19Q ABWR Shutdown Risk Assessment

19Q.1 Introduction

Due to events at operating plants in the past several years such as the loss of offsite power at Vogtle on March 20, 1990 and the loss of decay heat removal (DHR) at Diablo Canyon on April 10, 1987, the shutdown risk associated with nuclear power plants has become more of a concern to the industry. On January 17, 1992 the NRC issued Draft NUREG-1449, "NRC Staff Evaluation of Shutdown and Low Power Operation." In NUREG-1449 the NRC staff identified some safety issues that may result in new regulatory requirements.

As part of the certification process for the advanced boiling water reactor (ABWR), an evaluation of the shutdown risk associated with the ABWR was completed. This Appendix discusses the design and procedural features of the ABWR that contribute to the conclusion that the ABWR shutdown risks are negligible.

19Q.2 Evaluation Scope

The ABWR shutdown risk evaluation covers the important aspects of NUREG-1449 as well as specific items requested by the NRC.

The evaluation encompasses plant operation in Modes 3 (hot shutdown), 4 (cold shutdown), and 5 (refueling). The ABWR full power PRA covered operation in Modes 1 (power operation) and 2 (startup/hot standby). This evaluation addresses conditions for which there is fuel in the reactor pressure vessel (RPV). It includes all aspects of the Nuclear Steam Supply System (NSSS), the containment, and all systems that support operation of the NSSS and containment. It does not address events involving fuel handling outside the primary containment or fuel storage in the spent fuel pool.

The evaluation was broken down into several topics covering design, procedures, and ABWR features that have the potential to prevent/mitigate past operating events that are considered precursors to loss of decay heat removal capability and fuel damage. The design issues included: decay heat removal, inventory control, containment integrity, electrical power, reactivity control, and instrumentation. Guidelines for generation of ABWR procedures are covered in a separate section, as well as the risk implications of using freeze seals during ABWR maintenance.

In NUREG-1449 it was pointed out that due to the increased level of maintenance activity while shutdown, the potential for fires and flooding in operating nuclear plants is considered higher during shutdown. These topics are covered separately to highlight the ABWR features designed to minimize the shutdown risks from fires and flooding.

In order to evaluate the ABWR features that are capable of preventing or mitigating safety significant events that have occurred at operating plants in the past, a study was completed of specific past events that resulted either in a loss of offsite power or a challenge to DHR. Loss

of power events as described in NUREG-1410, "Loss of Vital AC Power and the Residual Heat Removal System During Mid-Loop Operation at Vogtle Unit 1 on March 20, 1990," were evaluated and ABWR features which could have prevented/mitigated the event were described. A total of 74 loss of power events were evaluated. In a like manner, events described in NSAC-88, "Residual Heat Removal Experience Review and Safety Analysis–Boiling Water Reactors," were reviewed along with certain loss of DHR events from INPO Significant Evaluation Reports (SERs) and Significant Operating Experience Reports (SOERs) and NRC Information Notices. Over 100 precursor events to loss of DHR were reviewed.

To ensure that new features (i.e., different than current operating BWRs) of the ABWR do not introduce any additional vulnerabilities to operation of the plant, a failure Modes and Effects Analysis (FMEA) was completed on these new features. The FMEA focused on the potential safety impact of identified failure modes and why these do not contribute to increased risk of ABWR shutdown operation.

Lastly, a detailed reliability study was completed of the ABWR DHR function. Probabilistic Risk Assessment (PRA) models including Fault and Event Trees were completed for all DHR and makeup systems. Based on PRA results, minimum sets of systems were identified that, if available, would result in acceptable shutdown risk. Additionally, a realistic core damage frequency assessment was performed to identify any other risk important plant features that may be related to loss of DHR, loss of support systems, loss of offsite power, flow diversions, and LOCA.

Based on this shutdown risk evaluation, input has been provided to other parts of Tier 2. Systems and components important to safety were identified for inclusion in the reliability assurance program. COL action items such as a need for shutdown procedures and important operator actions were specified. Plant features important to risk reduction were identified and made part of Tier 1.

19Q.3 Summary of Results

The ABWR design has been evaluated for risks associated with shutdown conditions (i.e., Modes 3, 4, and 5). The evaluation included the following shutdown risk categories discussed in NUREG-1449:

- Decay heat removal
- Inventory control
- Containment integrity
- Loss of electrical power
- Reactivity control

The evaluation also included shutdown risk reduction features of the ABWR design due to instrumentation, flooding and fire protection, use of freeze seals, and procedure guidelines. ABWR features that are not part of current domestic BWR designs were evaluated to determine if any new shutdown risk vulnerabilities would be introduced. Minimum sets of plant systems that if available would meet a goal of an acceptably low conditional core melt probability were identified. Finally, a realistic core damage frequency assessment was performed for various initiating events to identify any additional risk important features.

The results of this shutdown risk evaluation demonstrate that the ABWR incorporates design features which make the plant risk during shutdown negligible. This conclusion is based on the following principal ABWR features which are capable of mitigating shutdown risks:

Shutdown Risk Concern	Principal ABWR Feature
Decay Heat Removal	Three physically and electrically independent RHR and support systems
Inventory Control	Multiple makeup systems and sources
Loss of Electrical Power	Two offsite and four onsite power sources
Reactivity Control	RPS, ARI, and standby liquid control systems and interlocks to prevent accidental reactivity excursions

The ABWR is adequately protected from internal flooding by floor drains, sump pumps, watertight doors, water level alarms, automatic isolation of flow sources, equipment mounted 20.32 cm (8 inches) off the floor, and the ability to fully contain potential flood sources (where appropriate).

Adequate protection from fire is provided by means of fire barriers and physical separation of the three independent safety divisions. Use of fire detectors, alarms, automatic fire suppression, manual fire water system, and a trained crew of fire fighters keep the risk related to fire at a negligible level.

To assure the flood and fire related risks are kept low during shutdown, the shutdown procedures that the COL applicant is required to develop have been identified.

Based on an FMEA of the new features incorporated into the ABWR that are different from operating domestic BWR plants, it is concluded that none of the new features will introduce additional shutdown vulnerabilities.

Instrumentation was identified that is available during shutdown to adequately monitor the status of the plant and operation of systems which will result in low levels of shutdown risk.

Guidance was presented on how freeze seals could be used during maintenance on unisolatable valves to minimize the risk associated with loss of the freeze seal.

Recommendations on outage planning procedures were presented to ensure that activities scheduled during outages take into account plant status and potentially high risk periods or configurations during shutdown. It was pointed out that the single most important element of reducing shutdown risk is proper outage scheduling of maintenance on systems and support systems capable of removing decay heat or supplying inventory makeup.

An analysis of 70 loss of power and over 100 loss of DHR precursor events at operating BWRs confirmed that the ABWR design features would prevent or mitigate the most safety significant of these events.

The PRA model for analyzing the loss of DHR accident initiation identified about 12 systems that can be used to prevent core damage. The resultant core damage frequency was negligible but the focus of the study was to identify minimum combinations of systems that, if available, would result in a conditional core melt of an acceptably low probability given a loss of RHR event. It was found that generally about four of the 12 systems are sufficient to meet the goal.

In all cases, the minimum type and number of systems required by technical specifications (e.g., RHR) plus systems normally operating during shutdown (e.g., CRD and fire water) are sufficient to maintain adequate shutdown safety margins.

Many such combinations are possible, but certain specific combinations of minimum sets of systems have been identified to provide guidance to the COL applicant. Additional minimum sets of systems can be identified by the COL applicant, if needed, by using the PRA model. These combinations of systems identified will allow COL owners much flexibility in preparing outage plans to ensure that shutdown safety margins are adequate at all times.

In addition to the qualitative assessment of important design features, the importance measures from the CDF analysis were reviewed to identify if there were any important features that were not identified in the qualitative assessment. The CDF during shutdown is very low, and it follows that analysis results did not identify components, that if unavailable, would result in an unacceptable CDF, given the analysis assumptions chosen. Other risk measures, such as Fussell-Vesely, indicated that all individual risk contributors were insignificant under the same analysis assumptions. The results of this analysis are provided in Reference 19Q-1.

19Q.4 Features to Minimize Shutdown Risk

As part of the process for certifying the ABWR design, the NRC requested that General Electric provide a specific discussion of ABWR features that minimize shutdown risk.

The list of ABWR shutdown risk features is presented in Table 19Q-1. The features are grouped by risk categories as discussed in NUREG-1449, “NRC Staff Evaluation of Shutdown and Low Power Operation.” Fire protection was not discussed in NUREG-1449 but was added to the list based on discussions with the NRC. The risk categories are:

- Decay Heat Removal
- Inventory Control
- Containment Integrity
- Electrical Power
- Flooding Control
- Reactivity Control
- Fire Protection

NUREG-1449 also discussed reactor coolant system pressurization but this was not included in the list because it is mainly a PWR issue. BWR shutdown pressure control concerns are ultimately inventory (i.e., LOCA) concerns and are addressed under Inventory Control.

The ABWR has been designed with the minimization of risk being a high priority. PRA methods have been very influential in the design of the ABWR. The ABWR features described in Table 19Q-1 along with appropriate Technical Specifications and utility operating and maintenance procedures (which contain insights gained from risk based evaluations) all result in the conclusion that during shutdown conditions the ABWR is adequately protected against accidents and the estimated core damage frequency is negligible.

The following subsections describe the shutdown risk concern, past experience at operating BWRs for each risk concern, and the ABWR features that contribute towards minimizing shutdown risk for each concern.

19Q.4.1 Decay Heat Removal

Shutdown Risk

Loss of decay heat removal (DHR) while shutdown can lead to fuel uncovery and damage. It can be initiated by loss of the operating RHR System or by loss of an intermediate or ultimate heat sink. If loss of DHR occurs shortly after shutdown, bulk boiling of reactor coolant and fuel uncovery can happen quickly (i.e., less than one half hour for bulk boiling and approximately five hours to core uncovery if no protective action is taken).

Past Experience

There has never been a loss of DHR in a BWR which resulted in actual core uncovery but several precursors to such an event have occurred in the past. Subsection 19Q.11 discusses many of these precursor events and describes ABWR features that could have prevented or mitigated each event.

For BWRs, the most common precursor events involved temporary loss of RHR due to various reasons including inability to open Shutdown Cooling (SDC) valves inside containment and

isolation of SDC due to low water level in the RPV or loss of power to the Reactor Protection System (RPS). In all of these cases, redundant loops of RHR or alternate DHR methods were available.

ABWR Features

The ABWR contains many features to minimize the loss of DHR. The ABWR contains three divisions of RHR and associated support systems that are electrically and physically separated. This is the first line of defense in maintaining DHR. One RHR loop could be in maintenance and if a single failure were to occur to the operating loop, the third loop could be placed into service. It is also possible, if conditions warrant, to run RHR loops in parallel. In this case, failure of one loop would not result in even a temporary loss of DHR.

In the unlikely event that all RHR loops were unavailable, several alternate methods of DHR from the RPV could be used. Steam from the RPV could be directed to the main condenser (if available). Makeup to the RPV could be supplied by many sources as discussed in Subsection 19Q.4.2. Other potential heat sinks include the suppression pool (via the safety relief valves), or under certain conditions the Reactor Water Cleanup System, or the Fuel Pool Cooling and Cleanup System (if the reactor water level is raised to the refueling level). As a final method, if the RPV head was removed, bulk boiling of reactor coolant in the RPV with adequate makeup would prevent fuel damage.

From the above it can be seen that there are multiple methods to maintain DHR in the ABWR such that the shutdown risk associated with loss of DHR is negligible.

19Q.4.2 Inventory Control

Shutdown Risk

Loss of inventory control can lead to uncovering the fuel and damage by overheating. Reduction of reactor coolant inventory is more likely when the plant is shut down because additional paths for diversion of coolant (e.g., RHR System) are operable. In addition, there are shutdown activities such as test and maintenance that require seldom used valve line-ups and plant configurations which increase the probability of operator errors associated with inventory control.

Past Experience

As discussed in Subsection 19Q.11, events at operating plants have resulted in reduction of reactor coolant inventory. For BWRs this typically involved diversion of reactor coolant from the RPV to the suppression pool due to improper valve line-ups (e.g., opening suppression pool suction valve before SDC suction was fully closed) or valve leakage (e.g., RHR pump mini-recirculation valve). Other inventory losses were due to leaking RHR heat exchanger tubes, placing a partially drained RHR loop online following maintenance, and buckling of an RHR heat exchanger due to marine growth. In all cases, the loss of inventory was either recovered due to operator action or automatically stopped by isolation of SDC on low RPV level.

ABWR Features

The ABWR contains several design features to minimize the potential for inventory loss. Indication of RPV level is displayed to the operator in the control room continuously during all modes of plant operation (including refueling). To ensure that an adequate level is maintained in the RPV, multiple sources of makeup exist including:

- Suppression pool
- Condensate storage tank
- Main condenser hotwell
- AC-independent Water Addition System

To minimize the potential for pipe breaks, RHR system valves are interlocked with reactor system pressure to ensure that low pressure RHR piping is not exposed to full system pressure. In the event that the interlocks fail or are bypassed, the RHR piping is capable of withstanding full reactor pressure without rupture.

During shutdown there are many maintenance tasks and evolutions that could lead to potential draining of the RPV. These include: CRD and Reactor Internal Pump (RIP) removal and replacement, and failures or operator errors associated with operation of the Reactor Water Cleanup System and the RHR System. These potential drainage paths are discussed below.

CRD Replacement

CRD replacement for the ABWR will use the same procedure followed for current operating BWRs. The CRD is withdrawn to the point where the CRD blade back seats onto the CRD guide tube. This provides a metal to metal seal that prevents RPV drainage when the CRD is removed. The many years of BWR experience with CRD removal gives a high degree of assurance that the risk from this operation will be negligible for the ABWR.

See Subsections 4.6.1.2.1 and 4.6.2.3.4 for additional information on CRD replacement and maintenance.

RIP Motor and Impeller Replacement

Nuclear plants with RIPs have been in operation for over 15 years. Over 500 RIPs and motors have been successfully removed and reinstalled in European BWR plants. This has demonstrated that replacement activities can be carried out without draining the vessel.

Replacement of RIP motor and impeller involves the following steps. The RIP lower bolts are loosened and the pump allowed to move downward approximately 6.25 mm (1/4-inch) to the point where the impeller becomes backseated. An integral inflatable seal is then actuated as a backup sealing device to assure no RPV leakage occurs. The RIP motor can then be removed. Following motor removal, a temporary cover plate is bolted to the bottom. The impeller is then removed from the top. The bolted cover plate prevents leakage of coolant from the RPV. After

the impeller is removed, a plug is installed on the RPV bottom head at the impeller nozzle to provide additional protection against draining the RPV.

During maintenance activities on the RIP, there are two periods when the potential for leakage is greatest: when removing the motor and when completing maintenance on the secondary seals. In both these cases, the temporary bottom cover plate is removed. During motor removal, the primary and secondary seals prevent leakage but they could fail. In this case, only small leakage could occur because of the tight clearances between the RIP housing and the impeller shaft. If the seals were to leak, the bottom cover could be bolted in place to prevent further leakage. Maintenance on the secondary seals requires removal of the motor, impeller and shaft, and the temporary bottom cover. A temporary plug is installed in the RIP diffuser before removing the bottom cover plate. This temporary RIP diffuser plug is designed so that it can not be removed unless the RIP motor housing bottom cover is in place. Due to the multiple operator errors required to cause a major leak during RIP maintenance, the risk from RIP maintenance is considered negligible.

See Subsection 5.4.1.5 for additional information on RIP motor and impeller maintenance.

Control Rod Drive Hydraulic System

During operating Modes 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 head of water in the RPV; hence, draining the RPV is unlikely. In the event that neither pump is in operation, there are several potential paths for draining the RPV through the CRDHS.

With neither CRD pump operating, the scram valves will open due to low Hydraulic Control Unit (HCU) charging header pressure. The scram valves may remain open due to operator error in not resetting the RPS logic or other system failures such as loss of instrument air to the scram valve. This combined with multiple mechanical failures to check valves and operator errors in CRD hydraulic system valve lineups could result in RPV drainage through the CRD hydraulic system. Multiple failures are required for RPV leakage to occur and even if a leak were to develop, only two CRDs would be affected and the leak would be small since it would occur in a 32A (1-1/4-inch) line. Therefore, the probability of draining the RPV through the CRD hydraulic system is considered negligible.

Reactor Water Cleanup System (CUW)

During shutdown, the CUW provides continuous cleaning of the reactor coolant. Water is removed from the RPV through the RHR shutdown cooling suction nozzle and a line attached to the RPV bottom head and after passing through a series of heat exchangers and a filter demineralizer is returned to the RPV either via an attachment to the upper head or through the feedwater lines and spargers.

Potential drainage paths exist due to several maintenance flush and drain valves and CUW discharge paths to the low conductivity water (LCW) sump and the main condenser. The latter

two paths are used during reactor startup to control excess reactor water due to heat up and thermal expansion.

For any of the potential flow paths described above to result in RPV drainage, multiple failures of equipment and operator errors must occur. In addition, if the RPV were to start draining all but one of the potential flow paths (LCW sump) would be automatically isolated on low RPV level. The flow path to the LCW sump is controlled by two valves in series one of which is locked closed and both are under administrative control. If drainage were to occur, LCW sump well level alarms would annunciate in the control room. Also, the line is only 50A (2 inches) in diameter and so the flow rate would be slow enough to allow ample operator time to mitigate the leak.

Because of the multiple failures and operator errors that must occur to cause RPV drainage through the CUW and the automatic RPV isolation logic to stop most potential flow paths, the risk of RPV drainage though the CUW is considered negligible. Quantitative evaluations have also concluded negligible risk due to low event frequency and diverse and redundant mitigation pathways.

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 reactor pressure vessel (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. Protective interlocks are provided to prevent the most likely interactions of mode combinations.

The operator has five mode selection switches available that will automatically perform the required valve alignment for the mode selected. This feature reduces the chance of operator error by only requiring one action, selection of the mode switch, to realign several valves. Only one mode at a time can be operational, thus precluding potential undesirable multiple mode interactions. The five modes are:

(1) RHR initiation

(2) RHR suppression pool cooling

(3) RHR shutdown cooling

(4) RHR standby

(5) RHR drywell spray

There are two basic ways that the ABWR RPV water level can potentially be decreased through the RHR System during shutdown cooling. The first way is through operator error in opening manual isolation valves that are used for RHR System maintenance. These paths are to the High Conductivity Water sump and the Liquid Radwaste Flush System. These valves are normally closed during the shutdown cooling mode of plant operation. These are 50A (2-inch) and 150A (6-inch) lines respectively. Inadvertent opening of these valves would result in a relatively slow RPV level decrease which would be alarmed to the operator in the control room such that there would be adequate time to respond. If the operator failed to notice the decreased RPV level, an alarm would annunciate in the control room and the RPV isolation valves would automatically close on low RPV level. The fuel would remain covered with water and no fuel damage would occur.

The second way that RPV level could decrease would be for one of the motor operated valves (MOVs) in the RHR System to open inadvertently or by operator error. Most of the MOVs in the RHR System are interlocked to prevent inadvertent diversion of RPV water (e.g., the shutdown cooling (SDC) suction line is interlocked so that the suppression pool suction and return valves and wetwell spray valve must be closed before the SDC valve can be opened, the shutdown cooling suction valve must be fully closed before the suppression pool suction or return valve can be opened, the two series dry well spray valves cannot be opened at the same time unless the drywell pressure is high). Thus loss of RPV level through these paths is not likely. Loss of RPV level through the wetwell spray valve requires a mechanical failure or an operator error to open the valve when not required. The only other potential path is via the RHR pump mini-flow valve. This valve is designed to open to allow water flow back to the suppression pool if the RHR pump is running at shutoff head. This is a pump protection feature. The valve opens and closes automatically depending on measured RHR flow.

Whether the potential flow path is caused by mechanical failure or operator error, two features exist to mitigate the loss of RPV level. On a low RPV level signal, both RPV isolation valves close to stop all flow out of the RPV. The RPV low level setpoint is 3.81 meters above the top of the fuel. Even if the low RPV level isolation feature were to fail (after a previous valve mechanical failure or operator error), flow out of the RPV would automatically stop when the RHR shutdown cooling nozzle is uncovered. At this point, 1.7 meters of water would still be above the top of the active fuel. Therefore, the draining of the RPV via the RHR System to the point of uncovering the fuel and causing fuel damage is not considered credible for the ABWR. Quantitative evaluations have also concluded negligible risk due to low event frequency and diverse and redundant mitigation pathways.

Another potential for loss of inventory control is through the use of freeze seals on piping attached to the RPV. Subsection 19Q.8 discusses how freeze seals will be used on the ABWR and why the risks associated with freeze seals will be small.

In summary, the ABWR contains many redundant and diverse features such that, along with the use of experience proven administrative controls, loss of inventory control is not a significant safety concern.

19Q.4.3 Containment Integrity

Shutdown Risk

A breach of containment integrity is not by itself an issue of high safety significance but, in conjunction with other initiating events, could increase the severity of the initiating event. A breach of containment integrity followed by breach of another radiological barrier or boiling of the reactor coolant could lead to a direct release to the atmosphere. Attachment 19QB discusses potential offsite releases following boiling in the RPV with the head removed and shows that releases would be a small fraction of normal operating limits. In addition, the PRA results in Subsection 19Q.7 indicate that the risk of RPV boiling is low.

During refueling of the BWR, the primary containment is open and cannot be readily closed since the drywell head is removed. Nonetheless, loss of containment integrity has not been an issue for BWRs in the past.

The probability of core melt during shutdown is low, but if a core melt were to occur when the primary containment was open, the suppression pool may be bypassed resulting in high offsite doses.

ABWR Features

During shutdown with the drywell head removed, the ABWR has the secondary containment which can be automatically isolated on high radiation from a radiological boundary breach or fuel handling accident.

The Standby Gas Treatment System (SGTS) filters air from the secondary containment to reduce potential contamination to the atmosphere.

The ABWR secondary containment and use of the SGTS results in a negligible risk concern for loss of containment integrity.

19Q.4.4 Electrical Power

Shutdown Risk

A loss of all offsite power challenges the onsite sources to power safety-related equipment to maintain safe shutdown. Loss of individual buses (AC or DC) affects divisional train capability and results in loss of redundancy to complete required safety functions.

Past Experience

As discussed in Subsection 19Q.11, loss of power events have occurred at many nuclear power plants. There have been several cases of a total loss of offsite power which, in some instances,

led to loss of shutdown cooling and increases in coolant temperatures of as much as 333 K (140°F).

The majority of total loss of offsite power events were due either to severe weather or operator errors. Several losses of onsite power events were due to objects falling on transformers while operators were performing maintenance activities in the switchyard. In other cases, switching errors resulted in temporary loss of power to vital buses or offsite power.

ABWR Features

The ABWR electrical system has the following features to prevent or mitigate potential loss of power events:

- Three physically and electrically independent Class 1E emergency diesel generators
- Two independent sources of offsite power
- Three unit auxiliary transformers powering three Class 1E and non-1E power buses
- Combustion turbine generator (CTG) that can be used to power any of the Class 1E or non-1E buses

The ABWR electrical power system contains redundancy and diversity of electric power sources. This allows sources to be in maintenance during shutdown and still have adequate power sources to meet potential equipment failures. Even in the case of a loss of offsite power, the CTG has the ability to start a feedwater or other pump for DHR or inventory makeup if required. This means that the ABWR can use alternate sources of DHR with only onsite power sources.

In the event that one phase of the main transformer were to fail, an installed spare is available to return the preferred source of offsite power to service without the need to procure and deliver a new transformer.

As discussed more fully in Subsection 19Q.11, the ABWR electrical power distribution system has features that are capable of mitigating potential loss of power events that have occurred at operating plants in the past. The design features described above in conjunction with appropriate Technical Specifications and other administrative controls result in an electrical distribution system that is able to maintain an adequate level of redundancy and capacity even with equipment out for maintenance or testing. This ensures that safety margins can be maintained at all times during shutdown and normal plant operation.

19Q.4.5 Reactivity Control

Shutdown Risk

Reactivity control during shutdown may be a concern because local criticality can be achieved through movement of control rods or errors in fuel handling that may not be adequately detected

by installed neutron detectors. Also at lower temperatures, the inherent negative reactivity feedback available at normal operating temperature and pressure is less able to mitigate potential power excursions.

While overall core shutdown margins are adequate to protect the fuel as long as procedures are followed, inadvertent withdrawal of two adjacent CRDs or fuel handling errors can lead to fuel damage.

Past Experience

A few isolated cases of BWR shutdown reactivity control concerns have been identified in the past and were attributed to operator errors (e.g., withdrawing the wrong control rod).

Reactivity excursion events could occur due to any one of the following:

- Control Rod Drop
- Control Rod Ejection
- Refueling Error
- Rod Withdrawal Error
- Fuel Loading Error

Control Rod Drop

While shutdown, the only time a control rod drop could occur is during control rod testing. If two control rods associated with one Hydraulic Control Unit (HCU) are fully withdrawn, a rod block signal prevents withdrawal of a third control rod. If the rod block signal were to fail and the operator were to incorrectly select an adjacent control rod for withdrawal, a latch mechanism exists such that if the rod were to become stuck and decouple from its drive it could only drop a maximum of 20.32 cm(8 inches). In addition, a Class 1E separation detection system would sense a separated control rod drive and initiate a rod block signal.

Due to the combination of events required to cause a control rod drop including operator error coincident with multiple mechanical failures, the ABWR rod drop accident risk is considered negligible.

Control Rod Ejection

For a control rod ejection accident to occur while shutdown, RPV pressure would have to be increased (e.g., during a hydrostatic test). The series of events that would have to occur are:

(1) During RPV hydrostatic testing one or two control rods associated with an HCU are withdrawn for testing and,

(2) A break occurs:

(a) In the CRD housing of an adjacent rod which also results in failure of the internal control rod anti-ejection supports ("shootout restraints")

or

(b) In the CRD insert pipes coupled with failure of both its ball check valve and electro-mechanical brake.

Due to the short amount of time that the RPV undergoes hydrostatic testing and the multiple failures required for a control rod ejection to occur, the risk from this event is considered negligible.

Refueling Error

During refueling, inserting a fuel bundle into a fueled region of the core which has a withdrawn control rod blade could result in a reactivity accident.

The ABWR features that prevent or mitigate refueling errors are:

(1) An interlock with the mode switch in the REFUEL position which prevents hoisting another fuel assembly over the vessel if a control blade has been removed.

(2) While shutdown, only two control rods can be withdrawn at a time. Any attempt to withdraw a third control rod would result in a rod block signal being initiated by the rod control and instrumentation system. During refueling, technical specifications allow only one rod to be withdrawn at a time.

(3) The operator would be alerted to a refueling error by the source range neutron monitoring system.

Due to the combination of operator errors, interlock failures, and core configuration required for this event to occur, refueling accident risks are considered negligible.

Rod Withdrawal Error

If two adjacent control rods are withdrawn at the same time, the reactor may become critical. To prevent this, the ABWR has an interlock which prevents adjacent control rods being withdrawn at the same time. Two control rods associated with an HCU can be withdrawn at the same time but these rods are separated by at least two cells. An interlock prevents withdrawal of a third rod. If the interlock fails and the rod is withdrawn, the rods would scram on a high flux signal.

The coincident failures of the rod withdrawal interlock and Reactor Protection System in conjunction with operator error, which are required to cause a rod withdrawal error are considered improbable and the risk negligible.

Fuel Loading Error

This event is similar to a refueling error. In this case the refueling procedure is not followed and a higher than design core reactivity configuration is formed. If not identified by the core verification process, subsequent control rod testing may result in inadvertent criticality and power excursion. A high flux scram would terminate the excursion.

The risk from a fuel loading error is considered negligible because of the combination of events required for the accident to occur.

Summary of Reactivity Control

The ABWR refueling interlocks, control rod design, Reactor Protection System operability during shutdown, and strict administrative controls all combine to support the conclusion that shutdown Reactivity Control is a negligible risk concern for the ABWR design.

19Q.4.6 Summary of Shutdown Risk Category Analysis

The ABWR design was evaluated against shutdown risk categories from NUREG-1449. The analysis took into account past experience at operating BWRs. The conclusion from this analysis is that the ABWR design contains multiple features to minimize potential risk during shutdown for the major shutdown risk categories.

19Q.5 Instrumentation

The ABWR instrumentation system contains many features that help reduce shutdown risk. These features are contained in the basic design of the instrument systems and in the type and number of parameters monitored.

During shutdown, the main concern from a risk perspective is removal of decay heat from the fuel in the RPV. The large volume of water in the spent fuel pool and low probability of draining makes the risk associated with fuel pool operation relatively low. The smaller reactor pressure vessel (RPV) volume and relatively high decay heat load of the fuel increases the cooling requirements and decreases the available time to recover from loss of decay heat removal (DHR). Thus, to minimize shutdown risk, the instrumentation system must monitor RPV level and water temperature, status of makeup sources and heat sinks, and display these to the plant operators in a reliable and easy to understand manner.

Design Features

The ABWR utilizes redundant channels of safety-related instruments for initiating safety actions and monitoring plant status. This is accomplished by a four division correlated and separated protection logic complex called the safety system logic and control (SSLC). The SSLC receives signals from the redundant channels of instrumentation, displays information to the operator, and makes decisions on safety actions.

The safety system setpoints are determined by analysis and experience, factoring in instrument errors, drift, repeatability, safety margins, and the need to minimize spurious actuations. The

system provides continuous automatic online testing of the logic and offline semi-automatic end-to-end (sensor input to trip actuator) testing. This combination meets all current regulatory requirements.

Specific instrumentation features important to shutdown operations include:

- Automatic initiation of ECCS to ensure adequate RPV makeup.
- Four channels of instrumentation to allow for bypass during maintenance and testing while still retaining redundancy. (The two-out-of-four logic reverts to two-out-of-three during maintenance bypass).
- Continuous monitoring for detection of fires or flooding in safety-related and other areas.
- Operability of the Reactor Protection System (RPS) during shutdown to mitigate potential reactivity excursions.
- Interlocked refueling bridge operation to prevent reactivity excursion.
- Automatic isolation of shutdown cooling (SDC) on low level in the reactor pressure vessel (RPV) to ensure against fuel uncovery.
- Interlocked residual heat removal (RHR) valves (SDC and suppression pool) to reduce the potential for diversion of coolant from the RPV to the suppression pool.
- Ability to control shutdown plant status from the remote shutdown panel in the event that the control room becomes uninhabitable.
- Ability to monitor radiation levels throughout the plant to detect breaches in radiological barriers.

Parameters Monitored

The key shutdown parameters monitored by the ABWR instrumentation system include:

- RPV level, water temperature, and pressure
- Neutron flux
- Drywell and wetwell pressure and temperature
- Suppression pool temperature and level
- Reactor, turbine and control building flooding level
- RHR flow rate, temperature, pump motor trip, and loop logic power failure
- CUW outlet temperature

- Fire detection in various buildings
- Electric power distribution system parameters (e.g., power, voltage, current, frequency)
- Operation of fire water system

19Q.6 Flooding and Fire Protection

The ABWR has been designed to minimize the risks associated with fires and flooding through the basic layout of the plant and the choice of systems to enhance the plants tolerance to fires and flooding.

Plant Layout

The plant layout is such that points of possible common cause failure between safety-related and non-safety-related systems have been minimized. As an example, the control room is situated between the reactor building and the turbine building. Thus safety-related equipment and controls that are used to shutdown and maintain long term cold shutdown of the plant cannot be impacted by failures of non-safety-related systems in the turbine building. Likewise, non-safety-related systems/equipment in the turbine building that could be used to reach and maintain cold shutdown (e.g., condensate, main condenser) are not affected by failures of safety-related equipment, therefore, interactions between reactor and turbine building systems are minimized.

Normal and alternate preferred power is supplied through the turbine building to the reactor building for safety-related loads. These non-safety-related power sources are backed-up by safety-related diesel generators located in the reactor building. The diesel generators are thus not affected by events in the turbine building.

The buildings are laid out internally so that fire areas of the same division are grouped together in block form as much as possible. This grouping is coordinated from building to building so that the divisional fire areas lineup adjacent to each other at the interface between the reactor and control building. An arrangement of this fashion naturally groups piping, HVAC ducts, and cable trays together in divisional arrangements and does not require routing of services of one division across space allotted to another division.

A major difference between the ABWR and current reactor designs is that due to the data communication functions of plant systems, there is no need for a cable spreading room. This removes a significant source of potential fires that could lead to core damage both during normal plant operation and shutdown conditions.

Systems

The ABWR has three independent safety-related divisions, any one of which is capable of maintaining the reactor in a safe cold shutdown condition. With this arrangement, a single division may be out for maintenance and a single random failure could occur which disabled another division, but the third division could be available to ensure continued DHR. In addition,

there are non-safety-related systems such as condensate that can be used to maintain cold shutdown.

In general, systems are located and grouped together by safety division so that; with the exceptions of the primary containment, the control room, and the remote shutdown room (when operating from the remote shutdown panels); there is only one division of safe shutdown equipment in a fire area. Complete burnout of any fire area without recovery will not prevent continued decay heat removal (DHR), therefore, complete burnout of a fire area is acceptable from a public risk perspective.

The separation exception in the primary containment is made because it is not practical to divide the primary containment into three fire areas. The design is deemed acceptable because:

(1) Sprinkler coverage is provided by the containment spray system.

(2) Only check valves and ADS/SRV valves (if the RPV head is on) are required to operate within containment to provide DHR. A fire could not prevent the operation of a check valve nor would it prevent a safety valve from being lifted on its spring by pressure. The high pressure pumps are capable of providing water to the core up to the set point of the SRVs. Thus, a fire could not prevent injection of water to and relief of steam from the reactor vessel.

(3) In addition, maximum separation is maintained between the divisional equipment within primary containment.

All divisions are present in the control room and this cannot be avoided. The remote shutdown panel provides redundant control of the DHR and ECCS functions from outside of the control room. The controls on the remote shutdown panel are hard wired to the field devices and power supplies. The signals between the remote shutdown panel and the control room are communicated over fiber optic cables so that there are no power supply interactions between the control room and the remote shutdown panel.

There are some areas where there is equipment from more than one safety division in a fire area. Each of these cases is examined on an individual basis to determine that the encroachment is required and that failure in the worst conceivable fashion is acceptable. These are documented in Subsection 9A.5.5 under “Special Cases—Fire Separation for Divisional Electrical Systems.”

Divisions I and II 125 VDC and 120 VAC power supplies, reactor building cooling water pumps and heat exchangers, emergency chillers and emergency HVAC Systems are located in the control building. Since these systems are required for DHR if the function of the control room is lost, they are separated from the control room complex and its HVAC System by rated fire barriers. A fire resulting in the loss of function of the control room will not affect the operation of the remote shutdown or remote shutdown support systems.

When the plant is shutdown and, if due to normal maintenance or other work, fire barriers must be breached between two safety divisions, the third division must be operable and its barriers checked to ensure they are intact.

Fire Containment

The fire containment system is a combination of structures and barriers that work together to confine the direct effects of a fire to the fire area in which the fire originates. The fire containment system is comprised of the following elements:

(1) Concrete fire barrier floors, ceilings and walls which must be at least 15.24 cm (6 inches) thick if made from carbonate and silicious aggregates. Other aggregates and thicknesses are acceptable if the type of construction has been tested and bears a UL (or equal) label for a three hour rating.

(2) Fire doors, which are required to have a UL (or equal) label certifying that they have been tested for a three hour rating per ASTM E119, including a hose stream test.

(3) Electrical penetrations which are required to have been type tested to ASTM E119, including a hose stream test.

(4) Piping penetrations which are required to have been type tested to ASTM E119, including a hose stream test.

(5) Fire dampers for any HVAC duct penetrating a fire barrier and which must have a rating of three hours. The only fire dampers separating divisions are in the HVAC duct for secondary containment (six total). The plant arrangement minimizes fire dampers.

(6) Fire rated columns and support beams, which are required to be of reinforced concrete construction or, if of steel construction, enclosed or coated to provide a three hour rating.

(7) Backup of the fire barrier penetration seals by the HVAC Systems operating in the smoke removal mode. This backup feature is accomplished in the reactor and control buildings by maintaining a positive static pressure for the redundant divisional fire areas with respect to the fire area with the fire. Leakage is into the fire impacted area under sufficient static pressure to confine smoke and heat to the fire area experiencing the fire, even if there is a major mechanical failure of the penetration seal.

Other aspects of the ABWR design that minimize the risk due to fires while shutdown are:

- HVAC Systems dedicated to the divisional areas which they serve.

- A smoke control system to remove smoke and heat from the affected area, to control the pressure in a room due to a fire, assure that any fire barrier leakage is into the fire area experiencing the fire, and supply a clean air path for fire suppression personnel. The HVAC System has been designed for the dual purposes of HVAC and smoke control.
- Fire alarm systems.
- Fire suppression system to automatically initiate, where appropriate, and extinguish fires.
- Manual fire suppression equipment such as hand held CO_2 or chemical fire extinguishers, and water hoses.
- Administrative controls to ensure that at least one safety division is available with intact barriers at all times.

Fires During Maintenance

When the plant is shutdown, maintenance activities may require breaching the fire barriers for one or more activities. The recommended outage philosophy regarding fire barrier integrity is that through administrative controls, one division of safety equipment will be available (i.e., not in maintenance) and its physical barriers will be intact. This division will be in standby and one other division will be operating to remove decay heat and complete other required functions (e.g., fuel pool cooling, CRD purging, reactor water cleanup). The third division could then be fully in maintenance. In this configuration, a fire in any one division would not result in loss of decay heat removal capability. If the fire were to occur in the intact division, the fire barriers would restrict the fire to that division only and the operating division could continue to remove decay heat. For fires in either of the other two divisions, even if the barriers between the two divisions were breached, the intact division would be available to remove decay heat. See Subsection 19.9.24 for COL license information requirements.

As discussed more fully in 19Q.7, the COL applicant must identify a minimum set of systems that will not be in maintenance such that the conditional probability of core damage due to certain initiating events is maintained acceptably low. The minimum set selected should take into account fires in various locations of the plant. If the above outage philosophy is followed, the risk from fires during shutdown conditions will be low.

Flooding

Many of the features that are designed to mitigate fires also serve to protect the plant from damage due to flooding. Physical separation of safety divisions not only prevents propagation of fires but also restricts or prevents flooding of safety-related equipment. The fire barriers will also prevent water due to flooding from non-divisional sources from entering a divisional area and contain water in the fire area from divisional water sources.

Other aspects of the ABWR design that minimize the risk from flooding are the practice of not routing unlimited sources of water (e.g., service water) through ECCS room areas and ensuring

that other large water sources (e.g., suppression pool) can be contained without damaging equipment in more than one safety division if a flood were to occur.

A review has been completed of all ABWR internal flood sources and the results show that during shutdown conditions at least one safety division would be unaffected by water damage for any postulated flood. Features, beside separation, that contribute to this low level of risk are: Adequately sized room floor drains, water level alarms and automatic isolation of flood sources for potentially affected rooms, mounting motors and other electrical equipment at least 20.32 cm above floor level, and using watertight doors. As was discussed under fire protection, administrative controls will be implemented to assure that at least one safety division with intact barriers is available at all times during plant shutdown. In the ECCS rooms, the seals on the doors seat with water pressure from floods outside the room, which act to minimize leakage past the seals. With the watertight doors dogged closed, only a small leakage past the seals is expected from flooding in the room. Therefore, during shutdown if maintenance tasks require breaching the barriers of two divisions, flooding in the intact division will not cause damage to equipment in all three divisions. For Reactor Service Water (RSW) pump house floods, the watertight doors for the pump rooms and electrical equipment rooms are capable of withstanding floods from either direction. Additional details on the ABWR flood mitigation capability is contained in Appendix 19R.

Summary of Fire and Flood Features

The ABWR has been designed to minimize the risk due to fires or flooding during shutdown conditions by plant configuration and system design. Divisional separation, both physically and electrically, as well as fire/flooding mitigation systems exist to reduce plant risks from these potential accidents. Along with these design features, administrative controls are implemented to ensure that at least one safety division is not in maintenance and its physical barriers are intact.

19Q.7 Decay Heat Removal Reliability Study

19Q.7.1 Introduction

As part of the ABWR shutdown risk evaluation, a reliability assessment of the decay heat removal (DHR) capability was completed. Decay heat removal reliability has received increasing attention due to events such as those at Vogtle and Diablo Canyon where decay heat removal systems were made inoperable due to loss of electric power and other causes.

Attachment 19QC summarizes approximately 200 events at operating plants which were either loss of decay heat removal events or precursors to such events. The relatively large number of events underscores the potential for loss of decay heat removal events and the potential for associated core damage.

19Q.7.2 Purpose

The purpose of this study is to determine the minimum number of systems that might be available during shutdown to ensure that the risks associated with loss of decay heat removal events are acceptable. That is, given a loss of the operating RHR System for any reason, the subsequent conditional probability of core damage remains acceptably low using only those systems that are potentially available (i.e., system not in maintenance but which could experience random failures).

The results of this study provide guidance regarding various combinations of systems, that if kept available during a plant outage, will ensure that the risk associated with loss of DHR Systems will be acceptable. A utility may choose to keep more systems available but as long as a minimum set is made available, shutdown risk will be considered acceptable. This minimum set of systems will give a utility flexibility in scheduling maintenance activities for DHR Systems. The minimum sets described in this study are representative of acceptable combinations. There may be additional sets of equipment that were not included in this study which would also result in acceptable risk levels.

The minimum sets of systems take into account plant conditions (i.e., modes) and the fuel decay heat generation rate as a function of time. Both safety and non-safety (e.g., power conversion) systems are included in the minimum sets.

In addition to the minimum sets analysis, several probabilistic analyses were performed to analyze CDF for loss of decay heat removal initiators and for loss of inventory control initiators, such as LOCA and RPV drainage events from flow diversions.

19Q.7.3 Summary

Using probabilistic risk assessment (PRA) techniques, an acceptable level of shutdown risk was demonstrated for various minimum sets of equipment and systems that were assumed to be available (i.e., not in maintenance).

These minimum sets were determined for an initiating event involving loss of an operating RHR System. The three primary causes of a loss of the RHR System were identified to be the following:

(1) Mechanical or electrical failures in the operating RHR System

(2) Loss of the operating service water pump associated with the operating RHR System

(3) Loss of offsite power

Loss of operating service water pump and offsite power were evaluated separately as the cause for loss of the operating RHR because of their impact on other DHR Systems. Each potential cause for loss of the RHR System was considered an initiating event.

Success criteria were determined for each initiating event, taking into account decay heat load and plant operating mode. Minimum complements of systems that will prevent core damage given the initiating event and the time dependent core decay heat generation rate were then identified.

Event trees were developed based on the assumed initiating event and applicable success criteria. Accident sequence logic was developed for each event tree core damage endstate. A linked fault tree approach was used to develop branch event system fault trees. System failure probabilities were determined with the help of fault tree analysis.

The results from the study are summarized in Tables 19Q-3, 19Q-4, and 19Q-5. The tables show that significant flexibility exists for completion of system maintenance during outages while still maintaining adequate safety margins. These minimum sets of systems can be used by utilities for initial outage planning and for evaluating changes to outage schedules to ensure adequate safety margins are maintained at all times during the outage. The risk goal can, in general, be met by just those systems required to be operable (and therefore available) by the ABWR Technical Specifications plus normally operating systems (e.g., CRD, fire water, CUW, FPC).

19Q.7.4 Methodology

The methodology used in this study was the same utilized in full power PRAs (i.e., event trees and fault trees). The plant is assumed to be shutdown with decay heat being removed by the RHR System in the shutdown cooling (SDC) mode. For the conditional probability of core damage analysis, loss of the operating RHR System is then assumed. The loss could occur due to mechanical or electrical component failures of the RHR System, loss of service (i.e., cooling) water pump in the same division as the operating RHR System, or loss of offsite electrical power. The three types of failures are assumed to be initiating events. For the CDF analysis, detailed initiating event models were used for RHR and its support systems to calculate the frequency of loss of the operating shutdown cooling loop.

For each initiating event, the success criteria were determined. The success criteria are the minimum complement of systems that are capable of preventing core damage. As the decay heat load is dependent on the time following shutdown, the minimum systems required to remove the decay heat will also be time dependent. Therefore, the success criteria have been determined as a function of time. Subsection 19Q.7.6 discusses the success criteria in more detail.

With the help of the success criteria, event trees for each initiating event were developed for each period. Subsection 19Q.7.7 discusses the event trees.

The branch points on the event trees model the probability of success and failure for each system included in the success criteria. The failure probability for each system was evaluated by a fault tree analysis. The fault trees model potential system failures due to mechanical failure

of components, loss of electric power to pumps or valves, or operator errors associated with manual actions (e.g., valve line ups or remote control of pumps and valves). Unavailability due to maintenance was modeled as follows. For a system included in a minimum set, the maintenance unavailability was taken to be 0 (i.e., the system is assumed to not be in maintenance). For a system not in a minimum set, the maintenance unavailability was taken to be 1. In other words, the system was assumed to be completely unavailable. This is a very conservative assumption because it is unlikely that all systems allowed to be in maintenance would all be in maintenance at the same time. In addition, some systems in maintenance might be returned to service in time. The fault trees used in this study are contained in Attachment 19QA. A mission time of 24 hours was used for this study. The loss of RHR event is assumed to terminate successfully if the mitigating systems start and run for a period of 24 hours. It is assumed that provisions for long term maintenance of decay heat removal will be made within 24 hours. This assumption is consistent with other full power PRAs.

A number of deterministic analyses were performed and documented in Attachment 19QB. These include the estimation of time available for operator action and human reliability analysis to estimate the probability of operator error under various conditions.

The event accident sequences were quantified with an initiating event frequency of 1.0. Thus the core damage probability that is obtained by this evaluation yields the conditional probability of core damage given a loss of decay heat removal event. The accident sequences were quantified assuming various complements of systems to be available. The various minimum complements of systems that met the goal were selected for inclusion in Tables 19Q-3 through 19Q-5.

For the CDF analysis, the event trees were quantified with realistic initiating event frequencies to determine importance of initiators, design features, component failure modes and unavailability. Various assumed unavailability cases were run and no components were found that, if unavailable, would result in exceeding the CDF criteria for the assumed maintenance configuration. Additionally, for all cases, the overall CDF was negligible. The results of the CDF analysis are documented in Reference 19Q-1.

Maintenance of the suppression pool was not modeled in this study. If the suppression pool level must be lowered for any reason, several options exist, such as: off loading all fuel in the RPV to the spent fuel pool or making systems available which do not rely on the suppression pool as a source of water (e.g., condensate, fire water, HPCF). From a risk perspective, the suppression pool should only be drained during periods when it is not relied upon for a source of water or heat sink in performance of an ECCS function. If the above recommendations are followed, the suppression pool unavailability will have a negligible impact on core damage frequency during shutdown.

19Q.7.5 Core Damage Probability Goal and RPV Boiling

The conditional core damage probability (CCDP) goal was selected for this study for the following reasons. The initiating event frequency for loss of an RHR System is not included in this probability goal, but was quantified for the CDF analysis. In the CCDP analysis, it is conservatively assumed that all systems not explicitly required to be kept out of maintenance are totally unavailable (i.e., all in maintenance).

The ABWR meets the NRC goal of an overall core damage frequency of 1.0E–04 and a large release goal of 1.0E–06 per reactor-year. In reality, loss of RHR events occur less than assumed and more importantly, not all systems allowed to be in maintenance will all be in maintenance at the same time. Typically, the results show that more than six to ten systems are allowed to be under maintenance and there is a very low probability that all the systems will be simultaneously under maintenance because of administrative controls such as the NRC's maintenance rule. An analysis using more realistic maintenance unavailability assumptions results in lower core damage frequency estimates. The simplifying assumption of 0 or 1 for maintenance unavailability allows for the calculation of core damage probabilities without having to model maintenance unavailability for each system. This avoids discussion of overlapping maintenance periods for systems during outages. These conservative assumptions allow for a straightforward determination of minimum system availabilities that also meet the NRC risk goals.

In Mode 5 with the RPV head removed, it is assumed that successful DHR can be achieved by allowing water in the RPV to boil and making up lost water by various water sources. Boiling under these conditions is an effective means of DHR but it is not desirable because the resultant pressure buildup in secondary containment could cause loss of containment integrity (i.e., steam release to the atmosphere). Calculations presented in Attachment 19QB show that the boiling release rates, assuming no core damage, are well below allowable limits for normal plant operations.

Equipment in the reactor building would be exposed to the steam environment including: CRD, CUW, RHR, HPCF, and FPC. No other areas in the plant would be exposed to the steam environment that operators would need to enter to assure continued decay heat removal capability.

The RHR and HPCF Systems are qualified for a harsh environment and their operation would not be affected by the steam. The impact of the steam on operation of CUW or FPC is a moot point because either the systems had previously failed or the decay heat load exceeded their capacity or boiling would not have occurred.

The CRD System is not qualified for a steam environment but due to its hardy construction it would be expected to operate for some period of time. Depending on the decay heat load, the time to boiling could vary between 4 - 26 hours. After 4.5 days, the time to boiling is approximately 15 hours and after 14 days is 26 hours. Therefore, for most of the outage, the

CRD System could be relied upon for makeup for a significant period of time following loss of normal decay heat removal before being damaged by the steam environment.

There would also be non-safety-related equipment in other buildings that would not experience the steam environment which could be relied upon for makeup (e.g., condensate). The fire water system can also be used for makeup at low pressure.

The fire water system ties into the RHR System through a connection on the outside of the reactor building. Three RHR valves inside the reactor building must be manually opened to inject fire water into the RPV. Adequate time would be available to open these valves following loss of RHR before boiling occurred so that the operator would not be affected by the steam environment. All other operator actions to mitigate loss of RHR can be performed outside the reactor building.

19Q.7.6 Success Criteria

In order to prevent core damage given an initiating event, sufficient systems must be available to ensure that the core decay heat is removed and the fuel remains covered by water. No fuel damage will occur as long as the fuel remains covered by water. There are three ways to achieve success:

(1) Remove decay heat directly from the coolant in the RPV

(2) Remove decay heat indirectly by condensing the steam produced, and provide makeup water to the RPV

(3) Allow the coolant to boil in the RPV and provide makeup water to the RPV to keep the core covered

These three ways to achieve success are discussed in detail below:

(1) Direct Decay Heat Removal from RPV

Recovery of the failed RHR System, use of one of the other two RHR Systems (SDC) or the Reactor Water Cleanup (CUW) System (under certain plant conditions) is sufficient for success. The CUW System capacity is temperature dependent and requires one pump and both nonregenerative heat exchangers (the regenerative heat exchangers must be bypassed). In Mode 5, the Fuel Pool Cooling and Cleanup (FPC) System can be used after the reactor cavity is flooded. FPC alone after 10 days is sufficient to remove all the decay heat. Both FPC pumps and heat exchangers and the supporting systems are required. CUW can remove the entire decay heat 8 days after shutdown.

(2) Decay Heat Removal and RPV Water Makeup

Under certain plant conditions the main condenser, if available, can be used to remove decay heat by condensing steam. The MSIVs must be opened and a condensate return path to the RPV is required. If the condenser is unavailable, steam can be released through the SRVs into the suppression pool and RPV makeup can be supplied by several sources. The availability of the SRVs is not explicitly modeled. At least one SRV is expected to be operable in the safety mode (i.e., spring pressure) even if power is not available.

High pressure makeup can be accomplished by the HPCF, CRD, or feedwater and condensate systems. Low pressure makeup is available from the condensate, LPFL or AC-independent Water Addition Systems. Low pressure makeup may require depressurization of the RPV by actuation of ADS or individual SRVs.

(3) In Mode 5 with the RPV head removed, boiling of water in the RPV with adequate makeup from low or high pressure sources is considered success for the purposes of this study.

Mitigation of loss of offsite power requires recovery of offsite power or use of the emergency diesel generators or combustion turbine generator. The AC-independent Water Addition System can be used for make up in the event of a loss of all AC power.

The success criteria and loss of decay heat removal event trees do not explicitly model the failure to maintain RPV water level for availability of the Reactor Water Cleanup System or RHR. RPV level is assumed to be maintained by automatic activation of ECCS (i.e., LPFL or HPCF) in Modes 3 - 4 and Mode 5 (reactor cavity unflooded). In Mode 5 with the reactor cavity flooded, RPV level control is assured since the water level will be 7.01 m (23 feet) above the RPV flange.

Table 19Q-2 summarizes the loss of RHR success criteria.

In addition, for LOCA event trees, if a LOCA or RHR flow diversion occurs, continuous makeup may be required unless the break can be isolated. The design of the RPV with piping penetrations above the top of active fuel allows for many makeup sources to be used, but direct decay removal methods may be unavailable. If a break or flow diversion pathway remains unisolated, then the normal suction of RHR, Reactor Water Cleanup or Fuel Pool Cooling may become uncovered making direct heat removal unavailable by these systems. Therefore, RHR, Reactor Water Cleanup, and Fuel Pool Cooling are conservatively not credited if the break occurs in a non-isolable location or if isolation valves fail to close. If isolation is successful, all three ways to achieve success are credited as appropriate for the plant mode and time after shutdown.

19Q.7.7 Accident Progression and Event Trees

Loss of RHR may initiate from a failure in the operating RHR System, loss of operating Service Water pump, or loss of offsite power. A LOCA event may initiate from a pipe break, valve failures or human error. The accident progression for each of the above initiators is discussed below.

19Q.7.7.1 Loss of RHR Due to Failure in the Operating RHR System

Following reactor shutdown, the plant is cooled down by rejecting steam to the main condenser and making up water loss in the RPV by the feedwater system. The RHR System in the SDC mode can be initiated at about 1.034 MPa which corresponds to approximately 456 K (360°F). The RHR System is then used to cool down to either Mode 4 [less than 367 K (200°F)] or Mode 5 (refueling). Loss of the operating RHR loop is assumed to occur sometime after it has been initiated.

Loss of RHR in Mode 3 or 4

Figures 19Q-1 and 19Q-2 are the event trees for loss of RHR in Mode 3 or 4, respectively. The following discussion applies to both event trees. Following loss of the operating RHR loop (event tree node RHR), the operator has to recognize the event and start following the correct procedure (OP). The sequence of events following the successful outcome at this node is described first. The operator can identify the failed system and request the maintenance crew to restore it to operation. An analysis showed that for the decay heat load at this time, water in the RPV would begin to boil in 1.3 hours. Using a typical mean time to repair for the RHR System, and 1.3 hours as the time for recovery, the system recovery probability was determined (REC).

If the failed RHR System cannot be recovered, the operator could initiate one of the other two RHR Systems, if available, in the shutdown cooling mode (R). If all RHR Systems fail, the RPV would pressurize and the main condenser could be made available (V2) by opening the MSIVs, drawing a vacuum in the condenser, and operating the feedwater, condensate booster, and condensate pumps for makeup.

If the main condenser fails or is unavailable, the operator can use the CUW System to remove the decay heat (W2) if the RPV temperature is above 386 K (234°F).

If all DHR means are unavailable, the only path to success is to keep the core covered by either high pressure or low pressure sources. The high pressure sources are feedwater and condensate (Q), HPCF (UH), or a CRD pump (C). The HPCF initiates automatically whereas the other two systems require operator action. If all these fail, the operator must depressurize the RPV by actuation of individual SRVs or ADS will initiate automatically (X) on low water level in the RPV. Successful depressurization would make the LPFL (VI), condensate (CDS), or AC-independent Water Addition (FW) Systems available.

Failure to depressurize the reactor or failure of FW leads to core damage.

If at node OP, the operator fails to follow the correct procedure, the reactor coolant temperature and pressure in the RPV will rise, the SRVs will open and discharge steam to the suppression pool and eventually the HPCF will initiate (UH) on low RPV water level. If HPCF fails, ADS will actuate on low water level (X). Failure to depressurize will lead to core damage. Following successful reactor depressurization, LPFL will inject on low water level(VI). Failure to inject with LPFL leads to core damage.

Loss of RHR in Mode 5

Figure 19Q-3 shows the event tree for loss of RHR in Mode 5 less than 3 days after shutdown. This sequence is the same as the previous one except that since the RPV head is removed, the main condenser and feedwater pumps are unavailable and ADS is not required as the RPV cannot become pressurized. Also, at this low temperature, CUW by itself is not capable of removing all the decay heat generated within three days of shutdown.

Figure 19Q-4 shows the event tree for loss of RHR in Mode 5 for 3 - 8 days after shutdown. Figure 19Q-5 shows the event tree for loss of RHR in Mode 5 for the period 8 - 10 days and Figure 19Q-6 shows the event tree for greater than 10 days. The differences in these event trees are that for the period 8 - 10 days CUW alone is success (W2) and beyond 10 days FPC alone (FPC) is success.

19Q.7.7.2 Loss of RHR Due to Loss of Service Water

Figures 19Q-7 through 19Q-16 show the event trees for loss of the Division A or C operating service water pump. The scenarios are basically the same as for a loss of RHR except that loss of the operating service water pump may impact other DHR or makeup systems in addition to the operating RHR pump. Loss of both service water pumps in Division A or B (operating and standby pumps) also results in loss of CUW and FPC. For Division B, the HPCF(B) is also lost (Division A contains RCIC which is not available during shutdown). Likewise, loss of both service water pumps in Division C causes loss of HPCF(C) in addition to the Division C RHR pump. Loss of Division B service water is identical to loss of Division A service water, therefore no event trees were developed specifically for Division B.

19Q.7.7.3 Loss of RHR Due to Loss of Offsite Power

Figures 19Q-17, 19Q-18 and 19Q-19 show the event trees for loss of offsite power in Modes 3, 4, and 5, respectively. The success criteria are the same but longer time is available for recovery in Mode 5. Following a loss of offsite power, it is possible to recover power in time to prevent core damage. If power is not recovered, the available DG will start automatically, and if the DG fails, CTG can be manually initiated. Following loss of all AC power, the AC-independent Water Addition System can be used for make up if the RPV can be depressurized by opening SRVs.

19Q.7.7.4 LOCA and Flow Diversions

Several LOCA and flow diversion initiating events were postulated to occur, causing RPV drainage and challenges to inventory control. Subsection 19L.6 discusses flow diversion paths in the Reactor Water Cleanup, CRD and RHR systems. These paths were reviewed against screening criteria. The review resulted in nine paths that were retained for quantitative analysis. In addition to these diversion pathways, pipe break LOCAs were postulated in RPV connecting systems. The selected initiators and their quantitative analysis are discussed in Reference 19Q-1.

LOCAs are addressed based on size and on plant mode. Human error probabilities are assessed based on the size of the break, the plant mode, and if the refueling cavity is flooded. To reduce the number of event trees, specific system success criteria for time after shutdown are addressed in the system logic. Therefore, all the LOCA events can be addressed with the three event trees discussed below.

Small LOCA in Mode 3 or Mode 4

Figure 19Q-20 is the event tree for small LOCA and flow diversion during Modes 3 and 4. Following the LOCA event, if the operator follows procedures to recover the affected train of RHR, and LOCA isolation is successful, the event progression follows that of a loss of an operating train of RHR. If the break occurs in a non-isolable location or the isolation valves fail to close (LISOL), water level is assumed to drop below RPV suction lines and fail both RHR and the Reactor Water Cleanup System. Additionally, the low level isolation signal is conservatively assumed to preclude reestablishing steaming to the condenser (V2) with a feedwater return path for makeup. HPCF (UH) and CRD (C) makeup systems are credited. If the LOCA occurs below TAF, as would be if the CUW system suction line broke, then CRD (C) is not credited and is failed in the system logic. If both HPCF and CRD fail, ADS (X) is required to depressurize the RPV to allow low pressure makeup from LPFL (WDCS), one condensate pump (CDS) or ACIWA (FW). The break size is assumed smaller than what will maintain RPV pressure low if decay heat removal is lost. If the operator fails to follow procedures (OP), then only those systems that are automatically actuated, HPCF and LPFL after successful ADS, are credited.

Large or Medium LOCA in Mode 3 or Mode 4

Figure 19Q-21 is the event tree for large or medium LOCA in Mode 3 or Mode 4. This event tree is identical to the small LOCA tree, except that if isolation (LISOL) fails, the RPV pressure is assumed to remain low and low pressure makeup systems are not dependent on ADS success. If LOCA isolation is successful, then ADS would be required for success of low pressure makeup.

LOCA in Mode 5

Figure 19Q-22 is the event tree for all LOCAs or flow diversions that may occur in Mode 5. As with the other LOCA event trees, if the operator follows procedures to recover the affected train of RHR and LOCA isolation is successful, the event progression follows that of a loss of an operating train of RHR. Mode 5 operation allows for decay heat to be removed using CUW (W2) and Fuel Pool Cooling (FPC) after 8 days and 10 days, respectively. The availability of these systems to provide cooling is modeled in the systems logic. Because the RPV is open, cooling by boiling is credited and ADS is not required for low pressure makeup. If isolation fails (LISOL) or the operator fails to follow instructions (OP) the event progression follows that of the large or medium LOCA event tree sequences for Mode 3 or Mode 4 with the greatest difference being the time available to respond to the event being much longer after flooding.

19Q.7.8 System Fault Trees

The unavailability of a system to perform its safety function on demand given a loss of RHR was evaluated by fault tree analysis. Twelve system fault trees were used in this analysis. The fault trees are contained in Attachment 19QA.

Five of the fault trees: HPCF, RHR (SDC), RHR (LPFL), Reactor Service Water, and ADS, were taken from the full power PRA with modifications (e.g., maintenance unavailability and operator actions) to reflect shutdown conditions. The other seven fault trees were developed specifically for the shutdown PRA and include:

- Reactor Water Cleanup,
- Fuel Pool Cooling,
- Main Condenser,
- CRD,
- AC Independent Water Addition
- Condensate, and
- Feedwater.

The fault trees model system unavailability due to mechanical failures, loss of power, and operator errors. As previously mentioned, for the minimum sets analysis, maintenance unavailability is either assumed to be 1 or 0 (i.e., system is in or out of maintenance).

In addition to these system fault trees, five initiating event fault trees were developed for the CDF analysis: LOCAs and flow diversions, loss of offsite power, loss of RHR train A, loss of RSW train A and loss of RSW train C. For the LOCA event trees, a failure of LOCA isolation tree was developed.

19Q.7.9 Results and Conclusions

19Q.7.9.1 Introduction

A probabilistic assessment of minimum sets using CCDP and a probabilistic assessment of realistic CDF were performed. The results of the realistic CDF analysis, documented in Reference 19Q-1, show that ABWR shutdown risk is negligible for loss of decay heat removal events, loss of offsite power, LOCA, or flow diversion events. The remainder of this section focuses on the results of the minimum sets analysis.

For the minimum sets analysis, the loss of decay heat removal event trees described in the previous subsection were evaluated and the core damage probability calculated with certain systems assumed unavailable due to maintenance. In general, the minimum set of equipment assumed to be available was initially taken as that required by the Technical Specifications for the given operating mode. Combinations of systems were made available until a set resulted in a conditional probability of less than the selected threshold. Each of these sequences that met the acceptance criteria is considered a minimum set for assuring acceptable shutdown risk.

Minimum sets were obtained for each of the three loss of RHR initiators:

- Loss of Operating RHR System
- Loss of Operating RSW Pump
- Loss of Offsite Power

Tables 19Q-3 through 19Q-5 list certain minimum sets of systems that meet the acceptance criteria for loss of the operating RHR System initiator for the three major configurations during shutdown. The configurations are: Modes 3 or 4, Mode 5 prior to flooding the reactor cavity, and Mode 5 after the reactor cavity has been flooded. The effect of changes in decay heat, as a function of time, will be discussed for each of the three plant conditions.

With about 12 systems available, and about four needed to meet the goal, many minimum sets can be identified. In order to simplify the selection of minimum set systems, the following maintenance philosophy was assumed: all of division C in maintenance; division B, ADS, and combustion turbine generator (CTG) are available. Although the CTG is not covered by Technical Specifications, its availability is assumed to be controlled by Administrative Procedures. Other maintenance philosophies can be adopted and the model used to identify appropriate minimum systems. Additional details of the plant configuration based on selected maintenance philosophy is as follows. The plant is being cooled through use of RHR “A” and its support systems (i.e., service water “A”, RCW “A”, electric power division “A”). Other division “A” systems, including EDG “A” may be in maintenance unless specifically included as a support system in one of the minimum sets. All division “B” systems are assumed to be not in maintenance, although they may become unavailable due to random failures or operator errors. All division “C” systems are assumed to be in maintenance. For the above assumed

configuration, one of the isolation valves for RHRB is powered by division "C" (due to single failure concerns with containment isolation). If RHRB is required, division "C" power can be made available momentarily. This configuration was selected because it is one that meets minimum technical specification requirements (i.e., 2 ECCS and 2 RHR Systems available). Other configurations could have been selected but this one is typical and the resulting minimum sets identified will demonstrate the low risk associated with loss of decay heat removal for the ABWR and the flexibility afforded utilities for outage maintenance scheduling while still maintaining low risk levels. If one of the assumed power sources becomes unavailable, the utility should make another power source (e.g., a second EDG) available to ensure the safety criterion will be met. Normal surveillance testing should be used to assure the availability of these systems.

19Q.7.9.2 Loss of RHR Initiator

The minimum set for loss of RHR is discussed first. Table 19Q-3 lists some minimum sets of systems that if available during Mode 3 or 4 meet the core damage criterion. As can be seen, if the 2 ECCS Systems are assumed to be RHR, then only a CRD pump plus AC-independent Water Addition or CUW plus AC-independent Water Addition need be made available. This is not restrictive since one pump from CRD and firewater are usually available for other reasons (e.g., CRD to purge the FMCRDs and AC independent water addition for fire protection) and CUW is usually operable during this period. The table shows five different minimum sets. This is indicative of the flexibility for performing ABWR shutdown maintenance while still maintaining risk margins.

Table 19Q-4 lists some minimum sets of systems for Mode 5 during 2 - 3 days after shutdown. In this configuration the RPV head bolts have been detensioned and the head is off but the reactor cavity has not been flooded. For this Mode 5 configuration, fewer systems are available than during Mode 3 or 4 or after flooding the reactor cavity but enough systems are available to ensure adequate risk margins. Also, this is a relatively short duration of the outage. The main condenser is not available since the RPV cannot be pressurized. Fuel pool cooling cannot be used because the RPV and fuel pool have not been connected together and CUW capacity is not sufficient to remove all the decay heat due to the low RPV temperature and high decay heat load. The table shows three minimum sets of systems which meet the risk criteria. As was noted for Modes 3 and 4, the CRD pump which is normally available in addition to fire water and RHRB meet the core damage criterion. Another minimum set might be RHRB (SPC) condensate, and fire water.

Table 19Q-5 lists nine minimum sets for Mode 5 following 3 days after shutdown when the reactor cavity is flooded. RHR plus condensate and fire water meet the criterion. After 8 days, CUW and firewater along with either CRD or condensate meet the criterion, and after 10 days, FPC, CRD, and condensate could be a minimum set. As time following shutdown increases, more systems become able to remove decay heat and greater time is available for operator actions prior to boiling or core damage.

As Tables 19Q-3 through 19Q-5 illustrate, many combinations of systems can be made available to ensure adequate shutdown risk while still allowing for maintenance to be performed on systems. As previously mentioned, these minimum sets are only a few of the possible combinations that will ensure adequate shutdown risk margins. Other minimum sets can be identified for different assumed plant conditions. An important point that is illustrated by the minimum sets identified in this study is that under all shutdown plant conditions, minimum technical specification requirements plus systems that are normally operating or available during shutdown (e.g., CUW, FPC, CRD, and fire water) are enough to ensure adequate shutdown risk margins.

19Q.7.9.3 Loss of Service Water (SW) Initiator

If loss of the operating SW pump is assumed to be the initiating event, all the minimum sets in Tables 19Q-3 through 19Q-5 would be applicable. This is because there is only one RHR pump per division, while one standby pump supports the operating pump in each division of service water. Therefore, RHR (A) is not lost due to the failure of the operating RSW pump. With RHR (A) available, the minimum sets previously identified without RHR (A) must still be able to meet the acceptance criteria. Loss of the operating RHR pump is the limiting condition for this analysis.

19Q.7.9.4 Loss of Offsite Power Initiator

For a loss of offsite power initiator, calculations have shown that the probability of failing both the EDG and the CTG along with not recovering offsite power within 80 minutes is extremely small. For core damage to occur, loss of AC independent water addition or ADS must also occur. This scenario is less than the acceptance criteria and thus meets the criterion. Since the above maintenance philosophy assumes only EDGB and the CTG are available, no additions to the minimum sets already identified are required for the loss of offsite power initiator.

19Q.7.9.5 Adequacy of Technical Specifications

From the above results, the following can be stated regarding adequacy of the ABWR Technical Specifications. In Mode 5, the onset of boiling is most dependent on water level (or total inventory), and thus the most vulnerable condition is at low water level prior to flooding up of the reactor cavity. In this condition, not only is the time to boiling relatively insensitive to decay heat level, but RHR in shutdown cooling (SDC) is the only source of decay heat removal. This is the basis for the Technical Specifications requiring that two loops of RHR SDC be available in this condition; one normally operating and one in standby. Results of the analysis show that given the loss of the operating RHR pump, with one RHR loop in standby there is a small probability of the onset of boiling. This is acceptable given the short time duration the plant is expected to be in this unique condition and the benign consequences that are calculated to result so long as core damage is avoided. Clearly, a utility could further reduce the likelihood of boiling by assuring that the third division of RHR SDC provided in the ABWR design is available during these conditions. Thus, during the early stages of the transition from Mode 4 to Mode 5 (prior to flood-up), the availability of the third loop of RHR SDC further reduces

shutdown risk. However, given the other compensatory measures available to delay the onset of boiling and prevent core damage (e.g., condensate, AC independent water addition, CRD), the two loops of RHR SDC required by ABWR Technical Specifications are more than adequate during these plant conditions.

19Q.7.9.6 Contribution of Human Errors to CDF

The ABWR design is relatively insensitive to human error contributions to CDF during shutdown for the following reasons. Although several potential human errors have been identified (e.g., failure to recognize the loss of operating RHR loop and failure to manually actuate systems such as condensate, fire water, Reactor Water Cleanup, and Fuel Pool Cooling), multiple systems and paths for decay heat removal and makeup are available during shutdown to mitigate these errors. Also, automatic actuation of makeup from LPCF and HPCF and multiple alarms to alert the operator to potential unsafe conditions during shutdown (e.g., high RHR temperature, sump pump alarms, fire detection, low RPV level, high area radiation, and high neutron flux) all contribute to the conclusion that the ABWR is tolerant of human errors.

The methodology used in this study does not allow for a quantitative estimate of the impact of human errors to CDF, but based on the above discussion it is considered to be low.

19Q.8 Use of Freeze Seals in ABWR

Freeze seals are used for repairing and replacing such components as valves, pipe fittings, pipe stops, and pipe connections when it is impossible to isolate the area of repair any other way. Freeze seals have successfully been used in pipes as large as 700A (28 inches) in diameter.

The ABWR design has eliminated a significant amount of piping associated with the Reactor Coolant System (RCS)(e.g., no recirculation loops). This by itself will reduce the necessity for freeze seals in ABWRs over other plant designs.

In addition to reduced RCS piping, the ABWR design has most piping connected to the reactor pressure vessel (RPV) enter at a level significantly higher [152.4 cm(5 feet)] than the top of active fuel. Inadvertent draining from these lines will automatically stop without exposing the fuel. The only piping connection below the top of active fuel (Reactor Water Cleanup System) is small in size [<50A (< 2 inches)]. If a freeze seal were required on this line and it were to fail, several sources of makeup are available to refill the RPV to prevent core uncovery.

Whenever freeze seals or other temporary boundaries are used in the ABWR, administrative procedures will be necessary to ensure integrity of the temporary boundary. Also, mitigative measures will be identified in advance and appropriate backup systems made available to ensure no loss of coolant inventory occurs.

An option that a utility could choose is to off-load all the fuel in the RPV to the spent fuel pool when repair or maintenance of an unisolatable valve must be completed.

The selected method for working on unisolatable valves must take into account adequate safety margins, personnel experience with freeze seals, availability of backup systems, and the potential impact on other outage activities.

See Subsection 19.9.23 for COL license information requirements.

19Q.9 Shutdown Vulnerability Resulting from New Features

The ABWR has incorporated many new design features that do not exist in current operating domestic BWRs. These features have been added based on past operating experience, advances in technology since earlier designs were finalized, and the results of detailed probabilistic risk assessments (PRAs).

In order to evaluate the potential shutdown risk associated with these new features, a Failure Modes and Effects Analysis (FMEA) was completed for each new feature. The feature is identified followed by potential failure mode(s). The possible method for detecting each failure mode is then presented followed by the potential impact on safe shutdown and any preventive or mitigating feature that may exist. Finally, the overall shutdown vulnerability evaluation is described.

The FMEA is contained in Table 19Q-6. As the results presented in Table 19Q-6 show, there are no identified vulnerabilities resulting from implementation of new design features in the ABWR that affect shutdown risk.

19Q.10 Procedures

The ABWR has been designed to minimize risk associated with plant operations both at normal power and shutdown conditions. As previously mentioned, PRA techniques have been employed to identify potential accident scenarios and, where appropriate, design modifications have been included to reduce estimated risks. In addition to the physical plant design and configuration, the ABWR will incorporate operating procedures that are based on rigorous engineering evaluations including safety analyses. These procedures will be prepared consistent with NUMARC Guidelines presented in NUMARC 91-06, “Guidelines to Enhance Safety During Shutdown.”

Each utility must generate plant specific operating procedures based on individual site characteristics and training program requirements. A procedures guideline will be completed for the ABWR to address shutdown conditions. The guideline will provide insight into two general areas:

(1) Effective outage planning and control

(2) Maintenance of key shutdown safety functions:

(a) Decay heat removal capability,

(b) Inventory control,

(c) Electrical power availability,

(d) Reactivity control, and

(e) Containment integrity (primary and secondary).

Outage Planning and Control

Although design features help, shutdown risk can best be minimized through appropriate outage planning and control procedures. Planning is important because of the large number and diversity of tasks that must be completed during the outage. Safety and support systems must be taken out of service for maintenance. This reduces redundancy of safety systems. If alternate means are not utilized to backup the lost safety system, a reduction in safety margin may occur. The ABWR contains multiple normal and alternate systems to complete all required shutdown safety functions. Availability of normal and alternate systems must be made known to all personnel involved in planning and execution of the outage. This is an ever-changing situation during outages and proper planning and tracking of activities is required to ensure safety margins are maintained.

The plant specific procedures for outage planning and control should ensure that the appropriate focus is maintained on the following activities:

(1) Documentation of outage philosophy including organizations responsible for outage scheduling. This should address not just the initial outage plan but all safety significant changes to the schedule.

(2) Ensuring that all activities, particularly higher risk evolutions, receive adequate resources. The plan should consider scope growth and unanticipated changes.

(3) Ensuring that the “defense in depth” concept that is central to power operation be maintained during shutdown to ensure that safety margins are not reduced. Safety systems must be taken out of service for maintenance but alternate or backup systems can be made available if proper planning is completed.

(4) Ensuring that all personnel involved in outage planning and execution receive adequate training. This should include operator simulator training to the extent practicable. Other plant personnel, including temporary personnel, should receive training commensurate with the outage tasks they will be performing.

(5) After completion of outage planning, but prior to final approval, a review of the schedule should be completed by an independent safety review team. The main objective of this review is to assure that the defense in depth principal will not be violated at any time during the outage.

See Subsection 19.9.25 for COL license information requirements.

Shutdown Safety Issues

Procedures for outage planning and control address general aspects of risk reduction during shutdown. Specific shutdown procedures are required to maintain key safety functions during shutdown (See Subsection 19.9.25 for COL license information requirements). The following guidelines should be used for each key shutdown safety function.

(1) Decay Heat Removal Capability

The normal method of Decay Heat Removal (DHR) is through use of the Residual Heat Removal System (RHR) in the shutdown cooling mode. As discussed in Subsections 19Q.7 and 19Q.11, there have been many events at operating plants that have resulted in partial or total loss of DHR. A recovery strategy should be established to address loss of normal RHR. This should include identification of alternate DHR Systems as well as personnel responsible for execution of the recovery plan. In addition to recovery plans, outage planning should emphasize availability of DHR by postponing maintenance on RHR Systems to later in the outage when decay heat loads have been reduced or to when the core has been off-loaded to the spent fuel pool. In the case of core off-load, procedures should be prepared to ensure maintenance of spent fuel pool cooling.

(2) Inventory Control

If DHR were to be lost, the time to reactor coolant boiling and core uncovery will be determined by the initial coolant inventory and makeup capability. Procedures should be prepared to ensure that adequate coolant inventory is maintained at all times during shutdown. Also, plant activities or configurations where a single failure can result in loss of inventory should be identified and compensatory measures established. Specific activities for the ABWR that should be reviewed for the potential of inventory deduction are: Use of freeze seals (see Subsection 19Q.8 for a more complete discussion); removal of control rods, control rod drives, and reactor internal pumps; RHR valve actuations or leakage leading to diversion of RPV coolant to the suppression pool (e.g., RHR pump mini-flow valve failure/leakage, switching shutdown cooling from one division to another); and inadvertent actuation of safety relief valves.

(3) Electrical Power Availability

As discussed in Subsections 19Q.4.4 and 19Q.11, loss of electrical power during shutdown has resulted in loss of DHR in the past. The ABWR has two sources of offsite (preferred) and four sources of onsite electrical power. Procedures should be utilized to ensure that defense in depth for electrical power sources is maintained. Maintenance of power sources should reflect the current plant conditions. Availability of normal and alternate power sources should be ensured especially during periods of higher risk evolutions (e.g., unbolting the RPV head prior to

flooding the reactor cavity). Many of the loss of power events discussed in Subsection 19Q.11 were caused by operator errors (e.g., switching errors, inadequate maintenance/testing procedures) and grounding of transformers in switchyards due to movement of equipment by cranes and trucks. All maintenance and switchyard activities should be reviewed to identify single failures or procedural errors that could result in loss of power to vital buses during shutdown. Procedures should be developed for implementation of alternate sources of power including applicable breakers and bus locations, required tools, and sequence of steps to be performed.

(4) Reactivity Control

Shutdown reactivity control for the ABWR is maintained by core design analysis and interlocks that restrict fuel and control rod drive movements. Procedures are required to ensure that the core is loaded per design requirements and that unauthorized fuel movement does not occur simultaneous with CRD mechanism maintenance. If the refueling sequence must be altered, new shutdown margin analyses should be performed. All fuel movements should be verified by knowledgeable trained personnel.

(5) Containment Integrity

The ABWR primary containment will not be available during most of the refueling outage but procedures should be developed to ensure its availability during Mode 3 and during Mode 4 (if appropriate). During all modes, procedures should be available to ensure that secondary containment can be maintained functional as required, especially during higher risk evolutions.

Procedure Reviews

An important part of procedures implementation is a review of the adequacy of all operating procedures. All shutdown operating procedures should be reviewed periodically to ensure that the defense in depth concept is being maintained given the actual events occurring at each site. This review should include not only procedure adequacy but dissemination of the outage philosophy to all personnel involved in scheduling and executing the outage plan and training of personnel including temporary personnel. This review should be documented and retained as a permanent plant record.

19Q.11 Summary of Review of Significant Shutdown Events: Electrical Power and Decay Heat Removal

As part of the certification process for the ABWR design, the NRC has requested that General Electric complete a review of significant shutdown events in operating plants and discuss ABWR features which could prevent or mitigate such events.

To complete this evaluation, a review was made of operating events involving loss of offsite power (LOOP) and loss of Decay Heat Removal (DHR). These two areas appear to have the

greatest potential for causing core damage during shutdown based on past experience. The sources utilized for information on past shutdown events were:

- "Residual Heat Removal Experience Review and Safety Analysis", NSAC-88, March 1986
- "Loss of Vital AC Power and the Residual Heat Removal System during Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990", NUREG-1410, June 1990
- "NRC Staff Evaluation of Shutdown and Low Power Operation", NUREG-1449, March 1992
- Selected INPO SEO Reports and NRC Information Notices

The results of this evaluation are contained in Attachment 19QC, Tables 19QC-1 and 19QC-2 for LOOP and loss of DHR respectively. The following is a discussion of the results for each event type.

LOOP

NUREG-1410 contains a discussion of 70 LOOP events at operating plants both PWR and BWR. Although the response to LOOP events will differ for PWRs and BWRs, the initiating events are similar in that offsite and onsite power configurations are similar for both reactor types. The events evaluated in NUREG-1410 occurred between 1965 and 1989. Two additional LOOP events were added to this list and are included in Table 19QC-1.

The LOOP events can be grouped into the following categories:

- Loss of all offsite power sources due to various reasons including weather, operator errors or grid upset
- Loss of one or more offsite sources with at least one offsite source remaining
- Isolation of offsite power due to onsite electrical faults
- Degraded offsite or onsite power sources resulting from errors in maintenance activities

As discussed in Table 19QC-1, the ABWR electrical distribution system has several features which would prevent or mitigate every precursor event evaluated in this study. Prevent or mitigate in this case means that at least one Class 1E power supply would be available to energize equipment to maintain plant cold shutdown.

The main features of the electrical system are:

- Two independent sources of offsite power
- Three physically and electrically independent Class 1E emergency diesel generators

- Three unit auxiliary transformers powering three Class 1E and three non-1E power buses
- Combustion Turbine Generator (CTG) that can be used to power any of the Class 1E or non-1E power buses

The above features of the ABWR electrical distribution system, along with appropriate Technical Specifications and other administrative controls, assures that adequate power sources would be available to mitigate potential electrical events such as those described in Table 19QC-1.

Loss of DHR

NSAC-88 contains a discussion of 90 loss or degradation of DHR events during the seven year period 1977 through the end of 1983. The source for these events were Licensee Event Reports (LERs). Other events described in INPO SEO reports and NRC information notices were also reviewed and included in the study.

Summary of DHR Events

The results of this evaluation are contained in Table 19QC-2. Not all of the events discussed in NSAC-88 are contained in Table 19QC-2. Those events that were due to random failures of single components and did not result in loss of DHR or other significant plant effects were not evaluated further. If the single failure resulted in loss of coolant, overpressurization, flooding, or loss of Shutdown Cooling (SDC) function, the event was included and the applicable ABWR feature to prevent or mitigate the event was discussed.

For the purposes of this study, prevention or mitigation means that, given the DHR challenge event, the ABWR design would either not be susceptible to the postulated failure or it has design features that could be relied upon to ensure that the fuel in the RPV remained covered with water at all times.

Of the events described in Table 19QC-2, some were single failures of RHR System components that resulted in either delayed achievement of shutdown cooling (SDC), reduction in reactor pressure vessel (RPV) water level, or a temporary loss of SDC. In all of these events, the fuel remained covered with water and alternate means of DHR remained available (e.g., Reactor Water Cleanup System, main condenser, and ECCS Systems). In the cases of delayed or temporary loss of SDC, RPV water temperature increases ranged from 261 K - 333 K (10° - 140°F). In all cases, SDC was restored and alternate means of DHR were not used although available. Operator errors associated with improper valve lineups or incorrect maintenance were identified. In these cases, delays in implementing SDC or temporary loss of SDC occurred while the error was corrected. In a few cases, marine growth caused failure of one or more RHR heat exchangers which resulted in temporary loss of SDC while other RHR loops or alternate cooling paths were implemented. In one case, a freeze seal failure in the RHRSW caused 56.8 m^3 (15,000 gallons) of water to damage ECCS power supplies resulting in temporary isolation of SDC.

None of the events described above and in Table 19QC-2 resulted in fuel being uncovered. The flexibility of the RHR System and the several alternate means of DHR that were available served to mitigate the component failures or operator errors.

Summary

Significant shutdown events in operating plants have been reviewed to determine ABWR features which could prevent or mitigate the events. Loss of offsite power and loss or degradation events from published nuclear industry reports were the database for this review. The results of this review demonstrate that ABWR design includes many features that prevent or mitigate unacceptable consequences of typical past events.

The main features of the ABWR that will prevent or mitigate shutdown events are:

- Three divisions of ECCS and support systems that are physically and electrically independent
- Two independent offsite power sources
- Four onsite power sources (three emergency diesel generators and one combustion turbine generator)
- Plant configuration and structural integrity to minimize common mode failures due to fire and floods
- Appropriate Technical Specifications and other administrative controls to ensure availability of systems during periods of potentially high risk operations
- Several alternate means of DHR if normal systems were to fail or be out of service for maintenance
- Instrumentation availability during shutdown to monitor plant safety status and initiate safety systems when needed

19Q.12 Results and Interface Requirements

19Q.12.1 Insights Gained from the Analysis

Completion of the ABWR shutdown risk analysis has resulted in the following insights:

(1) The most important element in control of shutdown risk is adequate planning of maintenance on systems and support systems that can be used to remove decay heat or supply inventory makeup to the RPV.

(2) The ABWR design has incorporated a significant number of new design features relative to operating BWRs. Past events that have led to loss of decay heat removal capability or loss of offsite power can, in general, be mitigated by ABWR design features.

(3) The ABWR design has a very low risk associated with loss of decay heat removal. Adequate shutdown safety margins exist if only systems required by Technical Specifications and those that are already in operation (e.g., CRD, FPC, fire water) are relied upon. Minimum combinations of systems have been identified that, if available, will ensure adequate shutdown safety margins. Combinations other than those identified in this study may exist which also result in adequate shutdown risk margins. By taking advantage of these available decay heat removal and makeup systems, utilities can exercise much flexibility in outage maintenance scheduling while ensuring that adequate safety margins are maintained at all times during shutdown conditions.

(4) The above safety margins were calculated using very conservative estimates for human error probabilities. For all events analyzed during shutdown, sufficient time is available to prevent core damage that no extraordinary operator actions are required. ABWR safety is designed into the plant.

(5) Fire and floods during shutdown can be mitigated by ensuring, through administrative procedures that at least one safety division is not in maintenance and its physical boundaries remain intact. If it is decided to breach the boundaries of two safety divisions to complete maintenance tasks, an evaluation must be completed to ensure that a minimum set of systems capable of meeting the shutdown safety criterion will remain available if a fire or flood were to occur. This applies to flooding/fire in the intact division as well as the breached divisions.

(6) The minimum technical specification requirements plus systems normally operating during shutdown (e.g., CRD, fire water, CUW) are adequate to ensure that safety margins can be maintained during shutdown due to a loss of an operating RHR train. Also, no technical specification changes are required to mitigate fires or floods during shutdown. Administrative controls are recommended on maintenance activities during shutdown to ensure the availability of systems to mitigate loss of RHR, fires, and floods.

19Q.12.2 Important Design Features

The ABWR features identified as important contributors to the low level of risk associated with shutdown are discussed in Subsection 19.8.6.

19Q.12.3 Operator Actions

The following operator actions have been identified that are important to minimization of shutdown risk and have been included as COL action items:

- Ability to recognize failure of an operating RHR System.

- Rapid implementation of standby RHR Systems following the loss of the operating RHR System.
- Use of alternate means of decay heat removal using non-safety grade equipment such as CUW, FPC, or main condenser.
- Use of alternate means of inventory makeup using non-safety grade equipment such as AC independent water addition, CRD pump, feedwater, or condensate.
- How to utilize boiling for decay heat removal in Mode 5 with the RPV head removed including available makeup sources.
- Implementation of fire/flood watches during periods of degraded safety division physical integrity.
- Fire fighting during shutdown.
- Use of remote shutdown panel during shutdown.
- Instrumentation must be made available during shutdown to support the following functions:
  - Isolation of RPV
  - ADS
  - HPCF
  - LPFL
  - RPV water level, pressure, and temperature
  - RHR System alarms
  - EDG
  - Refueling interlocks
  - Flood detection and associated valve isolation and pump trips
- Procedures should be prepared to address the following tasks during shutdown:
  - Fire fighting with part of the fire protection system in maintenance
  - Outage planning to minimize risk using guidance from NUMARC 91-06
  - Use of freeze seals

- Replacement of RIPs and CRD blades
- Loss of offsite power
- Increasing CRD pump flow when using it for inventory control
- Maintenance of suppression pool as it relates to maintaining safety margins for decay heat removal
- Ensure that one safety division is always available with intact fire/flood barriers.

19Q.12.4 Reliability Goals (Input to RAP)

The following assumed system unavailabilities were determined to be important in minimizing shutdown risk and are included in the ABWR Reliability Assurance Program:

System	Unavailability (Per Demand)
RHR (SDC)	†
RHR (LPFL)	†
HPCF	†
CRD	†
CTG	†
EDG	†
Offsite Power	†
ADS	†
DC Power	†

† Not a part of DCD (refer to Table 40 of Reference 19Q-1)

19Q.12.5 Conclusions

The ABWR has been evaluated for risks associated with shutdown conditions and for all postulated events, the risk has been determined to be low. Multiple means of removing decay heat and supplying inventory makeup have been identified that along with appropriate Technical Specifications and outage procedures result in acceptably low shutdown risk levels for the ABWR.

19Q.13 References

19Q-1 "ABWR Shutdown Risk Evaluation," Toshiba UTLR–0013.

Table 19Q-1 ABWR Features That Minimize Shutdown Risk

Category	Feature	Shutdown Risk Capability
Decay Heat Removal (DHR)	Residual Heat Removal (RHR) System	Three independent (100% capacity) divisions of RHR and support systems for normal DHR. Each RHR division has several DHR modes (e.g., SDC, SPC).
	Reactor Coolant Temperature Measurement	During shutdown, reactor coolant temperature is determined by measuring Reactor Water Cleanup (CUW) inlet water temperature.
	Shutdown Cooling Nozzle	The shutdown cooling mode of RHR uses suction piping that connects directly to a nozzle on the RPV instead of to an external piping system. This reduces the probability of losing RHR pump suction due to air entrapment or cavitation.
	Safety Relief Valves	Can be used as alternate means of decay heat removal by venting steam to the suppression pool. They are also actuated to depressurize the RPV to allow use of low pressure RHR or other low pressure systems.
	Suppression Pool	A potential heat sink and makeup source for decay heat removal. Pool temperature is monitored in the control room to indicate trends in pool temperature. This large heat sink allows sufficient time for appropriate operator actions.
	Reactor Water Cleanup System (CUW)	Can be used under certain conditions to remove decay heat. See Subsection 19Q.7 and Attachment 19QB for more details on this feature.
	RPV Boiling	When the RPV head is removed, boiling is an effective (although not preferred) heat transfer method as long as RPV water level can be maintained by available makeup sources.
	Condenser	The main condenser (if available) can be used for DHR.
	Remote Shutdown Panel (Two Divisions)	Cold Shutdown can be achieved and maintained from outside the control room if the control room is uninhabitable due to fire, toxic gas, or other reasons. The remote shutdown panel is powered by Class 1E power to ensure availability following a Loss Of Preferred Power (LOPP). Controls are hard wired and thus not dependent on data communications systems. A minimum set of monitored parameters and controls are included to ensure the ability to achieve and maintain cold shutdown.

Table 19Q-1 ABWR Features That Minimize Shutdown Risk (Continued)

Category	Feature	Shutdown Risk Capability
	Instrumentation	Adequate instrumentation is available to operators both inside and outside of the control room for monitoring shutdown conditions throughout the plant. Some of the safety significant parameters monitored during shutdown include: RPV water level, reactor coolant temperature, neutron flux, drywell pressure, RHR flow, reactor pressure, and suppression pool temperature and level. In addition to monitoring, signals are also available to actuate ECCS functions on low RPV water level, scram control rods on high flux, and close isolation valves on appropriate signals. Four divisions of instrumentation allow one division of monitoring sensors to be in maintenance without disabling the function, thus assuring availability of instrumentation during shutdown.
	Fuel Pool Cooling System	The Fuel Pool Cooling System (FPC) can be used for DHR under certain conditions during Mode 5 (refueling). See Subsection 19Q.7 and Attachment 19QB for more detail. The pool does not contain drains and includes antisiphon devices to prevent inadvertent drainage. The RHRS can be interconnected to the FPC to aid cooling of fuel in the pool if required.
Reactor Inventory	High Strength Low Pressure Piping	Low pressure piping connected to high pressure piping has been redesigned to a higher pressure rating up to the most remote closed valve and is therefore expected to withstand full reactor pressure on a rupture criteria basis. This minimizes the potential for loss of inventory.
	Interlocked RHR Valves (Mode Switch)	The RPV shutdown cooling suction valve must be fully closed before the suppression pool return or suction valves can be opened. Shutdown cooling suction valve cannot be opened until suppression pool suction and return valves are fully closed. This prevents inadvertent draining of the RPV to the suppression pool. Interlocks are part of mode switch design.
	RPV Isolation Valves	All large diameter [>50A (>2 inches)] isolation valves in the RHR and CUW Systems that connect to the RPV (except injection lines) automatically close on a low RPV water level signal. This reduces potential for the core being uncovered due to an inadvertent RPV drain down event.
	Makeup Control	If RPV level decreases, High Pressure Core Flooder (HPCF), Automatic Depressurization System (ADS), and Low Pressure Flooder (LPFL) Systems initiate automatically. If HPCF and LPFL Systems are in the test mode and a RPV low level signal is received, the systems automatically switch to the vessel injection mode.
	Feedwater, Condensate Booster, and Condensate Pumps	Four electric driven pumps that can be used during shutdown for makeup.

Table 19Q-1 ABWR Features That Minimize Shutdown Risk (Continued)

Category	Feature	Shutdown Risk Capability
	High Pressure/Low Pressure Interlocks	Controls position of RHR valves to ensure that the RHR is not exposed to pressures in excess of its design pressure.
	Makeup Sources	Multiple sources of RPV makeup are potentially available while the plant is shutdown (e.g., main condenser hotwell, condensate storage tank, suppression pool, control rod drive system, AC-independent Water Addition System).
	No Recirculation Piping	Elimination of Recirculation piping external to RPV reduces probability of LOCA both during normal operations and while shutdown.
	RPV Level Indication	Permanently installed RPV water level indication for all modes of shutdown. Redundant sensors use a two-out-of-four logic configuration to ensure high reliability.
Containment Integrity	Containment	Reinforced concrete structure surrounds RPV to withstand LOCA loads and contain radioactive products from potential accidents during hot shutdown. Secondary containment permits isolation and monitoring all potential radioactive leakage from the primary containment.
	Standby Gas Treatment System	Removes and treats contaminated air from the secondary containment following potential accidents.
	Reactor Building Isolation Control	Automatically closes isolation dampers on detection of high radiation. These dampers are potential leakage paths for radioactive materials to the environs following breach of nuclear system barriers or a fuel handling accident.
Electrical Power	3 Diesel Generators	One diesel for each safety division. Independent, both electrically and physically, of each other to minimize common mode failure. Allows for diesel maintenance while still maintaining redundancy.
	Combustion Turbine Generator	Redundant and diverse means of supplying power to safety and non-safety buses in event of loss of offsite power and diesel generator failures.
	2 Sources of Offsite Power	Reduces risk of LOPP due to equipment failure or operator error.
	Electrical Cable Penetrations	Will prevent propagation of fire damage and water from postulated flooding sources.
	4 Divisions of DC Power	Electrically and physically independent. Includes batteries and chargers. Diverse means of electrical power for control circuits and emergency lighting.

Table 19Q-1 ABWR Features That Minimize Shutdown Risk (Continued)

Category	Feature	Shutdown Risk Capability
Flooding Control	Flood Monitoring and Control	Reactor building, control building, RSW pump house, and turbine building flooding is monitored and alarmed in the control room. This alerts the operator to potential flooding during shutdown. Many flood sources (e.g., HVAC, EDG Fuel) are relatively small volume and are self limiting. Operation of the fire water system is alarmed in the control room to help the operator differentiate between a break in the fire water system and the need to extinguish a fire. Larger sources are mitigated by means of, equipment mounted at least 20.32 cm off the floor, floor drains, watertight doors, pump trips, valves closing, or operator actions except at the steam tunnel interface.
	Room Separation	The three divisions of ECCS are physically separated and self contained within flooding resistant walls, floors, and doors. ECCS wall penetrations located below the highest potential flood level in the reactor building first floor corridor will be sealed to prevent water entering the ECCS room from the corridor. No external potential flooding sources are routed through the ECCS rooms and potential flooding sources in other rooms will not overflow into the ECCS rooms and cause damage to ECCS electrical equipment. If ECCS flood barriers must be breached during shutdown, administrative controls ensure that at least one ECCS division is operable and all barriers in that division are maintained intact. RSW pump house divisions are separated into separate flood protected divisions. If RSW flood barriers must be breached during shutdown, administrative controls ensure that at least one RSW division is operable and all barriers in that division are maintained intact.
Reactivity Control	Refueling Interlocks	A system of interlocks that restricts movement of refueling equipment and control rods during refueling to prevent inadvertent criticality. When the mode switch is in the REFUEL position, a fuel assembly cannot be hoisted over the reactor vessel if a control rod is withdrawn. When the mode switch is in the REFUEL mode, only two control rods can be withdrawn at one time, but during fuel handling only one control rod can be withdrawn per Technical Specification requirements.
	Fuel Handling	Fuel handling and storage facilities are designed to prevent inadvertent criticality and to maintain adequate shielding and cooling for spent fuel.
	CRD Supports and Brake	CRD supports limit the travel of a control rod in the event a control rod housing is ruptured. The brake limits the velocity at which a control rod can fall out of the core should a hydraulic scram line break. The internal blowout support prevents rod ejection due to failure of flange bolts or a spool piece. Both of these limit reactivity excursions and thus protect the fuel barrier.

Table 19Q-1 ABWR Features That Minimize Shutdown Risk (Continued)

Category	Feature	Shutdown Risk Capability
	Instrumentation	Reactor Protection System (RPS) high flux (set down) and manual scram functions are operable during shutdown.
Fire Protection	Divisional Separation	The three ECCS divisions are physically separated so that a fire initiated in one division will not propagate to another division. Procedures ensure that during shutdown, if fire barriers between divisions must be breached due to maintenance, at least one division will be available with barriers intact.
	Detection	Fire detection sensors that alarm in the control room are located throughout the plant and operate during shutdown. Actuation of the fire water system is alarmed in the control room. Also, during shutdown more personnel are located throughout the plant to identify, extinguish, and report potential fires.
	Suppression	Water and chemical fire suppression systems are located at appropriate plant locations.
	Water Supplies	Multiple water supplies and both electric and diesel powered fire pumps can deliver water to various locations in the plant during shutdown.
	Data Communication Functions	Eliminates the need for a cable spreading room which is a major fire concern in most plants.
	HVAC	Dual purpose HVAC/SMOKE Control System, divisionally separated, to control individual room pressure and assure clean air path for fire suppression personnel.

Table 19Q-2 Success Criteria for Prevention of Core Damage

System(s)	Comment
1 RHR (SDC) or	All times when available.
Main Condenser or	If available, open MSIVs and establish condensate return path to RPV.
CUW or	If temp 386 K (>234°F) or after 8 days (using 1 pump and using 2 nonregenerative heat exchangers and with regenerative heat exchanger bypassed).
FPC or	Mode 5 only after 10 days. Both pumps and heat exchangers in each system required.
1 Feedwater + 1 Condensate Booster + 1 Condensate or	High pressure injection.
1 HPCF or	High pressure injection.
1 CRD or	High pressure injection (After 1 day shutdown. Prior to one day two pumps required).
1 Condensate or	Low pressure injection (may need ADS).
1 LPFL or	Low pressure injection (may need ADS).
1 AC-Independent Water Addition System	Low pressure injection (may need ADS).

Table 19Q-3 Minimum Sets of Systems for Modes 3 and 4

	RHRB	Main Condenser	CUW	HPCFB	CRD	ADS	RHRB (CF)	Condensate	Fire Water
1)	*				*	*	*		*
2)	*		*			*	*		*
3)	*					*	*	*	*
4)	*	*				*	*		*
5)	*			*	*	*		*	

Table 19Q-4 Minimum Sets of Systems for Mode 5 (Unflooded)†

	RHRB	HPCFB	CRD	RHRB (CF)	Condensate	Fire Water
1)	*		*	*		*
2)	*				*	*
3)	*	*	*		*	

† 2 - 3 days after shutdown

Table 19Q-5 Minimum Sets of Systems for Mode 5 (Flooded)†

	RHRB	FPC	CUW	HPCFB	CRD	RHR (CF)	Condensate	Fire Water
1)	*						*	*
2)	*				*	*		
3)	*			*	*		*	
4)	*					*	*	*
5)‡			*		*			*
6)‡			*				*	*
7)*f*		*			*		*	
8)*f*		*					*	*
9)*f*		*			*			*

† 3 days after shutdown
‡ After 8 days
f After 10 days

Table 19Q-6 Shutdown Vulnerability Evaluation of new ABWR Features

Feature	Shutdown Failure Mode	How Detected	Potential Impact on Safe Shutdown	Preventive/Mitigative Feature	Vulnerability Evaluation
Reactor Internal Pumps (RIPS)	RPV leakage during maintenance	Visual identification of leakage	Inventory loss, fuel uncovery.	Multiple seals, administrative controls, diffuser plug cannot be removed unless RIP motor cover is in place	None, past experience with maintenance on RIPs indicates no concerns.
Combustion Turbine Generator (CTG)	Fails to start or pick up load.	No output voltage on demand or test.	Loss of electrical power redundancy.	Two independent offsite power sources and three Emergency Diesel Generators (EDGs).	None, adequate offsite and onsite power sources exist if CTG were to fail.
	Improper synchronization to existing power sources.	Loss of bus voltage when CTG output breaker closes on demand or test.	Loss of vital power	Two other divisions Capable of supplying vital power, auto synchronization circuit, administrative controls.	None, redundant power supplies and administrative controls/antisync circuit prevent any impact on safe shutdown.
Third EDG	Fail to start or pick up load.	No voltage on vital bus on demand or test.	Loss of power to one bus.	CTG capable of feeding any vital bus, two independent sources of offsite power.	None, increases number of onsite vital bus sources.
Third ECCS Division	Single failure results in loss of third ECCS division.	Safety function not completed (e.g., no ECCS flow given initiation signal) on demand or test.	Loss on one ECCS division.	Two other divisions capable of completing safety function.	None, increases number of ECCS divisions to complete safety functions, allows for ECCS maintenance without total loss of redundancy, separation reduces common mode failure susceptibility.
Micro Processor Based Safety Logic	Fails to initiate safety signal.	ECCS function not completed on demand or during test.	Loss of ECCS function.	High reliability with redundancy and self test feature.	None, increased reliability of ECCS logic.

Table 19Q-6 Shutdown Vulnerability Evaluation of new ABWR Features (Continued)

Feature	Shutdown Failure Mode	How Detected	Potential Impact on Safe Shutdown	Preventive/Mitigative Feature	Vulnerability Evaluation
Fine Motion Control Rod Drives (FMCRDs), Alternate Rod Insertion (ARI)	Fails to control CRD motion on demand.	CRD does not move when directed or spurious movement.	Reduced shutdown margin.	Only two CRDs can be withdrawn at a time, RPS active during shutdown (hi flux or manual trip).	None, adequate preventive mitigative features exist.
Two Independent Preferred Power Sources	Loss of offsite power.	No voltage on bus.	Loss of safety division power sources.	CTG and three EDGs.	None, increased number of onsite and offsite power sources.
Control of System Sensor Interfaces	Loss of control power to ECCS.	ECCS functions not completed on demand or test.	Loss of ECCS function.	Self testing capability, high reliability with redundancy.	None, increased ECCS reliability and elimination of cable spreading room.
Closed Loop Reactor Building Cooling Water System (RCW)	Heat exchanger tube failure.	High temperature on RB equipment, water accumulation in RCW room alarms in control room.	Loss of safety equipment (e.g., RHR heat exchangers).	Redundant heat exchanger can supply necessary cooling.	None, closed loop RCW supplies cleaner water to safety equipment enhancing cooling capability (i.e., reduced fouling of heat transfer surfaces) as compared to direct cooling with service water.
	RCW Isolation Valve failed closed.	High Temperature on RB equipment.	See Heat Exchanger failure.	Three divisions of RCW.	See Heat Exchanger failure.
	RCW pump fails to supply water.	High temperature on RB equipment.	See Heat Exchanger Failure.	Redundant pump can supply necessary flow.	See Heat Exchanger Failure.

Table 19Q-6 Shutdown Vulnerability Evaluation of new ABWR Features (Continued)

Feature	Shutdown Failure Mode	How Detected	Potential Impact on Safe Shutdown	Preventive/Mitigative Feature	Vulnerability Evaluation
High Pressure Nitrogen Gas Supply to ADS and SRVs	Gas leak.	Loss of pressure in accumulators.	Loss of ADS/SRV capability to reduce RPV pressure and allow use of low pressure for Heat Removal (DHD) Systems.	Other high pressure DHR means exist (e.g., HPCF, feedwater/condensate RCIC). Can reduce RPV pressure through use of RCIC.	None, nitrogen supply instead of air reduces potential corrosion of valves and loss of system pressure due to compressor failures. More reliable than air systems.
	Bottle isolated due to valve closure (operator error).	Surveillance test.	See gas leak.	See gas leak.	See gas leak.
Enhanced Remote Shutdown Panel (e.g., 4 SRVs, HPCF)	Transfer and control switches fail to actuate fourth SRV and HPCF.	Safety equipment fails to actuate on demand or during test.	Loss of ability to control fourth SRV and HPCF from the remote shutdown panel.	Three SRV controls exist, local control of equipment is possible.	None, added features enhance shutdown safety.
Enhanced Suppression Pool Temperature Monitoring (64 T/Cs in four divisions instead of 16 in one division)	Fails to detect correct pool temperature.	During operation or test.	Loss of some redundancy in pool temperature monitoring.	None required.	None, enhancement to suppression pool monitoring function.
Suppression Pool Level Monitoring	Fails to detect correct pool level.	During operation or test.	Loss of pool water level monitoring capability.	Local indication.	None, does not perform a safety function.

Figures 19Q-1 through 19Q-22 are not part of the DCD (Refer to Figures A-1 through A-22 in Reference 19Q-1)