19L ABWR Shutdown Risk Evaluation

19L.1 Purpose

The purpose of this study is to review the potential risk associated with ABWR operation while the plant is at low power or shut down. Events that have a potential to lead to accidents when the ABWR plant is shut down for maintenance or refueling are identified and reviewed against ABWR plant features which prevent and mitigate these accidents.

Additional information on ABWR shutdown risk is contained in Appendix 19Q.

19L.2 Conclusions

It is concluded that the ABWR plant is adequately protected against accidents during shutdown conditions. It is judged that the probability of core damage during shutdown periods is negligible and therefore it is concluded that no modifications to the ABWR plant design are required. It is also concluded that a detailed probabilistic risk assessment (PRA) for the ABWR shutdown conditions is not required.

19L.3 Introduction

The internal event PRA (Section 19.3) provided an extensive analysis of transients and accidents that initiate during power operation. The seismic PRA (Section 19.4) also consisted of events that initiate during power operation. In both PRAs, it was judged that the risks during shutdown conditions would be low with respect to those during power operations for several reasons:

(1) Most of the transients that disturb power operations do not apply to the shut down plant

(2) Low system pressure reduces the already small frequency of loss of coolant events due to pipe break

(3) Low decay heat means long time periods are available to restore cooling capability should residual heat removal system cooling be interrupted

In the Reactor Safety Study (Reference 19L-2) the shutdown risks were estimated to be negligible. EPRI conducted a somewhat detailed review of the shutdown risks for the Zion plant, a pressurized water reactor (PWR) (Reference 19L-3), and concluded that the mean core damage frequency (CDF) for the shutdown conditions is about a factor of four lower than the corresponding value for power operation. In a subsequent study (Reference 19L-4) for the Seabrook plant, another PWR, the shutdown risk was calculated to be about a factor of 5 lower than that for power operation. A French study (Reference 19L-5) has concluded that shutdown risks for the Paluel PWR plant constitute about 60% of the total plant risk. The NRC launched studies to estimate the risk associated with shutdown conditions for two plants: Surrey (PWR

plant, analyzed by Brookhaven) and Grand Gulf (BWR plant, analyzed by Sandia National Laboratories).

Appendix 19Q contains additional information on ABWR shutdown risk including a risk assessment of the loss of an operating RHR system during shutdown. This risk assessment evaluates the conditional core damage probability given a loss of one RHR train. Minimum sets of systems are identified that, if administratively controlled to not be in maintenance, will ensure an acceptably low conditional core damage probability. Other items discussed in 19Q are:

- ABWR features to minimize shutdown risk
- Procedures for completion of outage plans
- Use of freeze seals
- Evaluation of potential vulnerabilities due to new ABWR features
- How ABWR features could mitigate past events at operating BWRs

19L.4 Scope of the Study

19L.4.1 Mode of Reactor Operation

The various modes of ABWR reactor operation as noted in the plant technical specifications are shown in Table 19L-1.

The ABWR PRA (Section 19.3) covers periods of power operation (Mode 1) and start up periods (Mode 2), whereas this shutdown study covers periods of hot shutdown (Mode 3), cold shutdown (Mode 4), and refueling (Mode 5). Hot shutdown can be seen as an extension of the shutdown process started during Mode 1 and the incremental increase in risk during this mode of operation is judged to be small since the safety systems available for achieving hot shutdown continue to be available during hot shutdown. Loss of RHR in Mode 3 is discussed in Subsection 19Q.7.

There are four risk categories addressed by this shutdown analysis.

- Decay heat removal,
- Inventory control,
- Reactivity control,
- Electrical power (as a subset of inventory control and decay heat removal)

19L.4.2 Noncore-Related Events

Events which occur inside the containment that are not related to the fuel in the reactor core, but have a potential to release radioactivity to the environment were not included in the PRA, but are addressed in this study. Events outside the containment, such as the rupture of the liquid radwaste tank, are not reviewed in this study since they are judged to be negligible contributors to ABWR Plant risk.

19L.4.3 Summary of Types of Events Considered

The types of events considered in this shutdown risk study are summarized as follows:

(1) Reactivity Control Events (Subsection 19L.5)

(2) Inventory Control Events (Subsection 19L.6)

(3) Loss of Core Cooling (Subsection 19L.7)

(4) Loss of Decay Heat Removal Events (Subsection 19L.8)

(5) Non-Core-Related Events (Subsection 19L.9)

19L.5 Reactivity Control Events

Reactivity events which have a potential to occur during power operations are examined for their likelihood to occur during shutdown conditions. In addition, events which have a potential to occur only during shutdown conditions are also reviewed.

19L.5.1 Control Rod Drop Accident

The ABWR fine motion control rod drive (FMCRD) is equipped with several new and unique features to prevent a control rod drop accident compared with locking piston control rod drives (LPCRD) used in the boiling water reactors (BWR) currently in operation. Three modes of failure that could lead to a control rod drop accident have been identified and a summary of the event causes and preventive and mitigative features included in the FMCRD design is provided in Table 19L-2.

Subsection 15.4.9 provides a detailed review of the control rod drop accident during power operation and describes the ABWR features that prevent and mitigate the accident. The following discussion extends the review to shutdown conditions (operating Modes 3, 4, and 5).

For the rod drop accident to occur during power operation, the control rod must stick initially and then physically separate from the drive on a control rod withdrawal command. Later the same control rod becomes unstuck and drops freely resulting in a rod drop accident. For the rod drop accident to occur during operating Modes 3, 4, and 5, in addition to the above failures, the reactor must also be critical. Since the reactor is subcritical in these modes, even with the above sequence of failures, it is impossible for a rod drop accident to occur. The only time when the

above sequence of events could potentially result in a rod drop accident is when it occurs in conjunction with the withdrawal of an adjacent control rod for reasons such as testing. As will be shown by the following consideration and analysis, the probability of a control rod accident during operating Modes 3, 4, and 5 is negligible.

The ABWR features that help prevent control rod accidents are as follows:

(1) Each FMCRD is equipped with dual Class 1E separation detection devices that will detect the separation of the control rod from the CRD if the control rod and hollow piston stick and separate from the ballnut of the CRD. The separation switches can also detect if the blade separates from the hollow piston, even with the hollow piston still resting on the ballnut. The separation detection device is in operation at all times. When the separation has been detected, the interlocks will prevent further rod withdrawal (i.e., will initiate a rod block). Also, an alarm signal will be initiated in the control room to warn the operator.

(2) The hollow piston part of the FMCRD is equipped with a latch mechanism. If the hollow piston is separated from the ballnut and the rest of the drive due to a stuck rod, the latch will limit any subsequent rod drop to a distance of 20.32 cm (8 inches). (More detailed descriptions of the FMCRD system are presented in Subsection 4.6.1.)

(3) There is a unique, highly reliable bayonet-type coupling between the control rod blade and the control rod drive. The coupling spud at the top end of the hollow piston engages and locks into a mating socket at the base of the control rod. The coupling requires a 45-degree rotation for engaging or disengaging. Once locked, the drive and rod form an integral unit that must be manually unlocked by specific procedures before the components can be separated. This feature practically assures that the rod and the drive are never accidentally separated, and offers protection against the rod drop failure Mode 2 (Table 19L-2).

(4) Procedural coupling checks are enforced to assure proper coupling.

(5) Interlocks have been provided to assure that inadvertent criticality does not occur because a control rod is withdrawn adjacent to another control rod.

The Class 1E separation detection device and the control rod withdrawal interlock help prevent each of the three control rod drop failure modes listed in Table 19L-2. The other features that help prevent specific failure modes are discussed below.

Control rod drop failure requires the following events/failures:

For Failure Mode 1:

(1) Operator withdraws two control rods for testing,

(2) A third adjacent control rod sticks and unsticks at specific times,

(3) Class 1E separation detection of the third control rod or rod block fails,

(4) Operator tries to withdraw the third control rod and the interlock fails,

(5) Operator ignores alarm and continues withdrawal of the third rod, and

(6) Hollow piston latch of the third rod fails.

For Failure Mode 2:

(1) Operator withdraws two control rods for testing,

(2) A third adjacent control rod sticks and unsticks at specific times,

(3) Positive bayonet coupling of the third control rod experiences structural failure,

(4) Class 1E separation detection of third control rod or rod block fails,

(5) Operator tries to withdraw the third control rod and the interlock fails, and

(6) Operator ignores alarm and continues withdrawal of the third rod.

For Failure Mode 3:

(1) Operator withdraws two control rods for testing;

(2) Operator installs a third adjacent control rod drive without coupling, and fails to detect the error during procedural coupling checks;

(3) The third control rod sticks and unsticks at specific times;

(4) Class 1E separation detection of the third rod or rod block fails; and

(5) Operator ignores alarm and continues withdrawal of the third rod.

It is clear from the above discussion that multiple hardware failures and human errors have to occur to cause a rod drop accident. Even without a detailed analysis, it can be seen that the rod drop accident frequency is negligible. It is therefore concluded that the rod drop accident is unlikely to occur during Modes 3, 4, and 5 and is therefore not a safety concern for the ABWR.

19L.5.2 Control Rod Ejection Accident

The control rod ejection accident during the ABWR power operation starts with a major break in the FMCRD housing weld between the housing and the RPV, or a major break in the drive mounting bolts or a drive spool piece. The accident can also be started with a break in the drive

insert line. Following the break, the reactor pressure exerted on the CRD coupling pushes down the hollow piston and the ballnut with a large force. The shaft screw and the motor are forced to unwind, resulting in the rod being ejected. For the control rod ejection accident to occur during operating Modes 3, 4, and 5, in addition to the above failures, the reactor must also be critical. Since the reactor is subcritical in these modes, even with the above sequences of failures, it is impossible for a control rod ejection accident to occur. Similarly, the low pressures associated with these operating modes makes the break in the FMCRD housing or drive insert line extremely unlikely. The only time when the above sequence of events (i.e. those that cause control rod ejection accident during power operation) could potentially result in a control rod ejection accident during operating Modes 3, 4, and 5 is when it occurs in conjunction with a reactor hydro-test and withdrawal of an adjacent control rod withdrawn for reasons such as scram time testing. A summary of the causes of the rod ejection accident and the ABWR preventive and mitigative features is provided in Table 19L-3. As will be shown by following consideration and analysis, the probability of control rod ejection accident during operating Modes 3, 4, and 5 is negligible.

The ABWR features that prevent and mitigate control rod ejection accidents are:

(1) A break in the FMCRD housing (or weld between housing and vessel or drive mounting bolts or drive spool piece) is mitigated by integral internal blowout supports (“shootout restraints”) (Subsection 4.6.1.2.2.9) which physically prevent the control rod from being ejected.

(2) A break in the drive insert line is mitigated by the following:

   (a) Ball check valve in the CRD insert port.

   (b) Electromechanical brake

   The FMCRD design incorporates an electromechanical brake keyed to the motor shaft. The brake is normally engaged by a passive spring force. It is disengaged when the spring load is overcome by the energized magnetic force. The braking torque between the motor shaft and the CRD spool piece is sufficient to prevent control rod ejection in the event of a failure in the pressure retaining parts of the drive mechanism. The brake is designed so that its failure will not prevent the control rod from rapid insertion (scram). Additional details on the electromechanical brake are provided in Subsection 4.6.1.

   (c) Holding torque provided by the permanent magnet in the step motor prevents rod from being ejected during operating Modes 3, 4, and 5 when the reactor is not under pressure.

Control rod ejection can occur only under the following conditions:

(1) Failure of FMCRD housing, etc., coupled with failure of integral internal blowout support of one FMCRD when an adjacent drive has been withdrawn for testing and reactor is undergoing hydro-test (i.e. reactor is at pressure).

(2) Break in any one of the FMCRD insert pipes coupled with the failure of the corresponding ball check valve in the insert port and failure of the corresponding FMCRD electromechanical brake when an adjacent drive has been withdrawn for testing and reactor is undergoing hydro-test.

During operating Modes 3, 4, and 5, the time duration that the reactor is at pressure due to hydro-test is very small. Also, because of multiple independent failures required, the probability of a control rod ejection accident through above sequences is judged to be negligibly low. It is therefore concluded that the control rod ejection accident is unlikely to occur during operating Modes 3, 4, and 5 and is therefore not a safety concern for the ABWR.

19L.5.3 Refueling Error

Refueling errors resulting in the loading of fuel bundles in two adjacent uncontrolled cells could result in a reactivity accident. Uncontrolled cells are fuel cells in which control blades have been withdrawn. An accident can result from inserting a fuel bundle into a fueled region of the core which has withdrawn control blades.

Preventive and mitigative features in the ABWR plant are summarized in Table 19L-4 and discussed below:

(1) In the ABWR plant there is very little incentive for unloading the entire core. Generally, utilities resort to unloading the whole core when there is a need to maintain a large number of control rod drives during a refueling outage. In the case of ABWR, very few FMCRD need to be removed for maintenance and therefore there is very little incentive for unloading the whole core.

(2) During refueling, only one rod can be withdrawn. This is because Technical Specifications require that the gang/single selector switch in the Rod Control and Information System (RC and IS) be placed in the single position during refueling. Any attempt to withdraw a second rod results in a rod block initiated by the RC and IS.

(3) With mode switch in the REFUEL position, if any one control blade has been removed, then the refueling interlocks prevent hoisting another fuel assembly over the vessel (Subsection 9.1.4.2.7.1).

Therefore, for this accident to take place, the following events must occur.

(1) Utility decides to unload the whole core or perform control blade shuffling in parallel with refueling.

(2) One control blade is removed and its CRD is valved out of service.

(3) The rod block fails and the operators remove the adjacent control blade, and its CRD is valved out of service.

(4) Operator starts loading the fuel bundles. All fuel cells adjacent to withdrawn blades have been loaded except for the last fuel bundle.

(5) The last bundle is lowered into the empty uncontrolled fuel cell.

(6) The control room operator fails to observe SRNM multiplication.

(7) The reactor goes critical and high flux initiates a scram signal but valved out drives cannot scram.

As a consequence of this accident, local fuel failures can be expected, but the probability of this accident is also expected to be negligible for ABWR plants.

19L.5.4 Rod Withdrawal Error

During shutdown, there is a potential for the reactor to become critical if two adjacent control rods are withdrawn inadvertently. The ABWR features that prevent and mitigate this event are as follows:

(1) During refueling, Technical Specifications only allow one rod to be withdrawn at a time. Any attempt to withdraw a second rod results in a rod block by the rod withdrawal interlock.

(2) If the rod block fails and the rod is withdrawn, the reactor will scram on a high flux signal. The scram system is in operation at all times during shutdown.

Therefore, for this event to take place, the following events must occur:

(1) Operator withdraws one control rod for testing.

(2) Operator decides to test a second control rod without inserting the first control rod (i.e., operator does not follow procedures).

(3) The second control rod is adjacent to the first control rod which was withdrawn for testing.

(4) The interlock designed to prevent the withdrawal of the second rod fails.

(5) Rod fails to scram as designed.

The refueling interlock and the scram systems are highly reliable. The combined probability of operator error and failure of the above systems resulting in a rod withdrawal error is judged to be negligible.

19L.5.5 Fuel Loading Error

During refueling, there is a potential for the reactor to become critical if a fuel loading error is followed by withdrawal of a potentially high worth control rod. The ABWR features that prevent and mitigate this event are as follows:

(1) Operators follow specific core loading procedures.

(2) During core loading, interlocks prevent withdrawal of more than one control rod.

(3) Following the full core loading, an as-loaded core verification process is completed.

(4) If the reactor does become critical on a control rod withdrawal, it will be followed by a scram immediately, since the neutron monitoring system is in operation during refueling.

Therefore, for this event to take place, the following events must take place:

(1) Operators fail to follow fuel loading procedures and commit specific loading errors.

(2) Core verification fails to reveal the fuel loading error.

(3) Operator withdraws a control rod for testing.

(4) Reactor fails to scram.

It should be noted that not all fuel loading errors can initiate this accident. For fuel loading error to be a concern, the high worth fuel bundles must be loaded at the wrong location. The combined probability of this error plus the others listed above is judged to be negligible. Therefore, it is concluded that a fuel loading error during refueling is not a concern for the ABWR plant.

19L.5.6 Conclusion

It is concluded that, during operation Modes 3, 4, and 5, reactivity excursion events have a negligible probability of occurrence and are therefore not a safety concern for the ABWR plant.

19L.6 Inventory Control Events

There is a potential for draining the reactor vessel during operating Modes 3, 4, and 5, either as a result of hardware failures or operator errors or a combination of both. There is a potential for

draining the vessel during maintenance activities such as the CRD or reactor internal pump removal and replacement. There is also a potential for draining the vessel when systems feeding to and bleeding from the RPV are in continuous operation. The control room operator routinely monitors the water level and takes corrective actions such as isolating the appropriate valve when the water level drops for unexplained reasons. Certain other corrective actions initiate automatically. A discussion of these drain paths and the preventive and mitigative features of the ABWR design are discussed below.

19L.6.1 FMCRD Replacement

FMCRD replacement can take place only during operating Mode 5. The replacement is done in two steps. First the control blade is withdrawn until the blade back-seats on the guide tube to provide a metal to metal contact. This provides the seal for preventing the reactor water from draining.Then the CRD spool piece is removed at which time the spindle adaptor seats on the splined spindle adaptor back seat to prevent any leakage of water from the RPV. The drive can then be removed and replaced. This arrangement of preventing vessel draining through back-seating of the control blade is the same as the one used in the operating BWR plants. There is still a potential for the operator to remove the blade inadvertently. The probability of this error is minimized through administrative controls. Occasionally a small amount of water leakage is experienced due to imperfect sealing of the control blade. However, based on hundreds of reactor-years of operating experience, it is judged that the probability of draining the vessel during FMCRD replacement is negligible.

19L.6.2 Reactor Internal Pump

There is a potential for draining the RPV while the reactor internal pumps (RIP) are undergoing maintenance or replacement. Two such maintenance activities, replacement of the RIP motor and replacement of the RIP impeller are discussed below and summarized in Table 19L-5.

19L.6.2.1 RIP Motor Replacement

This activity is carried out only during operating Mode 5. After the bolts are loosened at the bottom, the whole pump moves down by about 6 mm until the impeller backseats to prevent leakage of reactor water when the motor cover is removed. A secondary seal is then provided inflated with the help of a portable pump. At this point, the RIP motor can be removed and replaced.

19L.6.2.2 RIP Impeller Replacement

Impeller replacement can be carried out only after the RIP motor is removed as described above. Following the removal of the motor, a temporary cover plate is bolted at the bottom. The impeller is then removed from the top. The seal is provided by the bolted cover plate at the bottom. After the impeller is removed, a cap is installed on the RPV bottom head at the impeller shaft opening to provide additional protection against draining the RPV.

19L.6.2.3 Potential for Draining

Nuclear plants with RIPs have been in operation for over 10 years. Over 500 RIPs and motors have been removed and reinstalled in the European BWR plants without any problem. This has demonstrated that the replacement activities can be carried out without draining the vessel. For draining to occur, as a minimum, the impeller backseat and the inflatable seal have to fail when the motor is being replaced. Administrative procedures assure that impeller removal does not start until the RIP motor is removed and the temporary motor cover plate is bolted. In the most likely failure scenario, it is possible that the sealing between the impeller shaft backseat and the sealing provided by the inflatable seal may not be perfect. However, such failures are detectable, and result only in a small leakage [6.3×10^{-5} m^3/s (less than one gallon per minute)]. Under these conditions, the operator can always bolt the temporary bottom plate if needed. During impeller replacement, for drainage to occur, the impeller shaft nozzle cap must fail (or be dislodged), finally the bottom plate must also fail. During maintenance on the inflatable seals, a plug is placed over the impeller diffuser inside the RPV to prevent draining. Subsection 19Q.4.2 contains additional information on RIP maintenance.

19L.6.3 Control Rod Drive Hydraulic System

During operating Modes 3, 4, and 5, the control rod drive hydraulic system (CRDHS) continues operating with one pump running to provide purge water to the FMCRDs. With one pump in operation, the head of the pumping water can easily overcome the pressurized head of the RPV; hence, there is no possibility of draining the RPV. In the event that neither pump is in operation, there is a potential for draining the RPV through the CRDHS as discussed below, summarized in Table 19L-6, and shown in Figure 19L-1. As will be shown by the following considerations and analysis, the probability of draining the RPV through the CRD hydraulic system is negligible.

19L.6.3.1 Path 1

When neither pump is in operation, the scram valves will open due to low hydraulic control unit (HCU) charging header pressure, and will stay open if

(1) The reactor protection system (RPS) scram logic is not reset, or

(2) There is no instrument air available to the scram valve, or

(3) The scram pilot solenoid valves are disconnected from the RPS scram circuits.

This, combined with the failures of the CRD ball check valve and check valve (F115), and the mechanical failure of the HCU maintenance isolation valves (F101, F140) and HCU drain valve (F113) to isolate when closed by the operator or the operator error to leave them open, will lead to drainage of the RPV into the CRD hydraulic system.

Multiple failures are necessary for path 1 to occur. Should they occur in one HCU, only 2 CRD's will be affected. In addition, the size of the piping connection between the RPV and CRDHS, being only 32A allows for a discharge rate which will provide enough time to remedy the situation. Therefore, the probability of draining the RPV through this path is judged to be negligible.

19L.6.3.2 Path 2

In the event where neither pump is in operation and the scram valves fail to open, there is still another potential path for draining the RPV through the CRDHS. Similar to the failures that resulted in path 1, (Subsection 19L.6.3.1) the CRD ball check valve must fail, and the HCU maintenance isolation valves (F101 and F140) must be open by operator error or mechanical failure. In addition, the scram valve must fail to open, the test port valve (F141) must be open by operator error or by mechanical failure, and testing equipment (or lack of) must fail. A drainage of the RPV through this path would lead to contamination of the plant environment.

Again, multiple failures are necessary for path 2 to occur; and, should a failure occur, only 2 CRDs will be affected and the slow discharge rate will provide time to correct the situation. In addition, the size of the piping connection between the RPV and CRDHS, being only 32A allows for a discharge rate which will provide enough time to remedy the situation. Therefore, the probability of draining the RPV through this path is judged to be negligible.

19L.6.3.3 Path 3

Path 3 is similar to path 2 with the exception that the test port valve (F141) remains closed, the check valve (F138) must fail and HCU isolation valve (F104) must fail open or be left open by the operator. Such an event could cause drainage of the RPV water into the CRDH System. As with all other paths in this system, multiple combinations are needed for an event to occur and the drainage rate will be slow. Therefore, the probability of draining the RPV through this path is judged to be negligible.

19L.6.3.4 Conclusion

In conclusion, because of the multiple failures required in each HCU, it is judged that the probability of draining the vessel through the CRDHS during shutdown is negligibly low. Also, because of the small drain line size, adequate time is available to remedy the situation should vessel drain start. It is therefore concluded that during operating Modes 3, 4, and 5, draining of RPV through failures in CRDHS is not a safety concern for the ABWR plant.

19L.6.4 Reactor Water Cleanup System

During the operating Modes 3, 4, and 5, the reactor water cleanup (CUW) system is used in conjunction with the fuel pool cooling and cleanup system (FPC) to provide continuous cleaning of the reactor water. During these modes, a single pump is needed to operate to provide 100% capacity. Reactor water flows from the RPV via both the RPV bottom head line and a

shared nozzle with the RHR suction line. There is a potential for draining the RPV through the CUW System during shutdown mode as discussed below, summarized in Table 19L-7 and shown in Figure 19L-2. As will be shown by the following considerations and analysis, the probability of draining the RPV through the CUW system is negligible.

19L.6.4.1 Path 1

During Modes 3, 4, and 5, one potential path for RPV drainage occurs when valves F500 and F501 are open (failed open or inadvertently opened by operator). Reactor water will drain to the low conductivity waste (LCW) sump in the drywell through a 50A diameter vessel nozzle. This path is unlikely to occur because valves F500 and F501 are in series, F500 is locked closed, and both valves are under administrative control. However, should this drain path be established, when the LCW drywell floor sump water level reaches high level, a persistent alarm is annunciated in the main control room to alert the operator for proper action. Also, drainage will be slow because of the small (50A diameter) size of the vessel drain nozzle, thereby allowing adequate time to correct the situation. Because of the above features, the probability of draining the RPV by this path is judged to be negligible.

19L.6.4.2 Paths 2 and 3

Paths 2 and 3 are dependent on the normally closed valves F055A and F055B. Both are used for chemical flushing and decontamination before maintenance. Should either of these two valves be left open during operating Modes 3, 4, and 5 (either by equipment failure or by operator error), reactor water will drain into the reactor building. Floor drain sumps are provided in the reactor building to collect waste from the equipment drains. If the water level in the drain sumps reaches a high level, an alarm is annunciated in the main control room to alert the operator. Should paths 2 or 3 occur, the drain path, a 50A diameter pipe, will allow sufficient time to correct the situation. Should no corrective action be taken manually, on reaching reactor water level 2, valves F002 and F003 will be isolated automatically, terminating the event. Also, the operator monitors the reactor water level in the control room and takes mitigative actions. Because of all these preventive and mitigative features, the probability of draining the RPV by this path is judged to be negligible.

19L.6.4.3 Path 4

Valves F022, F024 and F025 are normally closed. During the plant startup mode, excess water generated by reactor water level swell is dumped in a controlled manner to the main condenser. Flow control valve F022 regulates the blowdown flow. Should all three be inadvertently left open or fail open at the same time during operating Modes 3, 4, and 5, RPV water will drain to the suppression pool. There are a number of preventive and mitigative features in the ABWR design. The valves are redundant and the valve status (open, closed) is indicated in the control room for all three valves. In the unlikely event that reactor water is drained through this path, high flow will be detected by flow element FT-017 and signals will be sent to the leak detection system to isolate the CUW system. Furthermore, if this drain path is established, it will terminate on reactor level 2 isolation of valves F002 and F003. Also, the operator monitors the

reactor water level in the control room and takes mitigative actions. Because of all these preventive and mitigative features, the probability of draining the RPV by this path is judged to be negligible.

19L.6.4.4 Path 5

Path 5 is dependent on valves F022 and F023. Both are normally closed during operating Modes 3, 4, and 5. During startup, excess water generated by reactor water level swell is dumped in a controlled manner to the LCW collector tank. Flow control valve F022 modulates the blowdown flow. If both valves are left open (by operator error or equipment failure), RPV water will drain to the LCW collector tank. There are a number of preventive and mitigative features in the ABWR design. The valves are redundant and the valve status (open, closed) is indicated in the control room for all three valves. In the unlikely event that RPV water drains through these valves, high flow will be detected by flow element FT-017 which will send a signal to the leak detection system to isolate the CUW System. If established, the drain path will terminate on reactor level 2 isolation as before. Also, the operator monitors the reactor water level in the control room and takes mitigative actions. Because of all these preventive and mitigative features, the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.4.5 Path 6

Valve F056, which is used for chemical washing and decontamination before maintenance, is normally closed during operating Modes 3, 4, and 5. If it fails open or is inadvertently left open by the operator when the CUW pump is in operation, reactor water will drain into the reactor building. Similar to path 2, floor drain sumps are provided in the reactor building to collect waste from the equipment drains and high water levels in these sumps will activate an alarm to alert the operator. Since this is a small diameter pipe, the slow drainage rate will allow sufficient time to correct the situation before level 2 is reached at which point the path will terminate on reactor level 2 isolation signal. Also, the operator monitors the reactor water level in the control room and takes mitigative actions. Because of all these preventive and mitigative features, the probability of draining the RPV by this path is judged to be negligible.

19L.6.4.6 Path 7

Path 7 is similar to path 4. If valves F022 and F025 are inadvertently left open or fail open at the same time, RPV water will drain to the main condenser. The two valves in series and the valve status indicator help lower the possibility of this path occurring. In the unlikely event this path were to occur, flow element FT-017 will detect the high flow and signal the leak detection system to isolate the CUW system. If unmitigated, the drain path will be terminated on reactor water level 2. The probability of draining the RPV through this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.4.7 Conclusion

Because of the multiple failures or operator errors required for each of the above paths to occur, and the leak detection instrumentation in the drywell and reactor building that will alert the operator, it is judged that the probability of draining the RPV during shutdown mode through the reactor water cleanup system is low. Five of the seven potential drainage paths were screened from the analysis (Reference 19L-8 Table 6); the remaining two were quantified with a very low probability of occurring as the result (Reference 19L-8 Appendix F). Furthermore, as a mitigative measure, at reactor water level 2, CUW system valves F002 and F003 isolate the reactor from the CUW system. In practically all cases, even if all the above features should fail, the RPV drain will stop automatically when the RPV outlet nozzle is uncovered. At that point, there is still 1.6 meters of water over the top of the active core. It is therefore concluded that draining of the RPV through CUW system failures is not a safety concern for the ABWR plant.

19L.6.5 Residual Heat Removal System

The ABWR residual heat removal (RHR) system is a closed system consisting of three independent pump loops (A, B, and C—where B and C are similar) which inject water into the vessel and/or remove heat from the reactor core or containment. Loop A differs from B and C in that its return line goes to the RPV through the feedwater line whereas loop B and C return lines go directly to the RPV. In addition, loop A does not have connections to the drywell or wetwell sprays. However, for purposes of this analysis, the differences are minor and the three loops can be considered identical. The RHR system has many modes of operation, each mode making use of common RHR system components. These components are actuated by the operator; hence, the operation is subject to operator error which could potentially lead to drainage of the RPV. Potential paths for draining the RPV through the RHR system during operating Modes 3, 4, and 5 are discussed below, summarized in Table 19L-8, and depicted in Figure 19L-3. Of the various modes of RHR operation it was judged that the potential for RPV draining was the greatest during the shutdown cooling mode. Therefore, the potential RPV draining paths start with the RHR in the shutdown cooling mode of operation. As will be shown by the following consideration and analysis, the probability of draining the RPV through the RHR system is low. Even if all the preventive and mitigative features fail, RPV draining will stop when the RHR shutdown cooling nozzle is uncovered at which point there is still 1.6 meters of water over the top of the active fuel.

19L.6.5.1 Path 1 (Loop B and C only)

During the shutdown cooling mode of operation, pump C001 is in operation and valves F010, F011, F012, F004, F005 and F007 are normally open. One potential path will occur if valve F026 is open (by mechanical failure or operator error). This will lead to drainage of RPV water to HCW (high conductivity water). The preventive and mitigative features are as follows: valves F010 and F011 will isolate the reactor from the RHR system at reactor water level 3; the operator monitors reactor waterlevel in the control room and correctly responds to control room indicators and alarms; and the drain path is only a 40A diameter line allowing sufficient time

for corrective action. Because of all these preventive and mitigative measures, the probability of draining the RPV by this path is judged to be negligible.

19L.6.5.2 Path 2

With the pump running during the shutdown cooling mode of operation, path 2 will be established if the liquid waste flush valves (F029 and F030) are open by mechanical failure or operator error. Through this route, RPV water will drain to radwaste via a 150A diameter pipe. To prevent this from occurring, valves F029 and F030 are required to be closed during shutdown cooling mode, and if open, their open status will be indicated in the control room. Also at reactor water level 3, valves F010 and F011 will isolate the system. Finally, the operator monitors the reactor water level in the control room and takes corrective actions. Because of all these preventive and mitigative measures, the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.3 Path 3

During the shutdown cooling mode of operation, if the suppression pool return valve (F008) is open (by mechanical failure or operator error), potential draining path 3 will be established. This path will drain reactor water to the suppression pool. The preventive and mitigative features are as follows: an interlock prevents opening of valve F008 if F012 is open and vice versa and indicators in the control room will show the status of F008 and the reactor water level which will prompt the operator to correctly respond to these control room indicators and alarms. In addition, valves F010 and F011 will isolate the RHR system at reactor level 3. Because of all these preventive and mitigative measures, the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.4 Path 4

The fuel pool isolation valves (F014 and F015) are normally closed during shutdown cooling mode. Potential path 4 is established when the fuel pool isolation valves are open (by mechanical failure or operator error). By this path, reactor water will drain into the fuel pool through a 300A diameter pipe. The preventive and mitigative features are as follows: valve F014 is equipped with a key lock; and valves F010 and F011 will isolate the system at reactor water level 3. Also the operator should correctly respond when alerted by control room alarms and indicators. Because of all these preventive and mitigative measures the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.5 Path 5

Potential draining path 5 will occur if the drywell spray isolation valves (F017, F018) are opened inadvertently or fail to close during the shutdown cooling mode of operation. If this path is established, RPV water will be sprayed in the drywell through a 250A diameter pipe. The preventive and mitigative features are as follows: during shutdown cooling, with the drywell

pressure low, valves F017 and F018 cannot be opened at the same time because they are interlocked such that both can be opened simultaneously only if the drywell pressure is high. The status of valves F017 and F018 is indicated in the control room. Futhermore, the isolation valves F010 and F011 will isolate on reactor level 3 and the operator monitoring the water level in the control room will take corrective actions to further mitigate this drain path. Because of these preventive and mitigative measures, the probability for draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.6 Path 6

During shutdown cooling mode operation, the wetwell spray isolation valve, F019 is normally closed. If F019 is open (by operator error or mechanical failure), RPV water will be sprayed in the wetwell through a 100A diameter pipe. This event is unlikely to occur since it requires F019 to be open, the operator to incorrectly respond to control room alarms and indicators, and the failure of valves F010 and F011 to isolate the reactor from the RHR system at level 3. Because of these preventive and mitigative measures, the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.7 Path 7

During shutdown cooling mode operation, opening of normally locked closed valves F016 (by mechanical failure or operator error) establishes drain path 7 between the RPV and the fuel pool. However, since the fuel pool is at a higher elevation than the RPV, water cannot drain from the RPV to the fuel pool when the RHR pumps are not operating, and therefore this path is not a concern for the ABWR plant.

19L.6.5.8 Path 8

Potential path 8 will occur during shutdown cooling mode of operation if the normally closed valve F001 is open (inadvertently or by mechanical failure). Path 8 will drain RPV water to the suppression pool through an 450A diameter pipe. The preventive and mitigative features in the design are as follows: both F010 and F011 are interlocked to be opened only when the RPV is depressurized, F012 is interlocked such that it cannot be opened unless F001 is closed, and similarly, valve F001 cannot be opened unless valve F012 is closed. If the RPV drain path is established, draining will stop on reactor level 3 isolation of valves F010 and F011. Also, the operator monitors the reactor level in the control room and takes corrective actions. Because of all these preventive and mitigative measures, the probability of draining the RPV through this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.9 Path 9

Path 9 has the potential to drain reactor water to the suppression pool. The minimum flow valve, F021, will automatically open when pump C001 is running and the flow through the main loop (downstream of F004 and F013) is below the low flow setpoint. The valve will automatically close when the low setpoint is reached indicating sufficient flow. Inadvertent opening of this

valve will divert the flow to the suppression pool. The preventive and mitigative features in the design are as follows: valve F021 closes on receipt of normal flow signal in the main loop, the isolation valves F010 and F011 will isolate on reactor level 3 and the operator monitors the reactor water level in the control room and will take corrective actions to mitigate the event. Because of all these preventive and mitigative measures, the probability of draining the RPV by this path is minimal; however, it was quantified for this analysis (Reference 19L-8 Appendix F).

19L.6.5.10 Conclusion

Because of the multiple failures or operator errors required for each of the above paths to occur, and the numerous key locks, valve interlocks and control room indicators to prevent such paths, it is judged that the probability of draining the vessel during shutdown, through the RHR system is low. Two of the nine potential drainage paths were screened from the analysis (Reference 19L-8 Table 6; the remaining seven were quantified with a very low probability of occurring as the result (Reference 19L-8 Appendix F). Furthermore, as a mitigative measure, in all cases, at reactor water level 3, valves F010 and F011 isolate the reactor from the RHR system. Even if all these safety features fail, the RPV draining will stop automatically when the RHR shutdown cooling nozzle is uncovered at which point there is still 1.7 meters of water over the top of the active fuel. It is therefore concluded that draining of RPV through failures in RHR System is not a safety concern for the ABWR plant.

19L.6.6 Summary of Reactor Pressure Vessel Draining Events

Based on a review of maintenance activities which have the potential to drain the RPV and based on a review of the operation of water systems which are connected to the RPV, it is concluded that during operating Modes 3, 4, and 5, draining of the RPV is not a safety concern for the ABWR plant.

19L.7 Loss of Core Cooling

19L.7.1 Introduction

During operating Modes 3, 4, and 5, with the RHR system in operation in the shutdown cooling mode, no steam is being produced in the reactor and therefore there is no need for making up reactor coolant inventory using core cooling systems. Thus loss of core cooling capability in itself is not a concern unless either the RHR system becomes unavailable causing loss of coolant inventory through evaporation or the RPV is drained. As discussed in Subsection 19L.6 the probability of draining the RPV is low. The remaining sequences where loss of core cooling becomes a potential concern are discussed below.

Subsection 19Q.7 contains additional information on the risk associated with loss of core cooling during shutdown.

19L.7.2 Success Criteria

Many systems continue to be available for cooling the core during operating Modes 3 and 4.

A list of core cooling systems that satisfy the core cooling success criteria are as follows:

- CRDHS, or
- HPCF B or C, or
- LPFL A, B or C, or
- 1 feedwater pump + 1 condensate booster pump + 1 condensate pump + 1 condensate transfer pump, or
- AC-independent Water Addition System

Note that no credit is taken for the RCIC because of lack of steam in the reactor. If none of these systems are available initially, the reactor will heat up and be repressurized. If one of the high pressure make up systems is recovered, then immediate coolant makeup is possible. However, should one of the failed low pressure core cooling systems be recovered, the reactor will have to be depressurized prior to coolant injection.

The systems that satisfy the core cooling success criteria for operating Mode 5 are essentially same as those for operating Modes 3 and 4. One difference is that if none of these systems are available during operating Mode 5, the reactor will not be pressurized since the pressure vessel head has been removed. An additional difference is that if none of these sources of water is available, a flexible hose connected to the AC independent water addition system from any outside source of water can be used to cool the core since the decay heat rate diminishes substantially by the time operating Mode 5 is reached. It is thus concluded that loss of core cooling is more limiting for operating Modes 3 and 4 than for operating Mode 5. Therefore, the remainder of this review focuses on operating Modes 3 and 4.

19L.7.3 Review of Accident Sequence

The sequence of concern starts with a loss of RHR event. It is assumed that the low pressure core flooder LPFL (A, B and C) are unavailable and for core damage to occur the loss of RHR must be followed by failure of all remaining core cooling systems that meet the success criteria. Based on results of the internal event PRA, it is clear that the combined probability of failure of all systems is dominated by support system failures, especially offsite and onsite power failures. Table 19L-9 shows the dependency of the core cooling systems on power support systems. The ABWR plant technical specifications require that during operating Mode 4, at least one offsite AC power source and two diesel generators be available. In addition, the combustion turbine generator is expected to be available.

It is judged that the time window during which operating in Modes 3 and 4 is most vulnerable to accidents is the first week of operation in that mode. Following that period, decay heat levels are low enough that there is a high probability of recovering a failed system. During the first week, the most dominant cut-set for core damage is expected to consist of the following basic events:

(a) Loss of offsite power during the first one week period of operating in Mode 3 and 4 with no recovery, and

(b) Failure of diesel generators, and

(c) Combustion turbine generator failure to start, and

(d) Failure of operator to initiate the AC-independent Water Addition System, and

(e) Failure of operator to recover any one of the failed systems.

The combined failure probability of all these systems is negligible, even when excluding operator failure to recover.

It is recognized that there are other cutsets that could contribute to core damage. Also, at certain times, some of the systems may be unavailable due to maintenance. (The plant technical specifications control the number of safety systems that can unavailable at any given time.) On the other hand, the above calculation takes no credit for power or equipment recovery, even though sufficient time is available. Therefore, it is judged that even after the above considerations are factored in, the combined failure probability would be negligible.

19L.7.4 Conclusion

It is concluded that loss of core cooling capability during operating Modes 3, 4, and 5 is a negligible contributor to ABWR plant risk.

19L.8 Loss of Decay Heat Removal Events

19L.8.1 Introduction

In the ABWR internal event PRA, (Section 19.3) accident sequences were analyzed to a point where the reactor is in a condition of hot stable shutdown with the reactor mode switch in shutdown, the reactor subcritical, pressures and temperatures stabilized and within limits, containment and suppression pool cooling being maintained and vessel water level controlled. The heat removal systems were evaluated for the first 24 hours of operation. Therefore, the shutdown risk evaluation for operating Mode 4 begins at 24 hours after shutdown. Twenty four hours of shutdown cooling results in a reactor coolant temperature of 60°C or less. It takes about 2 to 3 days to reach operating Mode 5. Therefore, evaluation for operating Mode 5 starts at about 48 hours after reactor shutdown.

Subsection 19Q.7 contains additional information on the risk associated with loss of decay heat removal during shutdown conditions.

19L.8.2 Accident Initiators

The core cooling and heat removal systems are either available or in operation at the onset of operating Modes 4 and 5. (Scenarios involving failure of these systems prior to shutdown are analyzed in the internal event PRA.) This means, prior to operating Mode 4, at least 24 hours of core and containment cooling has been successfully in operation. At this point, accidents involving loss of the intended RHR heat removal function can be initiated only as follows:

- Internal failures in the RHR System, or
- Failures in the RHR support systems such as offsite and onsite power, or service water, or
- Improper operation of the RHR system (flow diversion by operator).

19L.8.3 Success Criteria

The ABWR plant features many redundant means of removing decay heat. In the internal event PRA, depending upon the sequence, credit has been taken for the following:

- Main condenser (normal heat removal path)
- RHR (3 redundant loops)
- Reactor water cleanup heat exchanger

An overpressure relief rupture disk (containment vent) has been added to the ABWR design and this can also be used to remove the containment heat under certain conditions.

The success criteria for operating Mode 4 are given in Table 19L-10. It should be noted that even though the reactor is at low pressure, main condenser and CUW heat exchangers can still be used to remove decay heat following failure of the RHR system. Also, there are two 100% CUW pumps, either of which can be used with the CUW heat exchangers. The overpressure relief rupture disk comes into play when the containment is pressurized following the loss of all heat removal systems.

During operating Mode 5 both the RPV and drywell heads are open and the containment is thus “vented” already. Complete failure of heat removal functions would result in initially heating the pool of water and eventually, in the worst case, boiling the water. For all practical purposes this is similar to removing the containment heat through the overpressure relief rupture disk (vent) following which the suppression pool begins to boil. In both cases water makeup to the respective pools is necessary. In other words, operating the reactor in Mode 5 can be seen as operating with a vented containment, and if heat removal functions are lost during this mode, the only action needed is to make up the water inventory lost by evaporation.

The RHR design has three RHR loops connected to the fuel pool with normally closed inter-ties to permit additional supplemental cooling during refueling outages to reduce outage time.

There is sufficient time available to provide the makeup water and therefore loss of RHR during operating Mode 5 is not judged to be a safety concern. Therefore, the rest of this review focuses on operating Mode 4.

19L.8.4 Review of Accident Sequence

At the start of the event, the core cooling as well as the heat removal functions are in operation. Initially, the heat is removed by the main condenser and after the reactor pressure is reduced, if the reactor is not isolated, the RHR system is engaged in the shutdown cooling mode. If the reactor is isolated, core cooling is provided by the high pressure system and the heat rejected to the suppression pool through the SRVs is removed by the RHR system in the suppression pool cooling mode. At about 24 hours into the event, with the reactor temperature at approximately 60°C, the RHR system fails as a result of internal failures, or support system failures. Loss of RHR function is the initiator. Success criteria are listed in Table 19L-10.

The probability that all these systems will fail due to unrelated problems is judged to be negligible. It is more likely that these systems will fail as a result of failures in the support systems. Table 19L-11 shows the power related support systems for the systems listed in the success criteria. The ABWR plant technical specifications require that during operating Mode 4, at least one offsite AC power source and two diesel generators be available. In addition, the combustion turbine generator is expected to be available. The most likely accident initiator is the loss of offsite power. If power is not recovered in time (say 24 hours), and the diesel generators and the combustion turbine generator fail to start, then the only heat removal system available is the overpressure relief rupture disk.

The combined failure probability of this event sequence is negligible. It is recognized that this analysis does not include all the failure paths and does not account for equipment that are unavailable due to maintenance. On the other hand, it should also be noted that failure of heat removal function does not automatically lead to core damage as has been assumed above. Only a fraction of these sequences lead to core damage as would be evident if detailed containment event trees were developed. On balance, it is concluded that the probability of core damage, resulting from a loss of containment heat removal function during operating Mode 4 is negligible. It has also been identified that no problems are anticipated during operating Mode 5 as long as the water evaporated by boiling is periodically made up. Thus, in summary, it is concluded that loss of containment cooling function during operating Modes 4 and 5 pose a negligible threat to the ABWR plant safety.

19L.9 Noncore-Related Accidents

19L.9.1 Introduction

Many noncore-related accidents can be postulated during operating Modes 3, 4, and 5. However, it is judged that the consequences of any accident that does not involve fuel bundles is negligible. Thus for instance, drainage of the radwaste tank is not considered in this study.

Accidents considered here are the fuel bundle drop accident, spent fuel cask drop accident, loss of fuel pool cooling, and drainage of fuel pool.

19L.9.2 Fuel Drop Accident

The fuel handling accident can only be assumed to occur as a sequence of failures in the fuel assembly lifting mechanisms which will result in the dropping of a fuel bundle and the subsequent release of radioactive materials from damaged rods. A detailed probabilistic analysis of such an accident was not performed based upon the following considerations.

(1) The probability for the failure of mechanisms involved in fuel handling either through mechanical failure or human action is assumed very small based upon the small number of cases seen to date throughout the nuclear industry in the handling of literally thousands of fuel bundles. Therefore, initially the probability of a fuel bundle being dropped is very small.

(2) Given the occurrence of a fuel bundle being dropped, the radiological consequences depend upon the distance of fall, the angle of impact, and the surface onto which the bundle would fall. For the exposure time during which any fuel bundle is being moved from point A to point B, the potential consequences are a function of probability involving distance of fall, type of bundle being dropped (exposed or fresh), and surface onto which the bundle can fall (steel, concrete, other bundles and their exposure history).

(3) Based upon the reasoning in paragraph 2 above and upon current operating experience, the more probable fuel drop events result in damage to no to a few rods (less than 10). Considering the factor of radioactive decay prior to handling exposed fuel, the use of safety systems (the failure of which would reduce the potential accident probability), volatility and migrability of the fission products through water pools and potential in plant transport analysis, maximal whole body and thyroid doses less than a few tenths of a milliRem at extremely low probabilities could be expected at the site boundary.

(4) Given releases for larger events at lower probabilities and the factors above, doses up to one millirem at even lower probabilities are estimated.

It is therefore concluded that this accident is a negligible contributor to ABWR plant risk.

19L.9.3 Spent Fuel Cask Drop Accident

The spent fuel cask drop accident is discounted as a credible accident based upon the following logic.

(1) The probability of dropping a spent fuel cask during handling is extremely low due to the mechanical interlocks and safety systems used. During handling the cask is

moved via a type 1 crane with redundant rigging with both procedural and mechanical interlocks to prevent movement of the cask over areas such as the spent fuel pool.

(2) During handling from the cask loading pit to the cleaning pit the cask lid is in place and the height of lift is limited such that a fall would not result in any significant damage to the cask and no damage to the cask contents. The cask is sealed in the cleaning pit and given that a drop occurs over the hatch in transient to the loading dock, the maximum fall would not be expected to result in sufficient impact to damage the cask based upon cask design requirements from DOE.

(3) Even assuming potential releases from a cask, the minimum time for fuel movement is generally one year after removal from the core which results in the decay of all volatile isotopes except Kr-85. Owing to Kr-85's low gamma energy, such a release would result in doses which are less than 0.1E–06 Sv or accidents of probability on the order of or less than 1.0E–06 at the site boundary.

It is therefore concluded that this accident is a negligible contributor to ABWR plant risk.

19L.9.4 Loss of Fuel Pool Cooling

In the ABWR plant, the fuel pool cooling and cleanup FPC system is backed up by the RHR system. Therefore, fuel pool cooling function is lost only if both the FPC and three loops of RHR system become unavailable. Even if these systems become unavailable, adequate time will be available for repairs to be made to restore the failed systems before fuel damage occurs. Providing makeup water alone will mitigate the accident and many sources of water exist including fire or potable water. The combined probability of loss of FPC and RHR and failure to repair the failed system or provide makeup water is judged to be negligible and therefore it is concluded that this event is a negligible contributor to ABWR plant risk.

19L.9.5 Drainage of Fuel Pool

FPC system is designed with no piping penetrations or drain paths which can drain the fuel pool. Further, there are no potential paths for siphoning water from the pool. Thus it is impossible to drain the pool inadvertently. For fuel pool drainage to occur, the pool liners must fail causing leakage of water from the pool. A postulated means of damaging the liners is dropping of a heavy load, such as the fuel transfer cask in the fuel pool. In WASH-1400 (Reference 19L-2) the probability of draining the pool by this postulated accident was estimated to be negligible. The WASH-1400 analysis is judged to be applicable for ABWR also, and it is therefore concluded that this event is a negligible contributor to ABWR plant risk.

19L.10 References

19L-1 Not Used.

19L-2 "Reactor Safety Study—An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014), USNRC, October 1975.

19L-3 "Zion Nuclear Power Plant Residual Heat Removal PRA", NSAC/84, NSAC/EPRI, July 1985.

19L-4 "Seabrook Station Probabilistic Safety Study—Shutdown (Modes 4, 5 and 6)", New Hampshire Yankee, May 1988.

19L-5 A. Villemeur, et al. (Electricite de France), "Living Probabilistic Safety Assessment of a French 1300 MWe PWR Nuclear Power Plant Unit: Methodology, Results and Teachings", Published at TUV-Workshop on Living PSA Application, Hamburg, FRG, May 7-8, 1990.

19L-6 Not Used.

19L-7 Not Used.

19L-8 "ABWR Shutdown Risk Evaluation", Toshiba UTLR-0013.

Table 19L-1 ABWR Modes of Operation

Mode*	Title	Reactor Mode Switch Position	Average Reactor Coolant Temperature, K (°C)
1	Power Operation	Run	Any temperature
2	Startup	Startup/Hot Standby	Any temperature
3	Hot Shutdown	Shutdown	>366.45 K (> 93.3°C)
4	Cold Shutdown	Shutdown	≤366.45 K (≤ 93.3°C)
5	Refueling	Shutdown or Refuel	≤366.45 K (≤93.3°C)†

* In Modes 1 through 4, fuel is in the reactor vessel with the reactor vessel head closure bolts fully tensioned. In Mode 5, fuel is in the reactor vessel with the reactor vessel head closure bolts less than fully tensioned or with the head removed.

† Technical specification states “any temperature”, but in this mode the temperature will be below boiling point.

Table 19L-2 Control Rod Drop Accident

Cause/Event		Preventive and Mitigative Features
Hardware	**Operator**	
Failure Mode 1		
1. —	Two control rods withdrawn for test.	—
2. A third adjacent rod sticks (still coupled to hollow piston)	—	—
3. —	The third control rod is withdrawn	Interlock prevents withdrawal of the third control rod
4. Separation of ballnut and hollow piston in the third control rod	Operator misses alarm and continues withdrawal of the third control rod	Class 1E separation detection
5. The third control rod unsticks and drops	—	Rod block + hollow piston latch
Failure Mode 2		
1. —	Two control rods withdrawn for test.	—
2. A third adjacent control rod sticks	—	—
3. —	The third control rod is withdrawn	Interlock prevents withdrawal of third control rod
4. Rod to hollow piston separation occurs in the third control rod	Operator misses alarm and continues withdrawal of the third control rod	1. Positive bayonet coupling 2. Class 1E separation detection
5. The third control rod unsticks and drops	—	Rod block
Failure Mode 3		
1. —	Two control rods withdrawn for test	—
2. —	A third adjacent control rod is installed without coupling	—
3. —	Error in the third control rod not detected during coupling check	
4. —	The third control rod withdrawn	Interlock prevents withdrawal of third control rod

Table 19L-2 Control Rod Drop Accident (Continued)

	Cause/Event		Preventive and Mitigative Features
	Hardware	Operator	
5.	The third rod sticks	—	—
6.	Rod to hollow piston separation in the third control rod	Operator misses alarm and continues withdrawal of the third control rod	Class 1E separation detection
7.	The third control rod unsticks and drops	—	Rod block

Table 19L-3 Control Rod Ejection Accident

Cause/Event		Preventive and Mitigative Features
Hardware	**Operator**	
Failure Mode 1		
1. Reactor under hydro test	—	This occurs during a small fraction of time during shutdown
2. —	Two control rods withdrawn for testing	—
3. Break in the adjacent FMCRD housing or weld between housing and vessel or CRD mounting bolts or CRD spool piece	None	Integral internal blowout support (“shootout restraints”)
Failure Mode 2		
1. Reactor under hydro test	—	This occurs during a small fraction of time during shutdown
2. —	Two control rods withdrawn for testing	—
3. Break of insert pipe in the adjacent CRD	None	1. Ball check valve in insert port 2. FMCRD electro-mechanical brake

Table 19L-4 Refueling Error

	Cause/Event	
	Hardware Failure	Operator Error/Action	Preventive and Mitigative Features
1.	—	Utility plans to offload all fuel bundles or perform multiple control blade shuffles	No incentive for unloading all fuel bundles because very few FMCRDs need to be maintained during refueling
2.	—	One CRD removed	
3.	—	Adjacent CRD removed	Interlock prevents withdrawal of second CRD
4.	—	Operator starts loading the fuel bundles, the last bundle is lowered into the empty uncontrolled fuel cell	Automatic refueling machine interlocked to prevent hoisting a fuel assembly over the vessel

Table 19L-5 Potential for Draining RPV During RIP Maintenance

Cause/Event		Preventive and Mitigative Features
Activity	Cause	
Replacement of RIP motor	Potential leakage path from RPV to outside due to pressure difference	1. Impeller backseats to prevent leak 2. Inflatable seal provides backup seal
Replacement of RIP impeller	Same as above	1 and 2. Same as above since initially the motor is removed 3. Temporary motor cover plate is bolted 4. Impeller removal results in the loss of the pump shaft backseat seal, but impeller diffuser cap is inserted in the impeller cavity to provide additional protection
Maintenance on inflatable seal	Same as above	1. Plug over RIP nozzle inside RPV prevents draining

Table 19L-6 Potential for Draining RPV Through Control Rod Drive Hydraulic System at Shutdown

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
1A	Both CRD pumps + CRD ball check valve + HCU maintenance isolation/drain valves (F101, F140, F113) + Check valve (F115)		Drain RPV water into CRDHS	Pump required to run continuously Multiple failures necessary Potential draining pipes are only 32 A each allowing sufficient time for mitigation
1B	CRD ball check valve + Check valve (F115)	Both pumps off + HCU maintenance isolation/drain valves (F101, F140, F113) left open	See 1A	See 1A
2A	Both CRD Pumps + CRD Ball Check Valve + HCU maintenance isolation valves (F101, F140) + Scram valve closed + Test port valve open (F141) + Test equipment		RPV water leaks into HCU environment	See 1A
2B	CRD ball check valve + Scram valves closed	Both pumps off + HCU maintenance isolation valves (F101, F140) open + Test port valve (F141) open + No test fixture in test port	See 2A	See 1A

Table 19L-6 Potential for Draining RPV Through Control Rod Drive Hydraulic System at Shutdown (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
3A	Both CRD pumps + CRD ball check valve + HCU maintenance isolation/drain valves (F101, F140, F104) + Scram valve closed + check valve (F138)		See 1A	See 1A
3B	CRD ball check valve + Scram valve closed + Check valve F138	Both pumps off + HCU maintenance isolation valves (F101, F140, F104) left open	See 1A	See 1A

Table 19L-7 Potential for Draining RPV Through Reactor Water Cleanup System

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
1A	Valve F500 fails open + Valve F501 fails open		Reactor water drains to low conductivity waste sump	Drain line is only 50 A diameter Leak detection alarm in main control room Valves are redundant Operator monitors reactor water level in the control room and takes corrective action
1B		Valve F500 open + Valve F501 open	See 1A	Valve F500 under key lock + administrative control + valves are redundant See 1A
2 and 3 A	Valve F055A fails open or Valve F055B fails open		RPV water drainage into reactor building	Drain Line is only 50 A diameter Leak detection alarm in main control room Path terminates on reactor Level 3 isolation signal Operator monitors reactor water level in the control room and takes corrective action
2 and 3 B		Valve F055A open or Valve F055B open	See 2A	See 2A

Table 19L-7 Potential for Draining RPV Through Reactor Water Cleanup System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
4A	Valve F022 fails open + Valve F024 fails open + Valve F025 fails open		RPV water drainage to suppression pool	Redundant (3) valves CUW isolation on high flow Control room indicator of valve status Path terminates on reactor level 3 isolation signal Operator monitors reactor water level in the control room and takes corrective action
4B		Valve F022 open + Valve F024 open + Valve F025 open	See 4A	See 4A
5A	Valve F022 fails open + Valve F023 fails open		RPV water drainage to LCW collector tank	Redundant (2) valves CUW isolation on high flow Path terminates on reactor Level 3 isolation signal Operator monitors reactor water level in the control room and takes corrective action
5B		Valve F022 open + Valve F023 open	See 5A	See 5A

Table 19L-7 Potential for Draining RPV Through Reactor Water Cleanup System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
6A	Valve F056 fails open		See 2A	See 2a
6B		Valve F056 open	See 2A	See 2A
7A	Valve F022 fails open + Valve F025 fails open		See 4A	See 5A
7B		Valve F022 open + Valve F025 open	See 4A	See 5A

Table 19L-8 Potential for Draining RPV Through Residual Heat Removal System

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
1A [A] =	Pump C001 running + Valve F011 open + Valve F010 open + Valve F012 open + Valve F026 fails open		Drain RPV water to HCW	1. F010 and F011 isolation on reactor level 3 2. Operator monitors level in control room and takes corrective action 3. Drain line is only 50 A diameter allowing sufficient time for corrective action
1B		[A] + Valve F026 inadvertently opened	See 1A	See 1A
2A	[A] + Valve F029 fails open + Valve F030 fails open		Drain RPV water to radwaste 150 A diam. pipe	1. Requires multiple valve failures/openings 2. Indicators in control room will show F029 and F030 open 3. F010 and F011 will isolate on reactor level 3 4. Operator monitors level in control room and takes corrective actions
2B		[A] + Valve F029 inadvertently open + Valve F030 inadvertently open	See 2A	See 2A

Table 19L-8 Potential for Draining RPV Through Residual Heat Removal System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
3A	[A] + Valve F008 fails open		Drain RPV water to suppression pool	1. Valve interlock between F008 + F012 2. Indicators in control room will show F008 open 3. F010 and F011 will isolate on reactor level 3 4. Operator monitors level in control roon and takes corrective action
3B		[A] + Valve F088 inadvertently opened	See 3A	See 3A
4A	[A] + Valve F014 fails open + Valve F015 fails open		Drain RPV water to fuel fool via 300 A diameter pipe	1. Requires multiple valve failures/openings 2. F014 is key locked 3. Indicators in control room show F014 and F015 open 4. F010 and F011 will isolate on reactor level 3 5. Operator monitors level in control room and takes corrective actions
4B		[A] + Valve F014 inadvertently opened + Valve F015 inadvertently opened	See 4A	See 4A

Table 19L-8 Potential for Draining RPV Through Residual Heat Removal System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
5A	[A] + Valve F017 fails open + Valve F018 fails open		Drain RPV water to drywell via spray through 250 A line	1. Requires multiple valve failures/openings 2. F017 and F018 interlocked such that both can be opened simultaneously only if the drywell pressure is high 3. Indicators will show F017 and F018 open 4. F010 and F011 will isolate on reactor level 3 5. Operator monitors level in control room and takes corrective actions
5B		[A] + Valve F017 inadvertently opened + Valve F018 inadvertently opened	See 5A	See 5A
6A	[A] + Valve F019 fails open		Drain RPV water to wetwell spray via 100 A diameter pipe	1. Requires valve failure/opening 2. Indicators in control room will show F017 open 3. F010 and F011 will isolate on reactor level 3 4. Operator monitors level in control room and takes corrective actions
6B		[A] + Valve F019 inadvertently opened	See 6A	See 6A

Table 19L-8 Potential for Draining RPV Through Residual Heat Removal System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
7A	[A] + Valve F016 fails open		Drain RPV water to fuel pool via 300 A diam. pipe	1. F016 is a locked closed manual valve 2. F010 and F011 will isolate on reactor level 3 3. Operator monitors level in control room and takes corrective actions
7B		[A] + Valve F016 inadvertently opened	See 7A	See 7A
8A	[A] + Valve F001 fails open		Drain RPV water to suppression pool via 450 A diameter pipe	1. Valve interlock between valves F001 and F012 2. F010 and F011 will isolate in reactor level 3 3. Operator monitors level in control room and takes correction actions
8B		[A] + Valve F001 inadvertently opened	See 8A	See 8A
9A	Minimum flow valve F021 opens during low flow during shutdown cooling mode		Reactor water is diverted to suppression pool	1. F021 closes on nominal flow signal in the shutdown cooling mode 2. F010 and F011 will isolate the reactor level 3 3. Operator monitors level in control room and takes corrective actions

Table 19L-8 Potential for Draining RPV Through Residual Heat Removal System (Continued)

Path	Equipment Failure	Operator Error	Results	Preventive/Mitigative Measures
9B		Operator inadvertently opens minimum flow valve F021 during shutdown pool cooling mode	See 9A	See 9A

Table 19L-9 Dependency of Core Cooling Systems on Electrical Power

	Power Systems								
System	Offsite Power	Combustion Turbine	DG1	DG2	DG3	Div 1 DC	Div 2 DC	Div 3 DC	Diesel Driven Fire Water Pump
RCIC						XX			
HPCF (B)	OR	OR		OR			XX		
HPCF (C)	OR	OR			OR			XX	
FW (A)	OR	OR							
FW (B)	OR	OR							
FW (C)	OR	OR							
FW (D)	OR	OR							
CRD (A)	OR	OR	OR*	OR*	OR*				
CRD (B)	OR	OR	OR*	OR*	OR*				
LPFL (A)	OR*	OR	OR			XX			
LPFL (B)	OR*	OR		OR			XX		
LPFL (C)	OR*	OR			OR			XX	
Firewater†	OR*	OR	OR*	OR*	OR*				OR
Condensate									
(A)	OR	OR							
(B)	OR	OR							
(C)	OR	OR							
(D)	OR	OR							
Condensate Booster									
(A)	OR	OR							
(B)	OR	OR							
(C)	OR	OR							
(D)	OR	OR							

* Assumes manual feedback capability for combustion turbine distribution system

† AC-independent water addition system

Notes:

DG1 - Diesel generator 1

FW - Feedwater

LPFL - Low pressure core flooder

OR - Redundant supply to other ORs

XX - Loss of this power supply means loss of system

Table 19L-10 Success Criteria for Long-Term Heat Removal for Operating Mode 4

Function	Success Criteria
Containment heat removal during operating Mode 4	RHR-A or B or C* or Normal heat removal using main condenser† or Reactor water cleanup‡ or Overpressure relief rupture disc*f*

* RHR can be operated in either the suppression pool cooling or the shutdown cooling mode. Shutdown cooling requires the reactor to be at low pressure.

† Reactor will have to be pressurized and MSIVs opened for establishing this path.

‡ Reactor may have to be pressurized to use the CUW system efficiently to remove decay heat or reactor water could be drained to the main condenser hotwell through the CUW system and reactor water makeup obtained from HPCF, feedwater, CRD hydraulic system, or the AC independent water addition system.

f Reactor will have to be pressurized and heat transferred to the suppression pool through safety/relief valves. Long-term suppression pool makeup will be required to compensate for water lost through evaporation and reactor water makeup must be obtained from any of the methods indicated in Note ‡ above.

Table 19L-11 Dependency of Heat Removal Systems on Electrical Power

System	Offsite Power	Combustion Turbine	DG1	DG2	DG3	Div 1 DC	Div 2 DC	Div 3 DC
RHR (A)	OR	OR	OR			XX		
RHR (B)	OR	OR		OR			XX	
RHR (C)	OR	OR			OR			XX
CUW (A or B)	OR	OR	OR*	OR*				
Overpressure Relief†								
Main Condenser	XX							

* Assumes feedback capability for combustion turbine distribution system.

† Does not need power source for operation. Also, the function provided by the overpressure relief can be provided by operator opening one of the containment doors.

Notes:

DG1 - Diesel generators

OR - Redundant supply to other ORs

XX - Loss of this power supply means loss of system

Table 19L-12 ABWR Seismic PRA: Highest Class I Accident Frequency Sequences

	Failure Events													
Seq. No.	Structural Integrity	Offsite Power	Onsite Power or Service Water	SRV	Scram	ADS Inhibit	Stuck Open Relief Valve	Flow Control	RCIC	HPCF	ADS	LPFL	Fire Water	RHR
1		X	X		X				X					
2		X	X										X	
3	X													
4		X	X						X				X	
5		X	X		X								X	
6		X	X								X			
7		X	X		X				X					
8		X							X	X		X		
9		X		X	X									
10		X	X						X		X			
11	X													X
12		X	X							X		X	X	X
13		X			X	X	X			X		X		
14		X	X						X				X	X
15		X	X		X			X						X

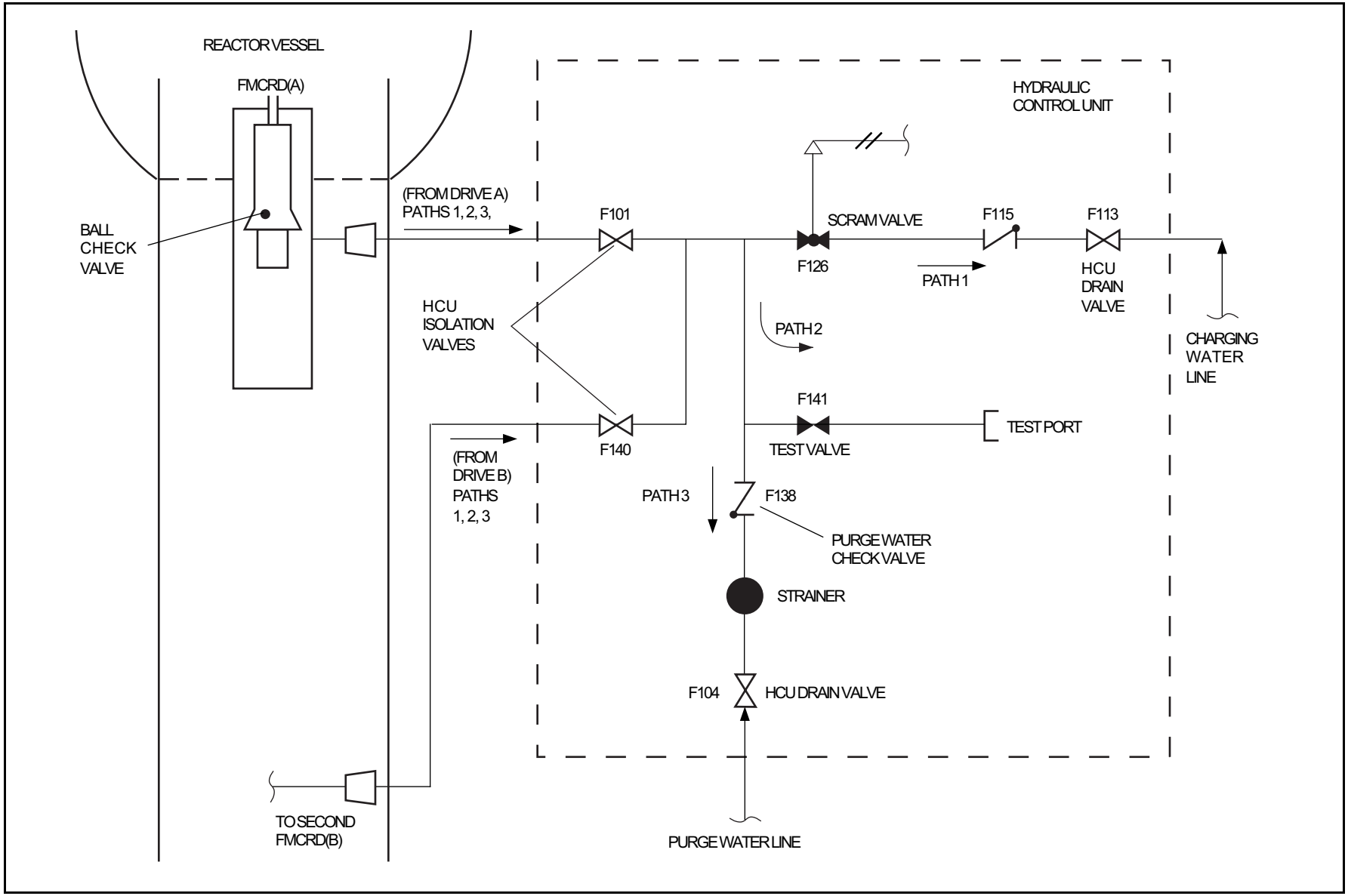

Figure 19L-1 Potential Paths for Draining RPV Through Control Rod Drive Hydraulic System

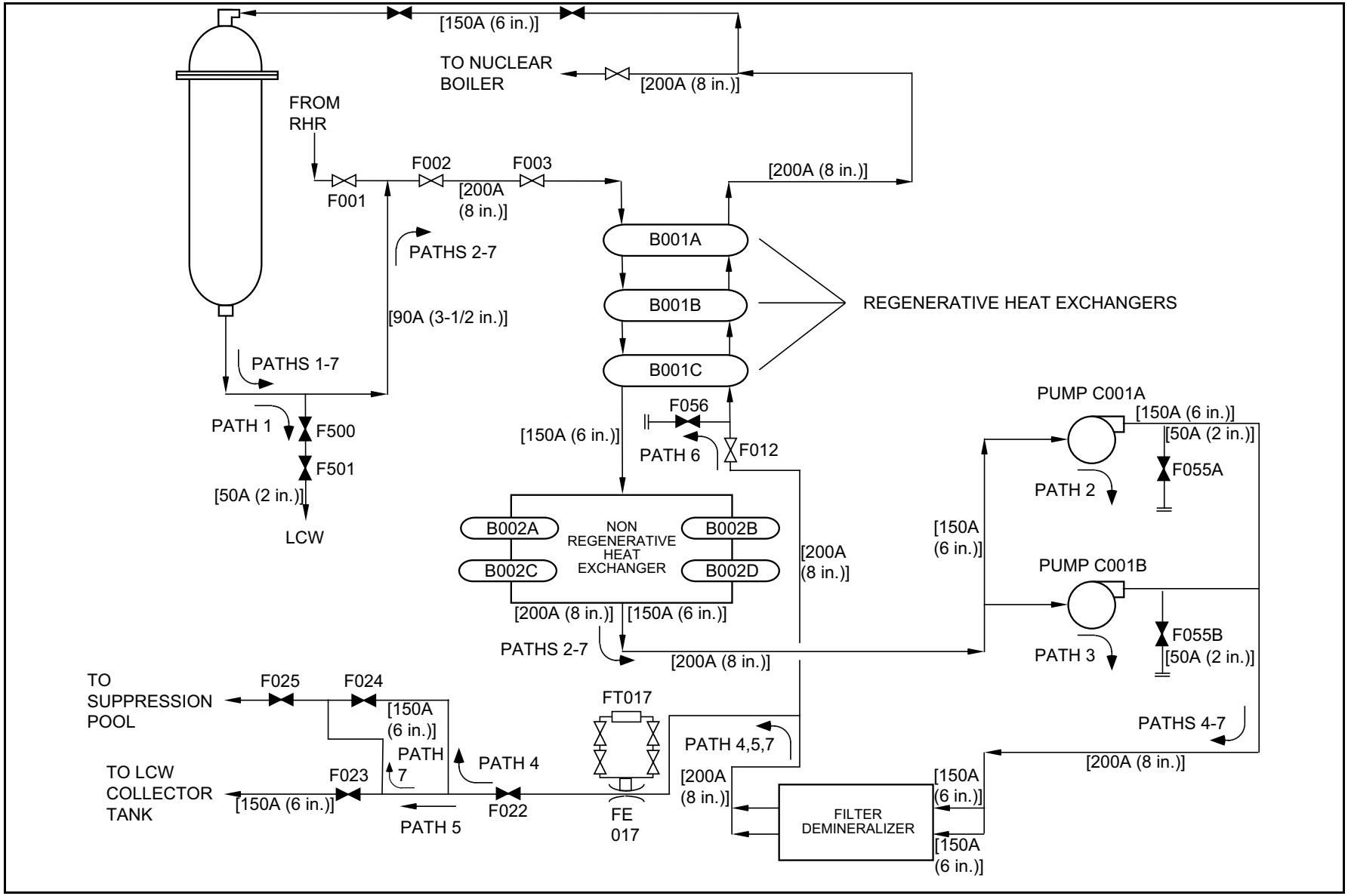

Figure 19L-2 Potential Path for Draining RPV Through Reactor Water Cleanup System

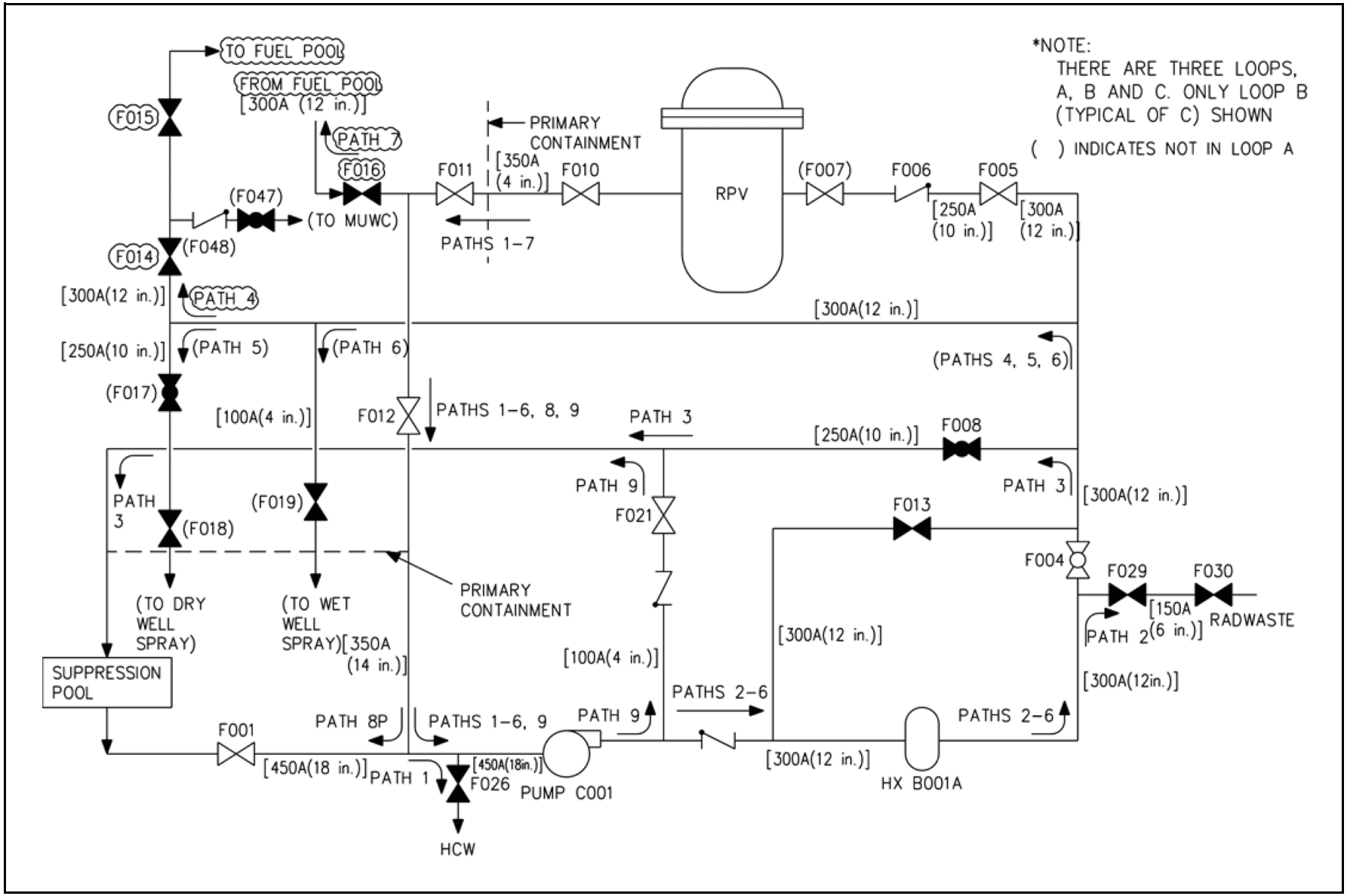

Figure 19L-3 Potential Path for Draining RPV Through Residual Heat Removal System (Pump On)