failure of grid recovery within 1 hour, which contributes 13.6 percent of the core damage frequency

3. Loss of normal residual heat removal system initiating event during drained conditions, which contributes 10.4 percent of the core damage frequency

4. Loss of offsite power initiating event during drained conditions, with success of grid recovery within 1 hour, which contributes 5.4 percent of the core damage frequency

5. Loss-of-coolant accident initiating event due to inadvertent opening of RNS-V024 during ~~hot~~safe/cold shutdown conditions, which contributes 5.0 percent of the core damage frequency

6. Reactor coolant system overdraining event during drainage to mid-loop, which contributes 3.4 percent of the core damage frequency

The descriptions of the dominant sequences are provided in the following paragraphs.

Loss of Component Cooling or Service Water System Initiating Event during Drained Condition

This sequence is a loss of decay heat removal initiated by failure of the normal residual heat removal system, as a result of failure of the component cooling water or service water system, during mid-loop/vessel flange operation, which has an estimated duration of 120 hours. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to loss of component cooling water system/service water system during drained conditions are:

- Hardware failures of both service water pumps, or common cause failure of the output logic I/Os from the plant control system

- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve

- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Offsite Power Initiating Event during Drained Condition (with failure of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel-flange operation, which has an estimated duration of 120 hours. In this sequence, the normal residual heat removal system fails to restart automatically following the initiating event, and the grid is not recovered within 1 hour. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency, given loss of offsite power (without grid recovery) during drained condition are:

- Software common cause failure of protection and safety monitoring system/plant control system, instrumentation and control logic cards

- Failure of normal residual heat removal system pump to restart or run

- Failure of a diesel generator to start and run

- Failure of main circuit breaker 100 (or 200) to open

- Failure to recover ac power within 1 hour

- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve

- Common cause failure of the strainers in the in-containment refueling water storage tank

Normal residual heat removal system failure has been modeled very conservatively for loss of offsite power. Although the success criterion is one-out-of-two normal residual heat removal trains operating, the shutdown fault tree models for normal residual heat removal for loss of offsite power require that both pumps restart, since they were assumed to both be running before the loss of power. If the fault trees had modeled one-out-of-two pumps, the loss of offsite power core damage contribution would have been lower, and the dominant hardware contributors for this sequence would have included common cause normal residual heat removal system pump failure instead of single normal residual heat removal system pump failure) and common cause diesel generator failure (instead of single diesel generator failure). The same is true for sequence 4.

Loss of Normal Residual Heat Removal System Initiating Event during Drained Condition

This sequence is a loss of decay heat removal initiated by failure of the normal residual heat removal system during drained condition. The loss of decay heat removal follows failure of normal residual heat removal system due to normal residual heat removal system hardware faults during mid-loop/vessel-flange operation. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to loss of normal residual heat removal system during drained condition are:

- Common cause failure of the normal residual heat removal system pumps to run
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valves
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Offsite Power Initiating Event during Drained Condition (with success of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel-flange operation. In this sequence, the normal residual heat removal system does not restart automatically following the initiating event, but the grid is recovered within 1 hour; however, manual normal residual heat removal system restart (after grid recovery) fails. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency given loss of offsite power (with grid recovery) during drained condition are:

- Software common cause failure of the protection and safety monitoring system/plant control system instrumentation and control logic cards
- Failure of normal residual heat removal system pumps to run or to restart
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve
- Common cause failure of the strainers in the in-containment refueling water storage tank

LOCA Initiating Event due to Inadvertent Opening of RNS-V024 during ~~Hot~~Safe/Cold Shutdown Conditions

This sequence is a loss-of-coolant accident initiated by inadvertent opening of RNS-V024 during ~~hot~~safe/cold shutdown conditions when the reactor coolant system is filled and pressurized (which has an estimated duration of 220 hours). Following the initiating event, the core makeup tanks are actuated, and the automatic depressurization system actuates. Core damage occurs if the in-containment refueling water storage tank injection check valves do not open automatically.

The major contributors to core damage frequency due to loss-of-coolant accident through RNS-V024 during ~~hot~~safe/cold shutdown conditions are:

- Inadvertent opening of RNS-V024 due to operator error (an initiating event frequency contributor)

- Common cause failure of the in-containment refueling water storage tank injection check valves

- Common cause failure of the strainers in the in-containment refueling water storage tank

Reactor Coolant System Overdraining Event during Drainage to Mid-Loop

This sequence is initiated by reactor coolant system overdraining during drainage to mid-loop conditions; draining to mid-loop has an estimated duration of 56 hours. Following the initiating event, manual isolation of the normal residual heat removal system fails. Core damage occurs if manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to reactor coolant system overdraining initiated during drainage to mid-loop are:

- Common cause failure of the chemical and volume control system air-operated valves to close automatically upon receipt of low hot leg level signals and failure of the operator to stop draining (initiating event frequency contributors)

- Operator fails to isolate the normal residual heat removal system

- Operator fails to open the in-containment refueling water storage tank injection motor-operated valves

- Operator fails to open the normal residual heat removal system pump suction valve

- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve

- Common cause failure of the strainers in the in-containment refueling water storage tank

The conclusions drawn from the shutdown Level 1 importance and sensitivity study are as follows:

- **Initiating Events Importance:** Initiating events during reactor coolant system drained conditions contribute approximately 85 percent of the total core damage frequency; loss of decay heat capability (during drained condition) due to failure of component cooling water system or service water system has the greatest contribution (54 percent of the core damage frequency).

  Overdraining the reactor coolant system during drainage to mid-loop, loss-of-coolant accidents due to inadvertently opening RNS-V024 during drained and nondrained conditions, and loss of decay heat removal during drained condition may have significant risk increase values. A high risk increase indicates it is important that the reliability of the systems, components or human errors that contribute to the initiating event frequency is (and remain) as good as shown in the PRA. The major contributors to reactor coolant system overdraining initiated during drainage to mid-loop are common cause failure of the chemical and volume control system air-operated valves to close automatically upon receipt of low hot leg level signals and failure of the operator to stop draining. The major contributor to loss-of-coolant accident through RNS-V024 is inadvertent opening of RNS-V024 due to operator error. The major contributors to the loss of decay heat removal initiating (during drained condition) event frequency are hardware failures of both service water pumps or common cause failure of the output logic I/Os from the PLS.

- **Common Cause Failure Importance:** Common cause failure of the in-containment refueling water storage tank components contribute approximately 83 percent of the total shutdown core damage frequency; common cause failure of the in-containment refueling water storage tank motor-operated valves contributes approximately 63 percent of the total shutdown core damage frequency.

  Common cause failure of the instrumentation and control (logic cards in the control and protection systems, and protection and safety monitoring system power interface output boards) and common cause failure of the in-containment refueling water storage tank motor-operated valves are major contributors to risk increase.

  Maintaining the reliability of the in-containment refueling water storage tank motor-operated valves and strainers is important in maintaining the current low level of core damage frequency at shutdown.

Similarly, maintaining a high reliability of the instrumentation and control is important in maintaining the current low level of core damage frequency at shutdown.

- **Human Error Importance:** Human errors are significant, but not overly important; there is no particular dominant contributor.

  One action, operator failure to recognize the need for reactor coolant system depressurization during ~~hot~~safe/cold shutdown conditions (LPM-MAN05C), was identified as having a significant risk increase. This indicates it is important that the operators understand and are appropriately trained for this operator action.

- **Component Importance:** Individual component failures are not significant contributors to shutdown core damage frequency, and there is no particular dominant contributor. This indicates that single independent component failures are not particularly important to the shutdown core damage frequency.

  Failure of the in-containment refueling water storage tank leading to failure of passive residual heat removal has a significant risk increase value. This simply underscores the importance of maintaining the reliability of this safety system component.

- **In-Containment Refueling Water Storage Tank Failure Sensitivity:** If the in-containment refueling water storage tank is assumed to be completely unavailable, the shutdown core damage frequency increases to 6.44E-04. The benefit and importance of the in-containment refueling water storage tank during low power and shutdown conditions is evidenced by this result. The results of this sensitivity show how failure of the in-containment refueling water storage tank directly affects the drained cases, which already dominate the core damage frequency, because the normal residual heat removal system is also not available.

- **Normal Residual Heat Removal Failure Sensitivity:** If the normal residual heat removal system is assumed to be completely unavailable, the core damage frequency increases to 3.16E-04. The benefit and importance of the normal residual heat removal system during reactor coolant system drained conditions is evidenced by this result. The results of this sensitivity indicate that failing the normal residual heat removal system causes the normal residual heat removal system initiating event sequences during drained conditions to dominate the core damage frequency.

- **Set all Human Error Probabilities to 0.0 Sensitivity:** If operator response is assumed to be perfect, the shutdown core damage frequency decreases by 9 percent. This small decrease indicates that, in general, the operator actions are not risk important at the level of plant risk obtained from the base case study. That is, improvements in the (human error probabilities would not provide significant core damage frequency benefit.

- **Set all Human Error Probabilities** to 0.5 Sensitivity: If operator response is assumed to fail 50 percent of the time, the core damage frequency increases to 2.99E-06. This increase indicates that, even though the shutdown core damage frequency would remain very low without operator response, the operator actions are important in maintaining the baseline core damage frequency for internal events at shutdown.

- **Allow Test & Maintenance of Electrical Components during Drained Condition Sensitivity:** If test and maintenance unavailability of electrical components is allowed during drained condition, the core damage frequency increases by a factor of 2. This increase in the base core damage frequency is somewhat significant even though a core damage frequency of 1.07E-07 is still quite low. The result emphasizes the importance of ensuring equipment operability before entering drained conditions.

- **Allowing Unscheduled Maintenance of Normal Residual Heat Removal System Components during Drained Conditions:** If unscheduled maintenance is allowed on RNS components during drained conditions, the core damage frequency increases by 18 percent. This increase of 18 percent in the base core damage frequency is not significant and indicates that performing unscheduled maintenance on one loop of the RNS is not risk-important relative to the risk obtained from the base case shutdown study.

- **Allowing Unscheduled Maintenance of Component Cooling Water System Components during Drained Conditions:** If unscheduled maintenance is allowed on CCS components during drained conditions, the core damage frequency increases by 16 percent. This increase of 16 percent in the base core damage frequency is not significant and indicates that performing unscheduled maintenance on one loop of the CCS is not risk-important relative to the risk obtained from the base case shutdown study.

- **Allowing Unscheduled Maintenance of Service Water System Components during Drained Conditions:** If unscheduled maintenance is allowed on SWS components during drained conditions, the core damage frequency increases by 27 percent. This increase of 27 percent in the base core damage frequency is not significant and indicates that performing unscheduled maintenance on one loop of the CCS is not risk-important relative to the risk obtained from the base case shutdown study.

54.14 References

54-1 *Advanced Light Water Reactor Utility Requirements Document*, Volume III, Appendix A to Chapter 1, PRA Key Assumptions and Groundrules, Revisions 5 and 6, December 1993.

54-2 "ATWS, A Reappraisal, Part 3 Frequency of Anticipated Transients," EPRI NP-2230, January 1982.

54-3 "AP600 Refueling Outage Maintenance Schedule," ~~GWGRL005,~~ Rev. 1, May 15, 1995.

54-4 "Seabrook Station Probabilistic Safety Study - Shutdown (Modes 4, 5 and 6)," Volume 1 - New Hampshire Yankee, May 1988.

54-5 "Reactivity Accident - A Reassessment of the Design-Basis Events," Brookhaven National Laboratory, NUREG/CR-5368, January 1990.

54-6 *GRAFTER Code System User Manual*, WCAP-11693 (Proprietary), Rev. 2, February 1990.

54-7 *WLINK Code System User Manual for Version 3.1*, WCAP-13400, 1992.

54-8 *Event Tree Development and Quantification System (WESCADET/WESQT) User Manual*, WCAP-13199 (Proprietary), February 1992.

Table 54-1

MATRIX: SHUTDOWN PHASES/OUTAGE TYPE/OPERATING MODE

Shutdown Phase	Outage Type			Operating Mode
	Nondrained Maintenance	Drained Maintenance	Refueling	
A	✓	✓	✓	3, 4, 5
B		✓	✓	5, 6
C			✓	6
D			✓	6
E		✓	✓	5, 6
F	✓	✓	✓	3, 4, 5

Table 54-2

SYSTEMS AVAILABILITY AND ACTUATING SIGNALS TYPE

System/Subsystem Name	At Power		Hot Standby		Safe/Cold Shutdown		Mid-Loop/ Vessel-Flange		Refueling	
	Mode	Signal	Mode	Signal	Mode	Signal	Mode	Signal	Mode	Signal
Chemical & Volume Control	A	h,i	A	h,i	A	h,i	M	--	--	
Startup Feedwater	A	g	A	g	A	g	--		--	
Passive Residual Heat Removal	A	j,k,l,m, o	A	j,k,l,p	A	o,k	--		--	
Core Makeup Tank	A	a,b,c,d	A	a,b,m	A	b	M		--	
Normal Residual Heat Removal (injection mode)	M		M		--		M		--	
Normal Residual Heat Removal (recirculation mode)	--	--	--		A$^{(1)}$		A$^{(1)}$		A$^{(1)}$	
Automatic Depressurization (Stages 1, 2 & 3)	A	f	A	f	A	f	M		--	
Automatic Depressurization (Stage 4)	A	q	A	q	A	q	M			
Accumulator	P	--	P	--	--		--		--	
In-containment Refueling Water Storage Tank (injection mode)	A	n,q	A	n,q	A	n,q	A$^{(2)}$	n		
In-containment Refueling Water Storage Tank (recirculation mode)	A	e	A	e	A	e	A	e	--	
Spent Fuel Pool Cooling	--	--	--		--		--		M	

Notes:
A = Automatic actuation (Manual actuation possible in automatic mode)
M = Manual actuation
P = Passive (Self actuating)

Notes (cont)

(1) Automatic actuation means that an automatic restart of RNS pumps is provided when, after loss of offsite power, transfer onto diesel generators has been completed.

(2) With reactor coolant system depressurization, before reaching a reactor coolant system pressure that permits in-containment refueling water storage tank gravity injection, closure of IRWST injection squib valves is maintained to avoid draining of in-containment refueling water storage tank water. Manual or automatic opening of these valves is required for gravity injection operation.

Actuation Signals

(a) Low steam generator level coincident with high hot leg temperature (PMS)
(b) Low pressurizer water level (PMS & DAS)
(c) Low pressurizer safety injection signal (PMS)
(d) Low pressurizer pressure or high containment safety injection signal (PMS)
(e) Low-3 in-containment refueling water storage tank water level and automatic depressurization system signal (PMS)
(f) Core makeup tank actuation and coincident low-1 core makeup tank level (PMS)
(g) Low narrow-range steam generator water level or low feedwater flow (PLS)
(h) Low pressurizer water level (PLS)
(i) High narrow-range steam generator water level (PLS)
(j) Core makeup tank automatic actuation (PMS)
(k) Low steam generator level - wide range (PMS)
(l) High hot leg temperature (DAS)
(m) S-signal (PMS)
(n) Low hot leg water level (PMS)
(o) Low pressurizer water ievel (PMS)
(p) Low narrow-range steam generator level plus low startup feedwater flow
(q) Automatic depressurization system stage 3 and core makeup tank low 2 level

Tables 54-3 through 54-7 are unchanged.

Table 54-8 (Sheet 1 of 4)

SYSTEM UNAVAILABILITY STATUS

System	**Unavailable Due to Test or Maintenance During Plant Shutdown Mode: (YES/NO)**			**T&M Reflected in Shutdown Model Fault Trees (See Note 1)**	**Comments**
	~~hot~~safe/ cold Shutdown	**Mid-Loop**	**Refueling**		
ADS	NO	YES	YES	NO	No credit is taken for ADS during shutdown modes in which the system is assumed unavailable. The maintenance guidelines are provided in SSAR, Chapter 16, Technical Specifications 3.4.12 to 3.4.14.
CIS	NO	NO	YES	NO	Valves for containment isolation for events initiated during shutdown are assumed to be maintained during refueling mode. The maintenance guidelines are provided in SSAR Chapter 16, Technical Specification 3.6.3.
CMT	NO	YES	YES	NO	CMTs are modeled only in events occurring during ~~hot~~safe/cold shutdown condition, therefore, unavailability due to test and unscheduled maintenance is not modeled for CMTs during this condition. Since CMT test and maintenance is also not modeled in the at-power fault tree cases, it is assumed CMT test and maintenance will only be allowed during refueling mode because the CMTs are not required to operate during mid-loop and refueling conditions. The maintenance guidelines are provided in SSAR, Chapter 16, Technical Specification 3.5.2.

Table 54-8 (Sheet 2 of 4)

SYSTEM UNAVAILABILITY STATUS

System	Unavailable Due to Test or Maintenance During Plant Shutdown Mode: (YES/NO)			T&M Reflected in Shutdown Model Fault Trees (See Note 1)	Comments
	~~Hot~~Safe/Cold Shutdown	Mid-Loop	Refueling		
IRWST	NO	NO	YES	NO	It is assumed that functional testing of the IRWST MOVs is conducted at cold shutdown condition just prior to isolating the IRWST; the RCS is cooled but pressurized. During this cold shutdown period, the plant risk is judged to be much lower than the risk while cooling down from ~~hot~~safe shutdown to cold shutdown condition. Therefore, IRWST unavailability due to test and unscheduled maintenance is not reflected in the IRWST fault trees for ~~hot~~safe/cold shutdown and mid-loop conditions. It is believed that excluding the risk while testing the MOVs does not impact the PRA results because the PRHR, CMTs, and ADS are available at cold shutdown when testing of the MOVs are conducted. The maintenance guidelines are provided in SSAR, Chapter 16, Technical Specification 3.5.6.
PCS	YES	YES	YES	YES	The PCS is called into operation from events initiated during any plant operating mode. It is assumed that the PCS could be maintained during power operation as well as during plant shutdown. The maintenance guidelines are provided in SSAR, Chapter 16, Technical Specification 3.6.6.
PRHR	YES	YES	YES	YES	It is assumed that some unscheduled maintenance of the PRHR is performed during ~~hot~~safe/cold shutdown condition, and scheduled maintenance is performed during mid-loop or refueling conditions. The PRHR system is not used during mid-loop operations or refueling mode. The maintenance guidelines are provided in SSAR, Chapter 16, Technical Specification 3.5.4.

Table 54-8 (Sheet 3 of 4)

SYSTEM UNAVAILABILITY STATUS

System	Unavailable Due to Test or Maintenance During Plant Shutdown Mode: (YES/NO)			T&M Reflected in Shutdown Model Fault Trees (See Note 1)	Comments
	~~Hot~~Safe/Cold Shutdown	Mid-Loop	Refueling		
RNS	NO	NO	NO	NO	RNS is maintained during power operation. The maintenance guidelines are provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2.
CCS	NO	NO	NO	NO	CCS is maintained during power operation. The maintenance guidelines are provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2.
SWS	NO	NO	NO	NO	SWS is maintained during power operation. The maintenance guidelines are provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2.
VLS	NO	NO	YES	NO	None
AC Power	YES	NO	YES	YES (See Note 6)	Unavailability due to test and unscheduled maintenance is modeled in the shutdown trees, as well as in the at-power trees. It is assumed that scheduled maintenance on this system is conducted during refueling mode. The maintenance guidelines are provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2.

Table 54-8 (Sheet 4 of 4)

SYSTEM UNAVAILABILITY STATUS

	Unavailable Due to Test or Maintenance During Plant Shutdown Mode: (YES/NO)			T&M Reflected in Shutdown Model Fault Trees (See Note 1)	
System	**~~Hot~~Safe/ Cold Shutdown**	**Mid-Loop**	**Refueling**		**Comments**
IE DC Power	YES	NO	YES	YES (See Note 6)	Unavailability due to test and unscheduled maintenance of the buses and batteries is modeled in the shutdown trees, as well as in the at-power trees. It is assumed that scheduled maintenance on this system is conducted during refueling mode. The maintenance guidelines provided in SSAR, Chapter 16, Technical Specification 3.8.1.
NON 1E DC Power	YES	NO	YES	YES (See Note 6)	Unavailability due to test and unscheduled maintenance of the buses and batteries is modeled in the shutdown trees, as well as in the at-power trees. It is assumed that scheduled maintenance on this system is conducted during refueling mode. The maintenance guidelines provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2.
I & C	N/A	N/A	N/A	N/A	Downtime due to failed components are incorporated into the availability equations which are used to generate the basic event data for the I&C models, consistent with the at-power PRA modeling. The DAS maintenance guidelines are provided in SSAR, Chapter 16, Reliability Assurance Program, Table 16.2-2. The PMS maintenance guidelines are provided in SSAR, Chapter 16, Technical Specification 3.3.

Notes:

1. It is assumed the scheduled maintenance on the systems in the table is conducted during refueling mode. Maintenance shown for the other shutdown modes are assumed to be unscheduled maintenance.

2. It is assumed that operability of the motor-operated valves on the gravity injection lines to open is verified prior to isolating the IRWST, before entering mid-loop condition. This functional test must verify both the automatic and manual actuation capabilities for these valves. Therefore, a conservative mission time of 220 hours is used to calculate the failure probabilities of these valves. Similarly, the operability of the motor-operated valve on the RNS pump suction line to open is also verified prior to entering a mid-loop condition. This test must verify the manual actuation capability. The drained mission time, 120 hours, is used to calculate the valve failure probability.

3. The same common cause failure probability of the instrumentation and control software, used in the at-power analysis, is used in the evaluation of all shutdown conditions.

4. The at-power PRA assumes a quarterly testing interval for the instrumentation and control hardware components. The quarterly testing interval is also reflected in the shutdown assessment for the instrumentation and control hardware failures for events during ~~hot~~safe/cold shutdown conditions. It is assumed that the instrumentation and control support for the IRWST valves is tested prior to entering mid-loop condition; therefore, the mission time of 220 hours is used to calculate the failure probability of the instrumentation and control that supports the IRWST operation for events during mid-loop condition.

5. For the normal residual heat removal and its support systems, there will be no planned maintenance during shutdown. Scheduled maintenance will be done during at-power operation. Therefore, both trains of normal residual heat removal will be available when entering shutdown conditions. If one train of normal residual heat removal is lost during nondrained, cold shutdown conditions, the plant will be kept in the nondrained, cold shutdown condition until normal residual heat removal capability is restored. If one train of normal residual heat removal is lost during drained conditions, the plant must be taken from drained condition to the depressurized but filled condition and normal residual heat removal capability restored.

6. Unavailabilities due to test and unscheduled maintenance of the electrical and instrumentation and control components that support the RNS and its support systems and the IRWST during mid-loop condition are not modeled, because of the operational requirements stated above. Because these unavailabilities are included in the fault tree models used, they were removed from the reduced files prior to event tree quantification.

7. Technical Specifications 3.4.12 to 3.4.14 specify the requirements for the ADS valves to be open prior to entering a reduced inventory condition.

Tables 54-9 through 54-54 are unchanged.

Table 54-55

COMMON CAUSE FAILURE EVALUATED FOR SHUTDOWN

Identifier	Description	Unavailability
IWX-MV-GO1	IRWST isolation valves PXS-121A/B fail to open when the plant is at mid-loop conditions	1.0E-5/hr x 220/2 x 5.0E-2 = 5.5E-05/d (see Notes 1 and 3)
RNX-PM-ERX	RNS pumps fail to run for 220 hours (nondrained) RNS pumps fail to run for 120 hours (drained)	2.5E-05 x 220 x 2.6E-02 = 1.4E-04/d 2.5E-05 x 120 x 2.6E-02 = 7.8E-05/d (see Note 2)
SFX-MV-GCS	Spent fuel system motor-operated valves SFS-V034 & -V035 fail to close	1.0E-5/hr x 17520/2 x 5.0E-2 = 4.4E-03/d
N/A	Hot leg level instruments fail to provide reactor coolant level indication	6.0E-7/hr x 17520/2 x 5.0E-2 = 2.6E-04/d (see Note 4)

Note:

This table documents common cause failures calculated specifically for the shutdown assessment. The common cause failures in this table were not used in the at-power PRA. The other common cause failures modeled in the shutdown assessment fault trees (or event trees) are also used in the at-power cases, and are not reflected in this table.

1. Motor-operated valves PXS-V121A&B are stroke tested just prior to entering mid-loop conditions; therefore the mission time of 220 hours at mid-loop is used to calculate this common cause failure. The mission time (t) is divided by 2, since the IRWST is in standby mode during this time.

2. The RNS is expected to operate throughout the 220/120 hour mission times (nondrained/drained), therefore this CCF calculations are done with the 220/120 hours without dividing by 2.

3. This common cause failure is conservatively calculated with only a beta factor, implying that 2 or more valves fail by common cause. Effectively no credit is taken for the third valve (RNS-V023) in CCF. This is done since:

   a. The beta factor is 0.78 and provides only a marginal improvement if used.

   b. This way, detailed modeling of the joint CCF between IWRNS and IW2A (or IW2AO or IW2AP) is avoided.

4. The beta factor of 0.05 for the hot leg level instruments is taken from Reference 54-1, Section A3 (Page A.A 29); 0.05 is the recommended generic beta factor for "failure to continue functioning or spurious operation" of components not specified in the URD, Table A3-1.

Tables 54-56 through 54-91 are unchanged.

Table 54-92 (Sheet 1 of 2)

MATRIX OF SHUTDOWN INITIATING EVENTS SCREENING PROCESS

Initiating Event	Modes 1&2 At-Power	Mode 3 Hot Standby RCS > 420°F	Mode 4 Safe Shutdown 420°F > RCS > 200°F	Mode 5 Cold Shutdown RCS < 200°F	Mode 6 Refueling RCS Open
Loss of Coolant Accidents					
Large LOCA	X	1	2	2	2
Medium LOCA	X	1	2	2	2
CMT Line Break	X	1	2	2	2
SI Line Break	X	1	2	2	2
Intermediate LOCA	X	1	2	2	2
Small LOCA	X	1	**4**	**4**	2
RCS Leakage	X	1	**4**	**4**	2
PRHR Tube Rupture	X	1	2	3	3
SG Tube Rupture	X	1	2	2	2
RV Rupture	X	1	2	2	2
ISLOCA	X	1	**4**	**4**	2
Transients					
Spurious Trip	X	2	2	2	2
Loss of RC Flow	X	1	1	3	3
LOMFW (1 SG)	X	1	3	3	3
Core Power Excursion	X	2	2	2	2

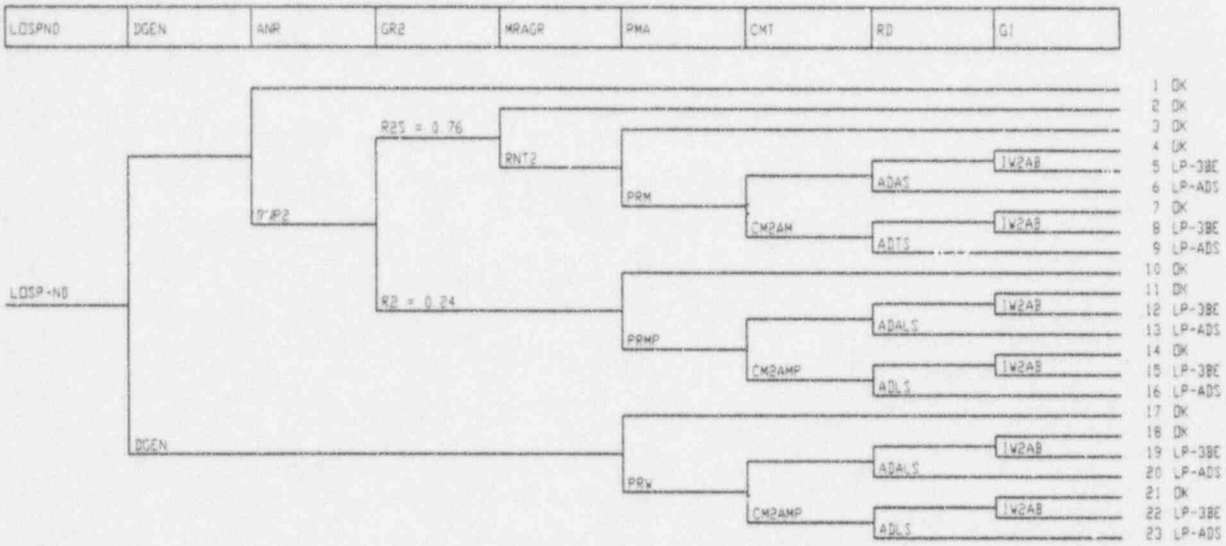
Table 54-92 (Sheet 2 of 2)

MATRIX OF SHUTDOWN INITIATING EVENTS SCREENING PROCESS

Initiating Event	**Modes 1&2 At-Power**	**Mode 3 Hot Standby RCS > 420°F**	**Mode 4 Safe Shutdown 420°F > RCS > 200°F**	**Mode 5 Cold Shutdown RCS < 200°F**	**Mode 6 Refueling RCS Open**
Loss of CCS/SWS	X	4	4	4	4
LOMFW (2 SG)	X	1	3	3	3
Loss of Condenser	X	1	3	3	3
Loss of Comp. Air	X	1	1	1	1
LOOP	X	4	4	4	4
MSLB (2 Categories)	X	1	2	2	2
Stuck-Open MSSV	X	1	2	2	2
Anticipated Transients Without Scram					
ATWS - 3 Categories	X	2	2	2	2

Notes:

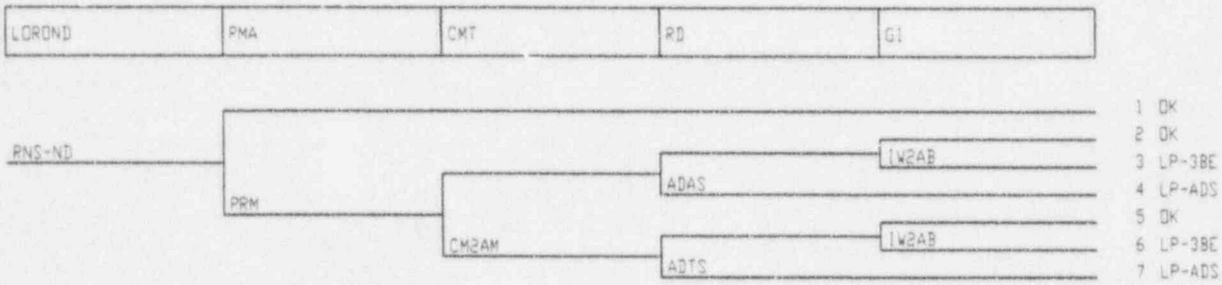
X -	Considered in at-power PRA.
1 -	Screened because plant response bounded by at-power event.
2 -	Screened because RCS conditions preclude occurrence of the event.
3 -	Screened because system alignment precludes occurrence of the event.
4 -	Evaluated in Shutdown PRA.



Event	Description
LOSPND	LOSS OF OFFSITE POWER DURING HOT/COLD SHUTDOWN (NON-DRAINED RCS)
DGEN	ONSITE AC POWER AVAILABLE THROUGH DIESEL GENERATORS
ANR	AUTOMATIC RNS RESTART
GR2	GRID RECOVERY WITHIN 2 HOURS
MRAGR	MANUAL RNS RESTART AFTER GRID RECOVERY
PMA	PRHR MANUAL ACTUATION
CMT	CORE MAKEUP TANKS
RD	RCS DEPRESSURIZATION
GI	GRAVITY INJECTION

Figure 54-1

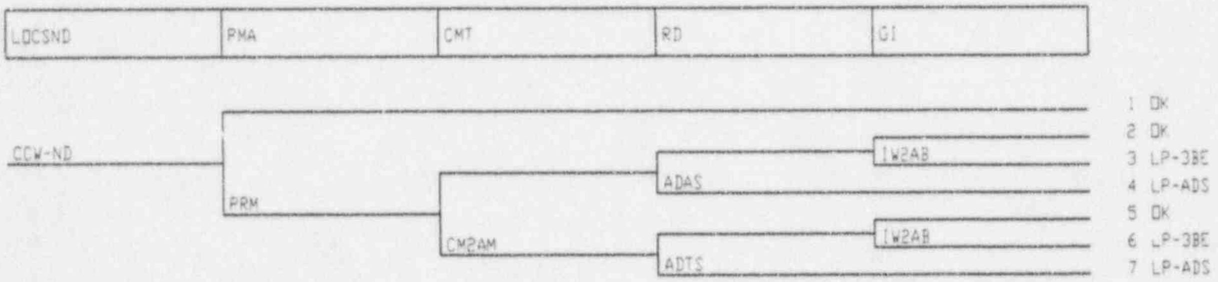
LOSP During Hot/Cold Shutdown (RCS Filled) Event Tree



Event	Description
LOROND	LOSS OF RNS OPERATION DURING HOT/COLD SHUTDOWN (NON-DRAINED RCS)
PMA	PRHR MANUAL ACTUATION
CMT	CORE MAKEUP TANKS
RD	RCS DEPRESSURIZATION
GI	GRAVITY INJECTION

Figure 54-2

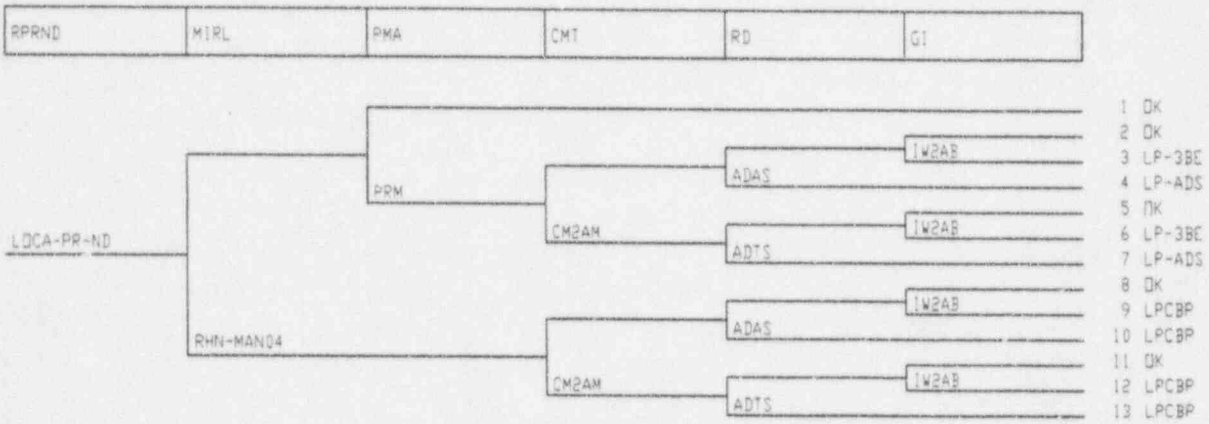
Loss of RNS Initiator During Hot/Cold Shutdown (RCS Filled) Event Tree



Event	Description
LOCSND	LOSS OF CCW/SW DURING HOT/COLD SHUTDOWN (NON-DRAINED RCS)
PMA	PRHR MANUAL ACTUATION
CMT	CORE MAKEUP TANKS
RD	RCS DEPRESSURIZATION
GI	GRAVITY INJECTION

Figure 54-3

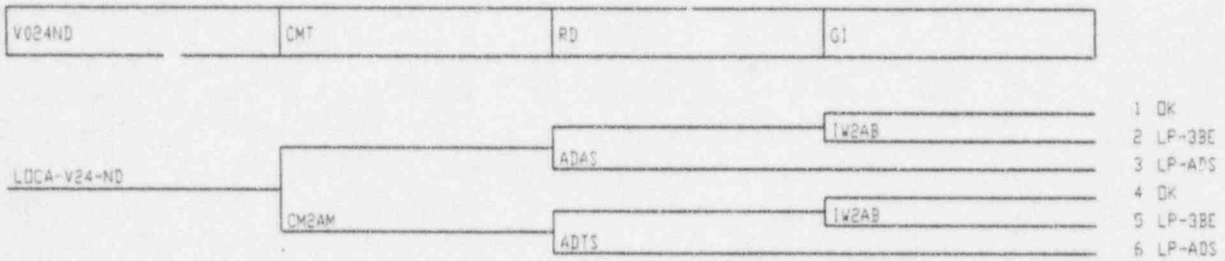
Loss of CCW/SW Initiator During Hot/Cold Shutdown (RCS Filled) Event Tree



Event	Description
RPRND	RNS PIPE RUPTURE DURING HOT/COLD SHUTDOWN (NON-DRAINED RCS)
MIRL	MANUALLY ISOLATE RNS LEAK
PMA	PRHR MANUAL ACTUATION
CMT	CORE MAKEUP TANKS
RD	RCS DEPRESSURIZATION
GI	GRAVITY INJECTION

Figure 54-4

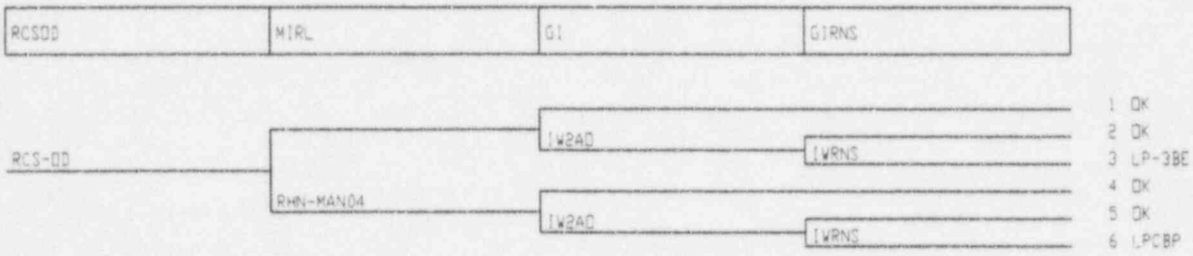
LOCA/RNS Pipe Rupture During Hot/Cold Shutdown (RCS Filled) Event Tree



Event	Description
V024ND	LOCA THROUGH RNS-V024 DURING HOT/COLD SHUTDOWN (NON-DRAINED RCS)
CMT	CORE MAKEUP TANKS
RD	RCS DEPRESSURIZATION
GI	GRAVITY INJECTION

Figure 54-5

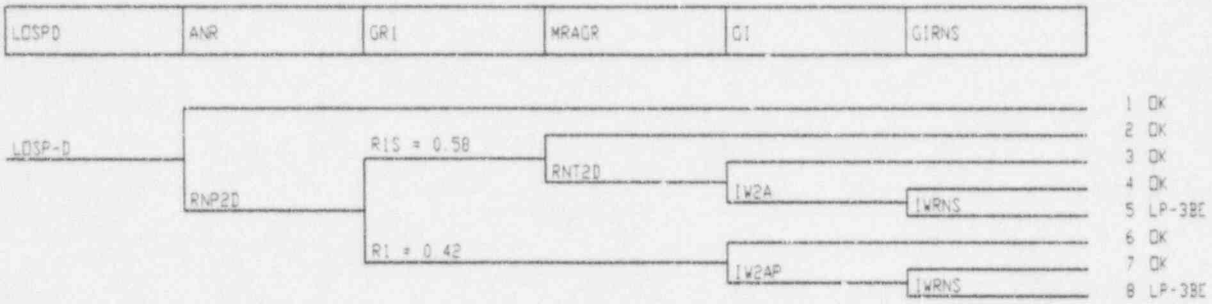
LOCA/RNS-V024 Opens During Hot/Cold Shutdown (RCS Filled) Event Tree



Event	Description
RCSOD	RCS OVERDRAINING DURING DRAIN-DOWN TO MID-LOOP
MIRL	MANUALLY ISOLATE RNS LEAK
GI	GRAVITY INJECTION
GIRNS	GRAVITY INJECTION FROM IRWST VIA RNS SUCTION LINE

Figure 54-6

Overdraining of Reactor Coolant System During Draindown to Mid-Loop

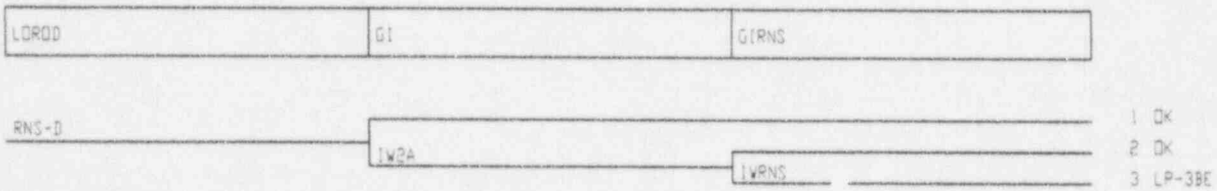


Event	Description
LOSPD	LOSS OF OFFSITE POWER DURING DRAINED MAINTENANCE (MID-LOOP/VESSEL FLANGE)
ANR	AUTOMATIC RNS RESTART
GR1	GRID RECOVERY WITHIN 1 HOUR
MRAGR	MANUAL RNS RESTART AFTER GRID RECOVERY
GI	GRAVITY INJECTION
GIRNS	GRAVITY INJECTION FROM IRWST VIA RNS SUCTION LINE

NOTE: RNP2D AND RNT2D ARE RNP2 AND RNT2, RESPECTIVELY, WITH TEST AND MAINTENANCE REMOVED.

Figure 54-7

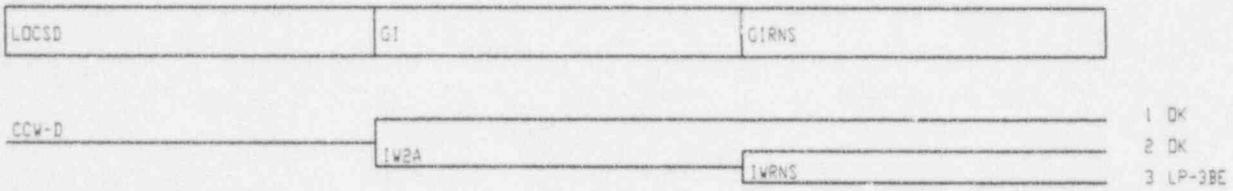
Lᴜss of Offsite Power (RCS Drained) Event Tree



Event	Description
LOROD	LOSS OF RNS OPERATION DURING DRAINED MAINTENANCE (MID-LOOP/VESSEL FLANGE)
GI	GRAVITY INJECTION
GIRNS	GRAVITY INJECTION FROM IRWST VIA RNS SUCTION LINE

Figure 54-8

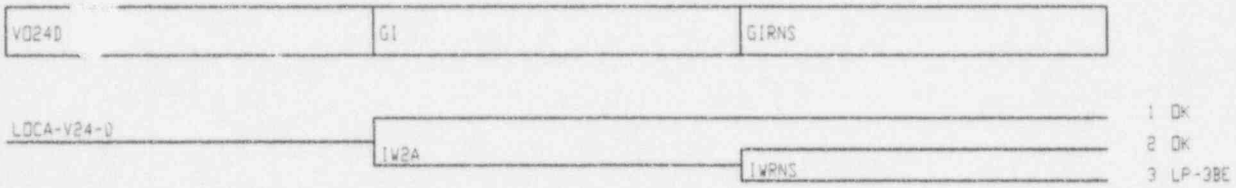
Loss of RNS Initiator (RCS Drained) Event Tree



Event	Description
LOCSD	LOSS OF CCW/SW DURING DRAINED MAINTENANCE (MID-LOOP/VESSEL FLANGE)
GI	GRAVITY INJECTION
GIRNS	GRAVITY INJECTION FROM IRWST VIA RNS SUCTION LINE

Figure 54-9

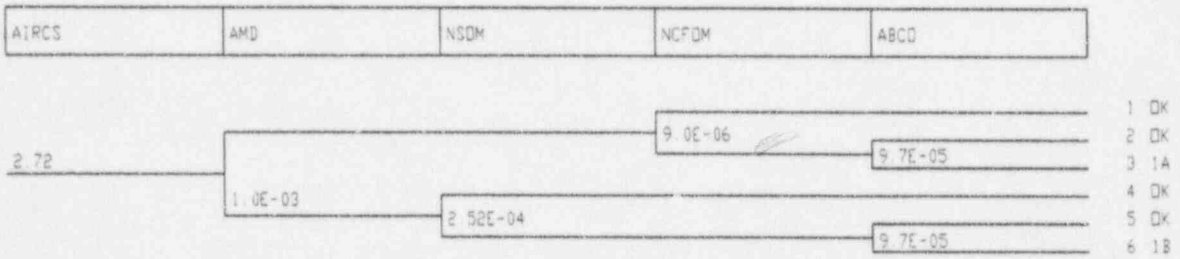
Loss of CCW/SW Initiator (RCS Drained) Event Tree



Event	Description
V024D	LOCA THROUGH RNS-V024 DURING DRAINED MAINTENANCE
GI	GRAVITY INJECTION
GIRNS	GRAVITY INJECTION FROM IRWST VIA RNS SUCTION LINE

Figure 54-10

LOCA/RNS-V024 Opens (RCS Drained) Event Tree



Event	Description
AIRCS	ACCUMULATOR INJECTION DURING REACTOR SHUTDOWN CONDITION
AMD	ACCUMULATOR MOVs DEENERGIZED
NSOM	NO SPURIOUS OPENING OF ACCUMULATOR MOVS
NCFOM	NO CATASTROPHIC FAILURE OF ACCUMULATOR MOVS
ABCD	ACCUMULATOR BORON CONCENTRATION OK

Figure 54-11

Accumulator Injection (Dilution Scenario) Event Tree

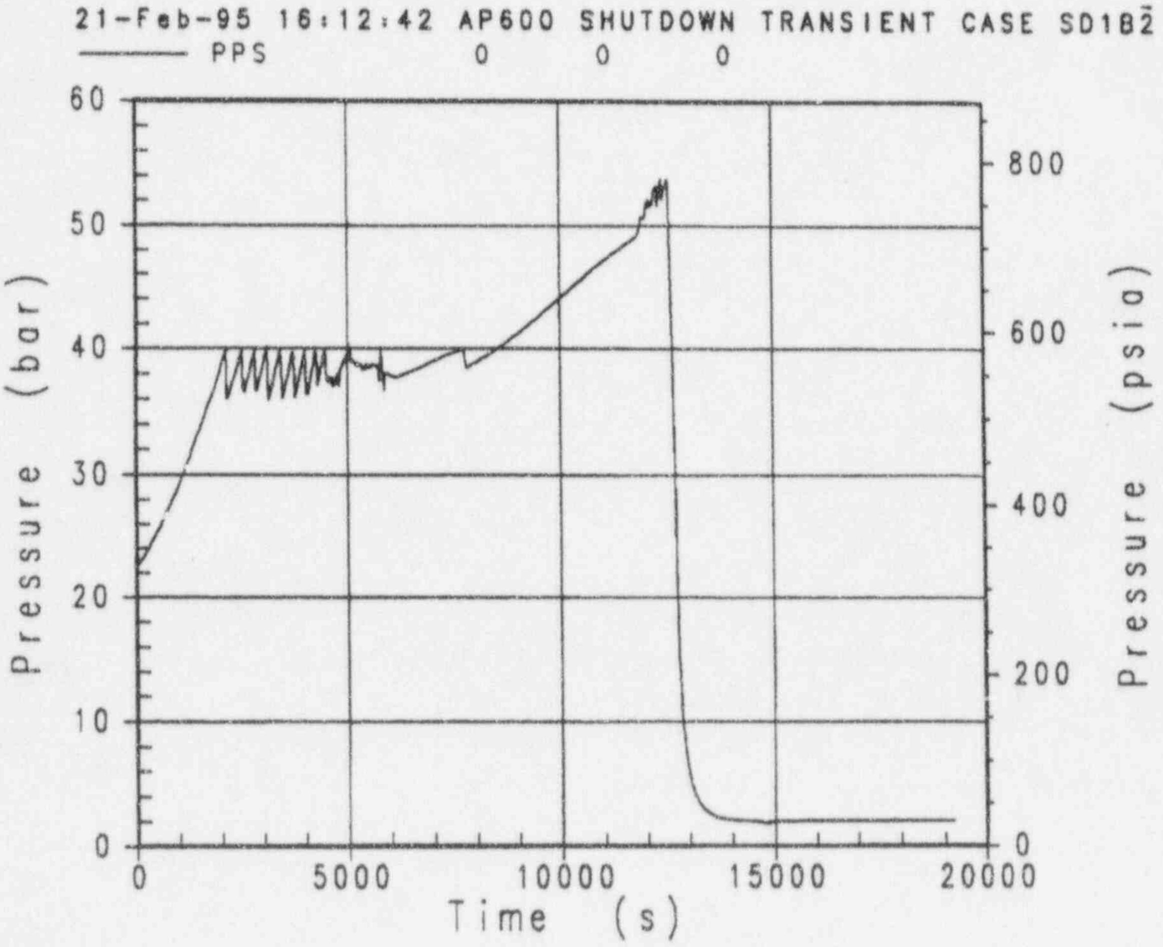


Figure 54-12

Shutdown Transient Case SD1B2 RCS Pressure vs. Time

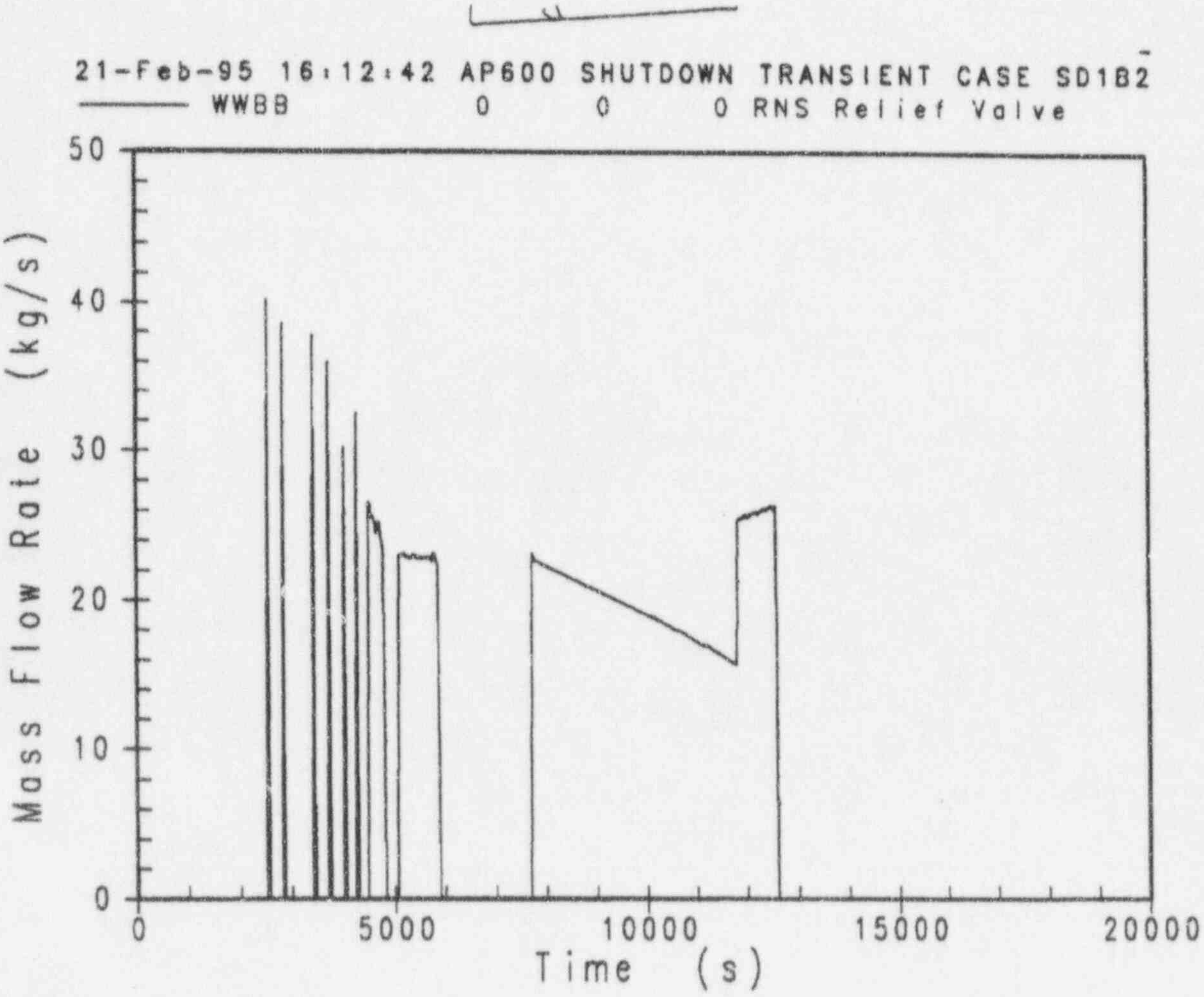


Figure 54-13

Shutdown Transient Case SD1B2 Mass Flow Rate vs. Time

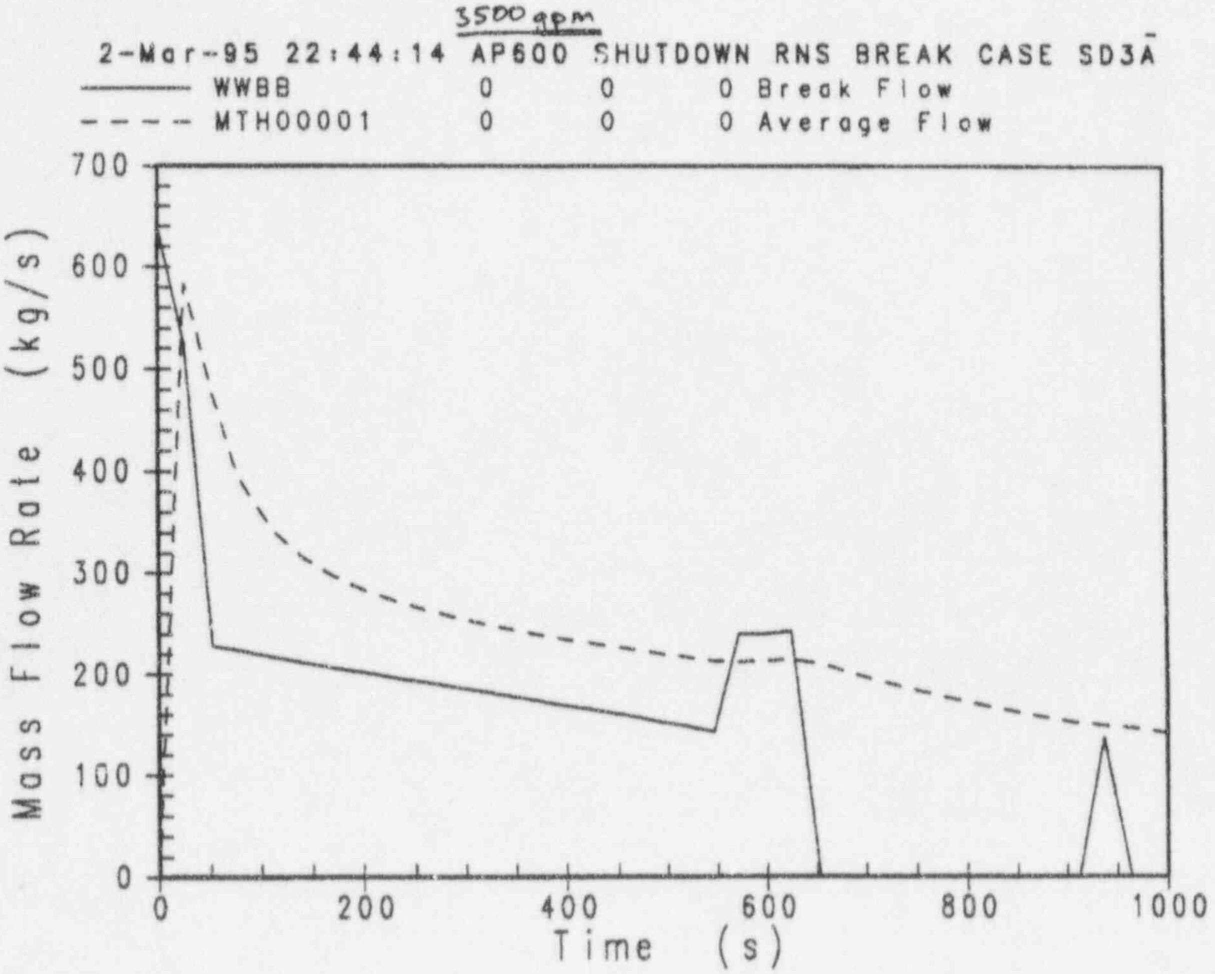


Figure 54-14

Shutdown RNS Break Case SD3A (3500 gpm)

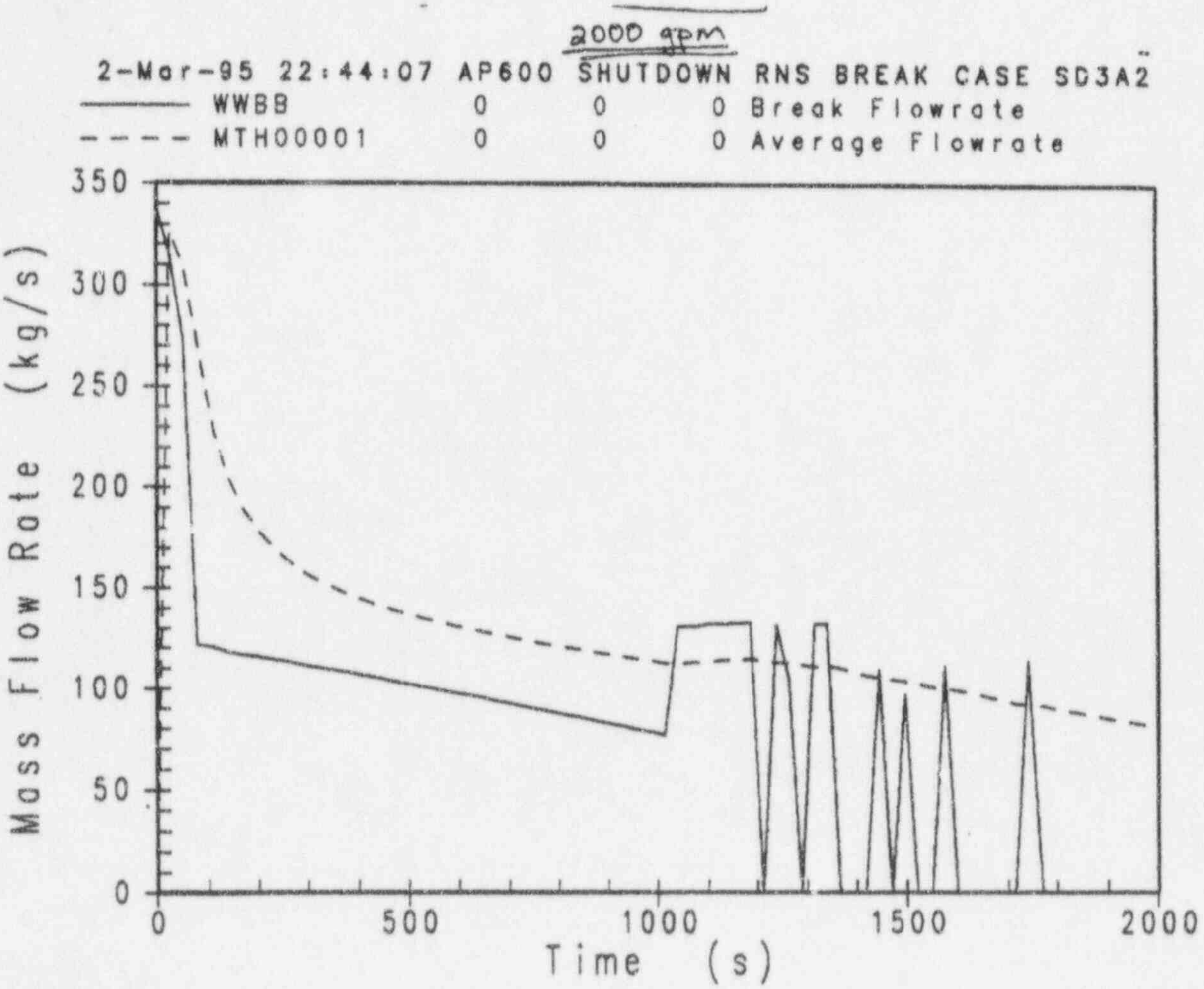


Figure 54-15

Shutdown RNS Break Case SD3A2 (2000 gpm)

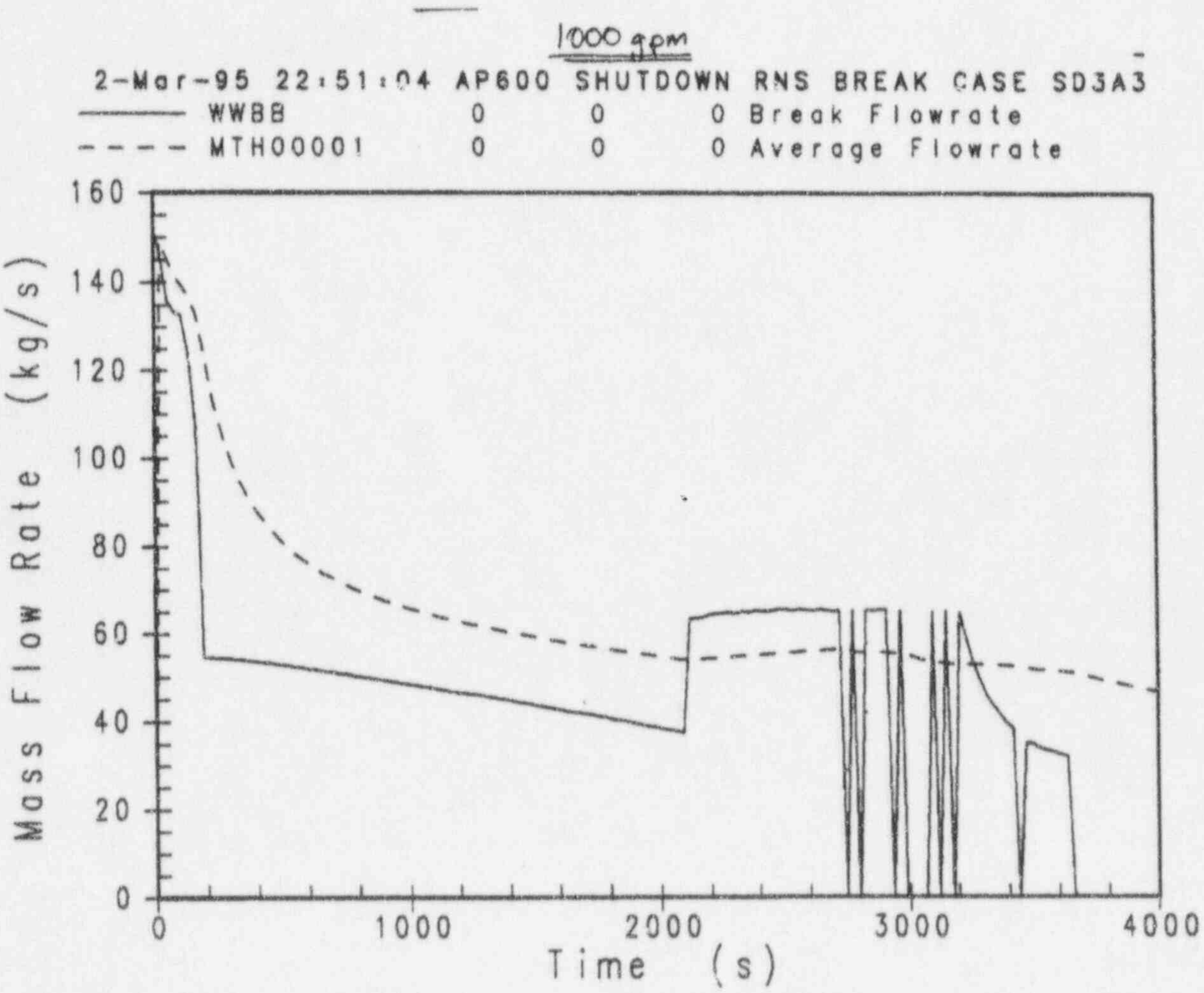
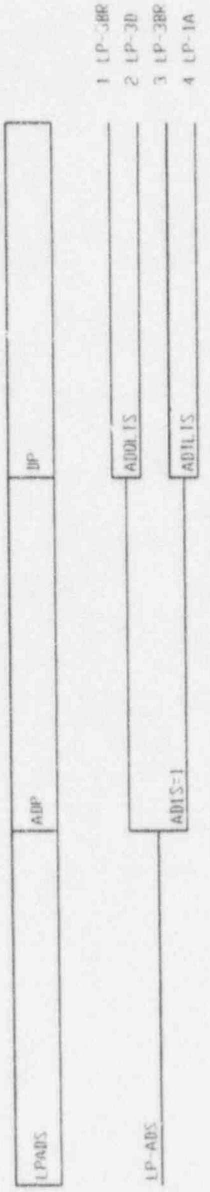


Figure 54-16

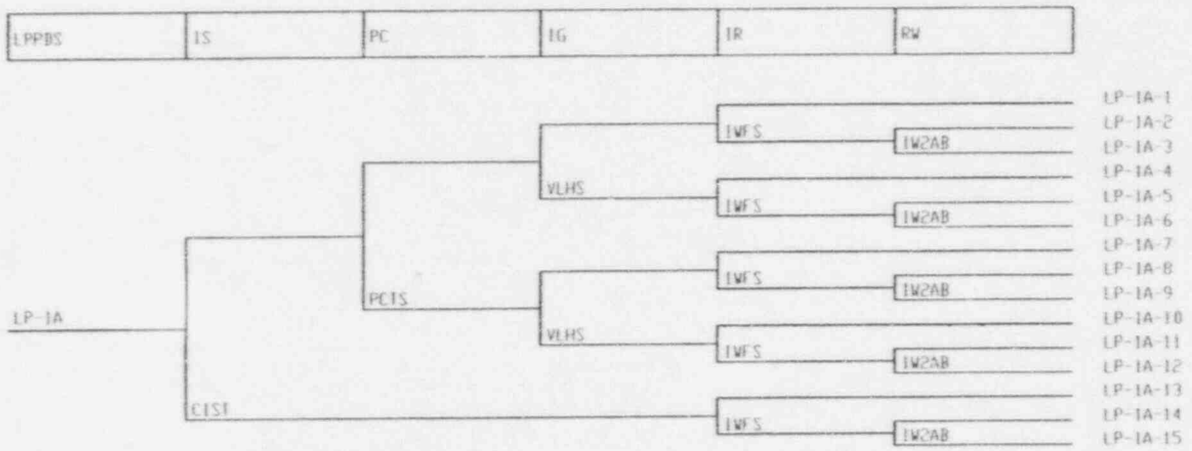
Shutdown RNS Break Case SD3A3 (1000 gpm)



Event	Description
ADP	PARTIAL DEPRESSURIZATION PRIOR TO CORE DAMAGE
DP	FULL DEPRESSURIZATION AFTER CORE DAMAGE

Figure 54-17

Shutdown Plant Damage State Substate Event Tree for LP-ADS

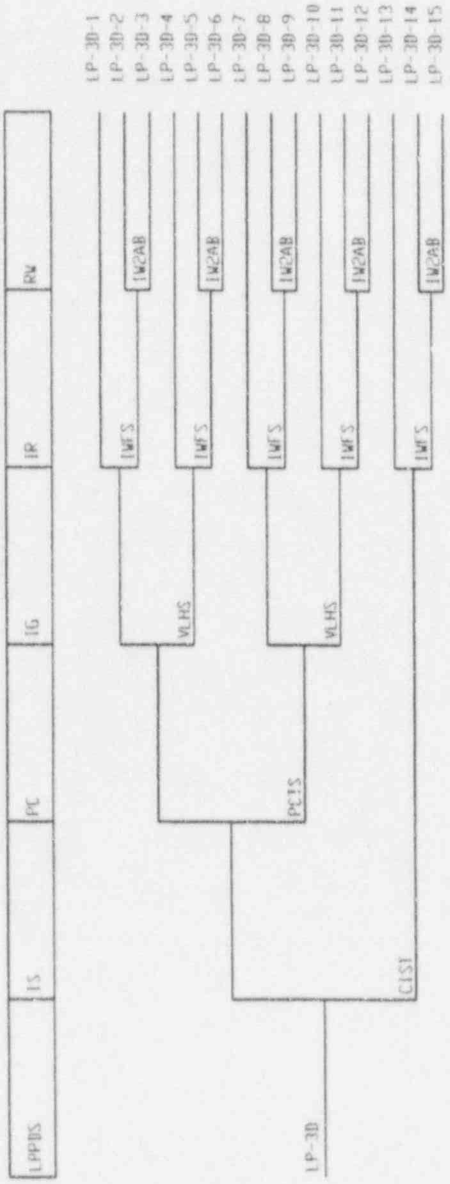


Event	Description
LPPBS	LOW POWER EVENT PLANT DAMAGE STATE
IS	ISOLATE CONTAINMENT
PC	OPERATE POSITIVE CONTAINMENT COOLING SYSTEM
IG	OPERATE HYDROGEN CONTROL SYSTEM
IR	FLOOD REACTOR CAVITY WITH IRWST WATER
RW	RECIRCULATE CONTAINMENT WATER INTO CAVITY FOR LONG-TERM DEB

Note: Failure of node RW is guaranteed if IR fails, because accumulators are isolated; there is insufficient water to recirculate into the reactor cavity.

Figure 54-18

Shutdown Plant Damage State Substate Event Tree for LP-1A

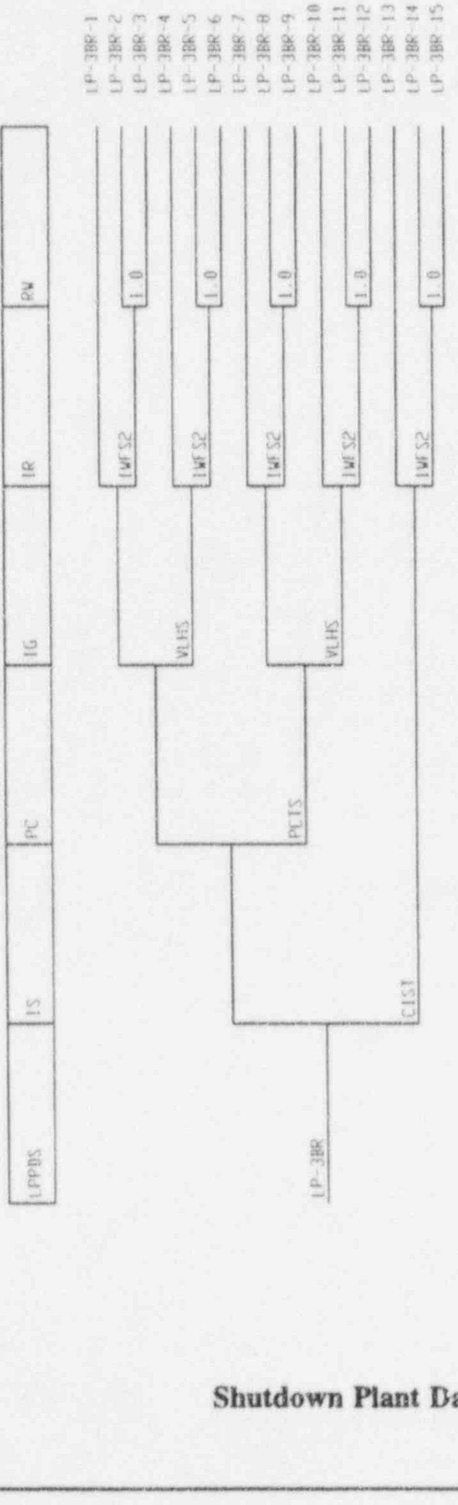


Event	Description
LPPDS	LOW POWER EVENT PLANT DAMAGE STATE
IS	ISOLATE CONTAINMENT
PC	OPERATE POSITIVE CONTAINMENT COOLING SYSTEM
IG	OPERATE HYDROGEN CONTROL SYSTEM
IR	FLOOD REACTOR CAVITY WITH IRWST WATER
RW	RECIRCULATE CONTAINMENT WATER INTO CAVITY FOR LONG-TERM DEB

Note: Failure of node RW is guaranteed if IR fails, because accumulators are isolated; there is insufficient water to recirculate into the reactor cavity.

Figure 54-19

Shutdown Plant Damage State Substate Event Tree for LP-3D



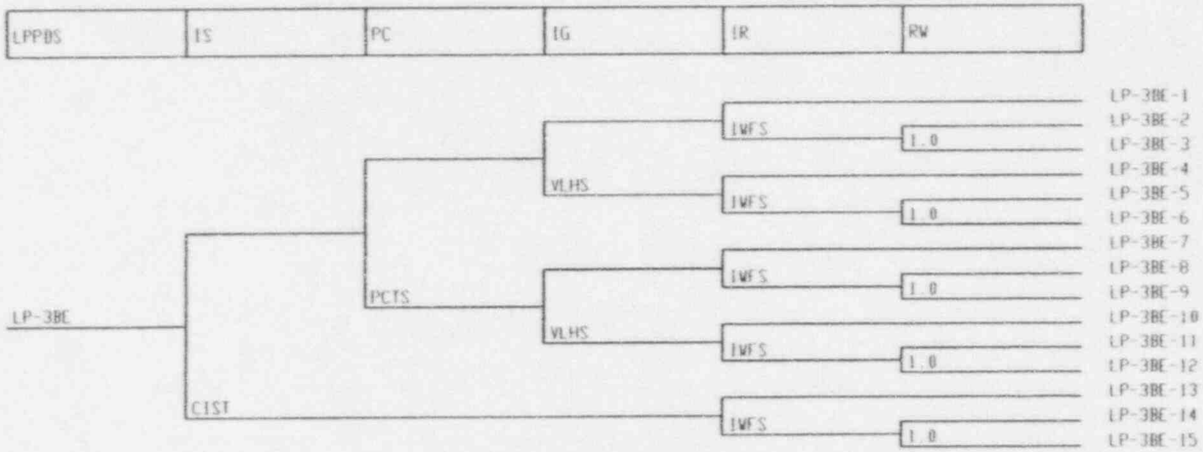
Event	Description
LPPDS	LOW POWER EVENT PLANT DAMAGE STATE
IS	ISOLATE CONTAINMENT
PC	OPERATE POSITIVE CONTAINMENT COOLING SYSTEM
IG	OPERATE HYDROGEN CONTROL SYSTEM
IR	FLOOD REACTOR CAVITY WITH IRWST WATER
RW	RECIRCULATE CONTAINMENT WATER INTO CAVITY FOR LONG-TERM DEB

Notes: Failure of node RW is guaranteed if IR fails, because accumulators are isolated; there is insufficient water to recirculate into the reactor cavity.

IWFS2 = IWFS * IW2AB

Figure 54-20

Shutdown Plant Damage State Substate Event Tree for LP-3BR



Event	Description
LPPDS	LOW POWER EVENT PLANT DAMAGE STATE
IS	ISOLATE CONTAINMENT
PC	OPERATE POSITIVE CONTAINMENT COOLING SYSTEM
IG	OPERATE HYDROGEN CONTROL SYSTEM
IR	FLOOD REACTOR CAVITY WITH IRWST WATER
RW	RECIRCULATE CONTAINMENT WATER INTO CAVITY FOR LONG-TERM DEB

Note: Failure of node RW is guaranteed if IR fails, because accumulators are isolated; there is insufficient water to recirculate into the reactor cavity.

Figure 54-21

Shutdown Plant Damage State Substate Event Tree for LP-3BE