NUCLEAR MANAGEMENT AND RESOURCES COUNCIL

1776 Eye Street, N.W. • Suite 300 • Washington, DC 20006-2496
(202) 872-1280

February 1, 1994

Mr. Dennis Crutchfield
Associate Director for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Dear Mr. Crutchfield:

Enclosed for NRC staff consideration is proposed information from the design PRA for the ABWR considered appropriate for inclusion as Chapter 19 of the design control document (DCD). The enclosure is based on Section 19.8 of the ABWR SSAR, "Important Features Identified by the ABWR PRA" (Amendment 33).

The enclosure represents implementation of the industry's recommended approach for incorporation of design PRA information in a DCD. This approach was described in a draft industry paper, "Regulatory Significance of Information Contained in DCDs," forwarded to you on November 8, 1993. This industry paper was prepared in response to NRC staff interest expressed in our meeting of October 12, 1993. The paper delineates the industry's concerns and recommendations on this matter relative to the position indicated in the staff's August 26, 1993, preliminary DCD guidance.

We believe the enclosure is generally consistent with NRC staff statements on this matter prior to issuance of the August 26 preliminary DCD guidance, including the criteria indicated in Enclosure 2 of your letter to William H. Rasin, dated June 20, 1993.

While the enclosure pertains specifically to the ABWR, this material has been coordinated with the other two ALWR plant designers and other members of the NUMARC ALWR Regulation Working Group. We consider the enclosure to provide an apt model for corresponding DCD material for the ABB/CE System 80+, Westinghouse AP600 and GE SBWR.

DD50

	Ltr.	Encl.
NRR/DIR	1	0
NRR/DESA	1	0
NRR/AMSB/ADM	1	1
OC/LFDCB	1	0

We hope to meet with the NRC staff shortly to discuss the industry's recommendations on the appropriate content of PRA information in a DCD. Resolution of this issue will facilitate early submittal of integrated DCDs by the evolutionary plant designers.

We will be contacting you shortly regarding an opportunity to meet with you and others of the NRC staff to discuss this issue in the context of the industry's draft paper and the enclosed material.

Sincerely,

Raymond N. Ng
Manager, Technical Division

RJB/ljw
Enclosure

19 Important Features Identified by the ABWR PRA

Introduction

The ABWR PRA has been reviewed to identify important design features, i.e., those features and actions that contribute significantly to the mitigation or prevention of a particular accident sequence or event scenario. These may be important contributions relating to

- System capability
- Structures, systems, and components denoted by importance measures such as Fussell-Vesely
- Bypass sequences (containment and suppression pool)
- Features identified in SECY 93-087
- How the design meets containment performance goals
- External events
- Shutdown events
- Important core damage sequences
- What keeps core damage frequency (CDF) low
- What has large uncertainty and in the extreme could become a significant contributor to CDF

This section describes the logical process used to identify the important design features and provides the basis for the importance of the feature. These design features are listed in Tables19 - 1 through19 - 7

Logical Process Used to Select Important Design Features

Although each design feature that can prevent or mitigate core damage is important to some degree and should be correctly and fully implemented, there are features that provide a greater degree of protection than others and can be considered more "important." For each initiating event (e.g., flood, fire, LOCA), there are components or features that are more important than others for the prevention or mitigation of the event being evaluated. Where contributions to CDF have been determined by the calculation of Fussell-Vesely or Risk Achievement factors, these parameters can be used to identify the most important features. If the analysis does not result in the calculation of importance measures, other bases are used. For example, a single feature that can fully mitigate or prevent an event by completing its function is more important than features that only contribute to the prevention or mitigation of an event or only partially

control that event. Also, components whose degradation can result in an increase in severity of an event are more important than those components with larger design margins. The specific bases for the selection of features that are considered important within each analysis category is provided with the features selected.

As a final check to ensure that important features were not overlooked, the processes in each area were reviewed by PRA engineers who performed reviews in the other areas and by senior engineering managers with broad system knowledge. This additional review resulted in the addition of a few features and the deletion of others.

It should be recognized that in identifying important features from a PRA perspective, those identified will generally be more important relative to the specific event (i.e., flood, fire, etc.) than to overall core damage. That is, a feature important for flood mitigation will have a lower overall significance than features for mitigating internally initiated events since flooding has a very low contribution to the total core damage frequency.

19.1 Important Features from Level 1 Internal Events Analyses

19.1.1 Summary of Analysis

The ABWR internal events probabilistic risk assessment (PRA) was performed to assess plant vulnerability to potential internal accident sequence initiators. The ABWR Level 1 internal events PRA is based upon detailed fault tree models of the various plant systems as well as event trees which define possible progressions and outcomes of each potential accident initiator. These fault trees and sequences of events are used to estimate core damage frequency due to each potential accident sequence. The sum of the sequence outcomes is the estimate of total internal event core damage frequency.

19.1.2 Logical Process Used to Select Important Design Features

Following completion of the Level 1 internal events PRA, it was systematically reviewed to identify important features. The internal events PRA allows compilations of minimal cutsets leading to core damage as well as importance measures of those components and systems represented as basic events in the models. These results provided one basis for a systematic review to identify important features and capabilities. In the majority of cases, cutsets and importance measures identify "features" at the component level. By reviewing the accident sequences and cutsets resulting from their detailed evaluation, it was possible to identify those systems, features and capabilities which are most important in assuring that the ABWR core damage frequency will be very low. Further insight was gained regarding risk by examining the Fussell-Vesely and Risk Achievement Worth importance measures of the basic components contributing to the performance of each system or feature.

As an example, the first 20 cutsets contribute more than half of the total core damage frequency. Two-thirds of this amount is due to station blackout events, all of which involve failure or unavailability of the Reactor Core Isolation Cooling (RCIC) system. In addition, eight of the twenty basic events of greatest Fussell-Vesely importance belong to RCIC. If the RCIC were not present in the design, the calculated CDF would be an order of magnitude higher. These observations highlight RCIC and its capability to operate without AC power for several hours as important features of the ABWR. They also identify the importance of station battery capability to provide RCIC control power for several hours.

As an additional example, failure of the combustion turbine generator (CTG) is included in each of the station blackout failure sequences and cutsets. It is also among the top twenty in Fussell-Vesely importance. These insights identify the diverse source of emergency power provided by the CTG as an important feature of the ABWR design.

Other systems and features which provide diversity in addition to fulfilling redundant functions were identified and their importance assessed. Following these evaluations important ABWR features and capabilities were identified.

19.1.3 Features Selected

The specific capabilities and features identified as being important to safety are listed in Table 19.1-1. The basis for the selection of each feature or capability is also provided in the table.

RCIC

In the unlikely event that offsite AC power is lost and the three Emergency Diesel Generators and the CTG are not available, the RCIC system can provide core cooling from a diverse power source (reactor steam) for an extended amount of time. RCIC operation for an extended period of time requires that makeup water supply be switched from the CST to the suppression pool. In addition, the station battery capability must be adequate to provide RCIC control power for eight hours. The capability of the RCIC to provide core cooling from a power source diverse from AC provides an order of magnitude reduction in the calculation of the estimated CDF. Sensitivity studies have shown that RCIC operation for two hours provides most of the benefit.

Combustion Turbine Generator

In the unlikely event that offsite AC power is lost and all three EDGs are unavailable, the CTG provides a diverse source of AC power. It is connectable to any of the three safety divisions and is capable of powering one complete set of normal safe shutdown loads. No plant support systems are needed to start or run the CTG. Safety-grade loads are to be added manually after the CTG starts. Although the probability of losing offsite power and all three EDGs at the same time is very small, the consequences of such an event is

potentially very significant. The capability to provide AC power from a diverse source substantially reduces the risk of a loss of offsite power resulting in a station blackout.

High Pressure Core Flooder (HPCF) Logic and Control

The operation of the HPCF is controlled by the digital safety system logic and control (SSLC) system. As identified in SECY 93-087, the common cause failure of digital instrumentation and control logic may result in the failure of redundant equipment. A postulated common cause failure of the SSLC would disable the HPCF without a diverse means to initiate at least one loop of the HPCF. One division of the HPCF has been provided with capability for initiation and operation through an independent and diverse "hard wired" circuit. Although the probability of a common cause failure of the SSLC is very low, an independent and diverse means of HPCF operation further reduces the risk associated with system operation through the multiplexed digital SSLC.

AC-Independent Water Addition (ACIWA) System

The ACIWA provides diverse capability to provide water to the reactor in the event that AC power or the ABWR engineered safety systems are not available. The system has a diesel driven pump with an independent water supply and all needed valves can be accessed and operated manually. In addition, support systems normally required for emergency core cooling systems are not required for ACIWA operation. Even though the ACIWA is not a first line prevention or mitigation system with respect to core damage, it is important in preventing and mitigating severe accidents in the unlikely event all other systems are unavailable.

Reactor Building Cooling Water (RCW) / Reactor Service Water (RSW)

The RCW system and the RSW system are each designed with two parallel loops in each division. Each loop (i.e., 50% of the capacity of each division) is capable of removing all of the component heat loads associated with operation of the ECCS pumps. Together, the two loops in each division are capable of removing heat from the suppression pool through the RHR heat exchangers during LOCA. The parallel loops of RSW and RCW within each division substantially reduce the calculated CDF.

Prevention of Intersystem LOCA

In SECY 90-016 and 93-087 it has been recommended that designers should reduce the possibility of a loss of coolant accident outside containment by designing (to the extent practical) all systems and subsystems connected to the Reactor Coolant System (RCS) to withstand full RCS pressure. All piping systems, major systems components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) which extend outside the primary containment boundary are designed to the extent practicable to an ultimate rupture strength (URS) at least equal to full RCPB pressure. The design provisions provided reduce the possibility of an intersystem loss of coolant accident (ISLOCA) and consequently the probability of a loss of coolant

accident outside the containment being an initiating event that could lead to core damage.

Reactor Protection System (RPS) / Control Rod Drive (CRD) System

The ABWR has a highly reliable and diverse CRD scram system incorporating both hydraulic insert and electric run-in capabilities. The control rod drive system utilizes hydraulic pressure as the principal scram mechanism with electric run in capabilities for backup to the hydraulic scram capabilities. The hydraulic scram system also includes additional backup scram valves to relieve scram air header pressure thereby causing the control rods to insert. Redundant and diverse scram signals are provided from the RPS and Alternate Rod Insertion (ARI) System to the hydraulic scram mechanisms and the electric run-in capability. The RPS is a four division system based on a two-out-of-four initiation logic. The ARI System is two-out-of-three initiation logic based on output signals from the Recirculation Flow Control System. This redundant, and diverse scram capability significantly reduces the probability of an ATWS.

Automatic Standby Liquid Control System (SLCS) and Recirculation Pump Trip

The ABWR has a highly reliable and diverse scram system incorporating both hydraulic and electric run-in capabilities to reduce the probability of an ATWS. In the unlikely event of an ATWS, the standby liquid control system and recirculation pump trip provide backup reactor shutdown capability. Automatic initiation of the SLCS avoids the potential for operator error associated with manual SLCS initiation and further reduces the already low probability of an ATWS leading to core damage.

Three Divisions of Engineered Safety Features (ESF)

There are three independent and separated divisions of ESF, each containing both high and low pressure emergency core injection and decay heat removal systems. Providing three complete divisions of ESF substantially reduces the calculated CDF for events that require ESF. The integrity of divisions is important. The high pressure or high temperature piping lines should not penetrate walls or floors separating two different safety divisions. Piping penetrations are assumed to be qualified to the same differential pressure requirements as the walls or floors they penetrate.

Automatic Depressurization System (ADS)

The Automatic Depressurization System provides a highly reliable means of depressurizing the reactor in the event of failure of the high pressure injection systems. This permits core cooling with low pressure systems, avoids high pressure core melt sequences, and substantially reduces the calculated CDF.

Three Emergency Diesel Generators (EDG)

There are three independent and separated EDGs, one dedicated to each of the three ESF divisions and each capable of powering the complete set of normal safe shutdown loads in its division. This configuration provides redundant sources of emergency AC power as added defense against loss of offsite power events. Three EDGs, each capable

of powering a complete set of normal safe shutdown loads, substantially reduces the calculated CDF for events that require emergency AC power.

Four Divisions of Safety System Logic and Control (SSLC)

There are four divisions of self-tested safety system logic and control (SSLC) instrumentation designed on the basis of two-out-of-four actuation logic. This configuration provides highly reliable initiation of ESF core cooling and heat removal systems as well as actuating the CRD scram system for defense against ATWS events. A four division two-out-of-four SSLC provides protection against inadvertent actuation in addition to assuring the highly reliable actuation capability. This redundancy in the SSLC substantially reduces the calculated CDF for events that require SSLC signals as well as the reduction in unwanted system actuation resulting from inadvertent signals due to spurious inputs, surveillance and maintenance errors, and other causes of single signals.

Each microprocessor-based logic processing unit within the Essential Multiplexing System (EMS) and SSLC undergoes continuous self-test. Undetected faults are identified during periodic (quarterly) surveillance testing, using the operator initiated, offline self-test feature available within each processing unit. This self-test function exercises all programmed logic and also causes outputs to toggle between untripped and tripped states. Faults are logged in each unit's self-test memory and are reported to the operator and process computer. The offline tests are expected to identify any faults not detected by the continuous self-test feature because more logic paths and trip states can be checked with reduced risk of spurious system actuation. This offline testing was judged to be important in the PRA analysis.

The avoidance of the following common-cause failures was also judged important.

(1) It has been assumed that remote multiplexing unit (RMU) miscalibration is not a credible source of EMUX common cause failure.

(2) Propagation of unidentified EMUX faults/failure modes (e.g., an undetected software fault) to other EMUX divisions are assumed to be effectively eliminated as a credible source of EMUX common cause failure. It is also assumed that adequate core cooling will be maintained in the hypothetical event of an entire EMUX system failure.

(3) Maintenance/test errors are assumed to be eliminated as a credible source of EMUX common-cause failure.

In addition, it is assumed that common mode failure of instrumentation is not credible.

HPCF Pumping Capability

For events where core cooling is successful but containment cooling is not the ability of HPCF to pump 171° C (340° F) water is important to ensure adequate core cooling can be maintained for the duration of the transient.

19.2 Important Features from Seismic Analyses

19.2.1 Summary of Analysis

A seismic margins analysis has been performed for the ABWR to calculate a high confidence low probability of failure (HCLPF) acceleration for important accident sequences and classes of accidents. Accidents were compared to an acceptance criteria of 1.67 times SSE.

Two implicit assumptions in the seismic margins analysis are that a seismic event will result in the unavailability of offsite power and the combustion turbine generator (CTG). The ceramic insulators in the switchyard are not tolerant of high seismic loads and therefore are assumed to fail. Also, the CTG is not qualified for seismic loads and is assumed to be unavailable in a seismic event. Therefore, all of the seismic analyses assume that only emergency AC power and DC power are potentially available.

19.2.2 Logical Process Used to Select Important Design Features

The seismic margins analysis did not include the calculation of minimal cutsets which contribute to CDF. Therefore, there was no calculation of importance parameters such as Fussell-Vesely or Risk Achievement. Since importance parameters were not available, two alternate bases were used to select the important features. The first basis used was the identification of the functions and equipment whose failure would result in the shortest path to core damage in terms of the number of failures required and the relative seismic capacities of the components involved. The second basis used was the identification of the most sensitive functions and equipment in terms of the effect on accident sequence and accident class HCLPFs due to potential variations of component seismic capacities. Using these two bases, the seismic margins analysis was systematically reviewed to identify the "important" features.

19.2.3 Features Selected

Table 19 –2 lists the features selected and the rationale for selection. These features met the criteria of either the shortest path to core damage or the most sensitive components.

Shortest Paths to Core Damage

It is assumed that the failure of any Category I structure leads directly to core damage. The structures with lowest HCLPFs are the containment and the reactor building. It is

important that HCLPFs for Category 1 structures not be compromised by future modifications or additions that could affect safety equipment.

Seismic failure of DC power also is assumed to lead directly to core damage. Without DC power, all instrument and equipment control power is lost and the reactor cannot be controlled or depressurized. In the seismic margins analysis it is assumed that this results in a high pressure core melt. The limiting components for DC power are the batteries and the cable trays.

It is possible that a large seismic event could impair the ability to scram due to deformation of the channels that enclose each fuel bundle. In the event that the scram function is impaired, the only means of reactivity control would be the Standby Liquid Control (SLC) System. Seismic failure of the SLC system to insert borated solution into the reactor is controlled by the seismic capacity of the SLC pump and the SLC system boron solution tank.

Emergency AC power and plant service water were both treated as having the same effects in the seismic margins analysis. Failure of either system would require only one additional failure to result in core damage. The limiting components for seismic failure of emergency AC power are the diesel generators, transformers, motor control centers, and circuit breakers. The limiting components for seismic failure of plant service water are the service water pumps, room air conditioners and the service water pump house.

Most Sensitive Components

The HCLPFs of the accident sequences with the lowest HCLPFs could be increased by increasing the individual HCLPFs of the AICWA pumps, the fuel channels, or the RHR heat exchangers. The HCLPFs of the appropriate accident sequences would be increased by an amount equal to the increase in the HCLPF of any of these components.

The only single item that could, by itself, decrease the HCLPF of any accident sequence below the acceptance criteria is a Category I structure having a HCLPF below 1.67 times SSE. This would also decrease the HCLPF of accident class IE; ATWS with high pressure melt due to loss of inventory. There are no Category I structure having a HCLPF of less than 1.67 times SSE.

The only system that could, by itself, result in lowering an accident sequence HCLPF below the acceptance criteria is DC power. DC power has two components that could fail the sequence—the batteries and the cable trays.

AC-Independent Water Addition (ACIWA)

The ACIWA provides a diverse capability to provide water to the reactor in the event that AC power is not available and is important in preventing and mitigating severe accidents. The system has a diesel driven pump with an independent water supply and all needed valves can be accessed and operated manually. In addition, support systems

normally required for ECCS operation are not required to function for ACIWA operation. The ACIWA can provide either vessel injection or drywell spray in the event all AC power is unavailable. Although the system pumps are housed in an external building (shed), the collapse of the building would not prevent the diesel driven pump from starting and running.

Soil Structure Interactions

The potential of seismic-induced soil failure (liquefaction, differential settlement, or slope stability) beyond the SSE level is assumed to be negligible.

19.3 Important Features from Fire Analyses

19.3.1 Summary of Analysis

An ABWR fire risk screening analysis based on the EPRI Fire Induced Vulnerability Evaluation (FIVE) methodology was performed to assess vulnerability to fires within the plant.

19.3.2 Logical Process Used to Select Important Design Features

The screening criterion for EPRI's FIVE methodology provided the primary basis for systematically evaluating important design features. The FIVE methodology provides procedures for identifying fire compartments for evaluation purposes, defining fire ignition frequencies, and performing quantitative screening analyses. The criterion for screening acceptability and dismissal from any more detailed consideration is that the frequency of core damage from any postulated fire be less than 1E-6 per year.

Five bounding fire scenarios and corresponding ignition frequencies were developed on the basis of the FIVE methodology. Each scenario was calculated to have a core damage frequency less than 1E-6 and hence screened from further consideration. Validity of these outcomes is contingent upon specific assumptions regarding the design features and performance capabilities of structures and equipment.

Consequently, the study was systematically reviewed to identify those procedures, assumptions, and features which are necessary in the fire risk assessment analysis to achieve core damage frequencies less than 1E-6 and thus pass the FIVE methodology screen.

19.3.3 Features Selected

Table 19 – 3 lists the features selected and the basis for each feature being considered important. These features are those necessary to maintain fire initiated core damage frequencies below the 1E-6 screening criterion. The proper functioning of these features assures the capability to mitigate the postulated fires. Features identified as a

result of the review of the Level 1 internal events analysis are also important in the fire analysis but they are not included here unless they have some fire unique significance.

Fire Detection and Suppression

The principal function of the Fire Protection System (FPS) is fire detection and suppression. It must be demonstrated that safe shutdown of the ABWR can be achieved, assuming that all equipment in any one fire area has been rendered inoperable by fire and that reentry to the fire area for repairs and for operator action is not possible. Divisional separation is provided by three hour fire barriers to contain the fire within the division. Fire detection systems include infrared sensors as well as product-of-combustion type smoke detectors. Automatic fire suppression systems include foam and sprinklers. Manual fire fighting methods use hand held fire extinguishers and water hoses. Fire detection and suppression systems are provided throughout the plant and FPS actuation is alarmed in the control room. Since the primary containment is inerted during normal plant operation, no FPS system functions are provided in this area.

Remote Shutdown Panel and RCIC and SRV Operation from Outside the Control Room

The dominant contributor to core damage was found to be the potential for a control room fire leading to abandonment of the area and requiring control of the plant from outside the control room. This finding identified the Remote Shutdown Panel as an important feature. The Remote Shutdown Panel provides capability to shut down the reactor that is physically and electrically independent from the control room.

The risk from control room fires is mitigated by providing redundancy for depressurization by providing control for a fourth SRV at the remote shutdown panel and redundancy and diversity for high pressure injection by providing the capability to operate the RCIC system from outside the control room.

Divisional Separation of ESF and Support Systems

Safety divisions, including necessary support systems, are isolated from each other by three hour rated fire barriers. The divisional separation requirement extends to and includes the intake structure. This includes fire barriers formed by concrete fire barrier floors, ceilings, and walls; partitions; rated fire doors; penetration seals for process pipes and cable trays; special assemblies and constructions; and fire dampers. In addition, the fire analysis assumes the routing of piping or cable trays during the detailed design phase will conform with the fire area divisional assignment documented in the fire hazard analysis. This design feature assures that the routing of piping or cable trays will not invalidate the requirement that all safety divisions are separated by three hour fire barriers. Subsection 9A.5.5 under *Special Cases—Fire Separation for Divisional Electrical Systems* lists the only areas of the plant where there is equipment from more than one safety division in a fire area. These should be the only areas where multiple divisions share the same fire area.

Smoke Control System

The EPRI FIVE methodology does not directly address the migration of smoke, and its impact is not explicitly estimated in the fire assessment. However, it is implicit in the analysis that the smoke control system will limit the spread of smoke and hot gasses, and fire suppressant between safety divisions to the extent that damage is limited to equipment in the division in which the fire started. SECY 93-087 and SECY 90-016 identify as important the prevention of the spread of smoke, hot gasses, and fire suppressant from migrating from one division to another to the extent that they cannot adversely affect safe shutdown capabilities, including operator actions. It is assumed in the fire analysis that the smoke control system is capable of preventing the migration of smoke or hot gasses between divisions with an open door between the division experiencing the fire and another division to the extent that they cannot adversely affect safe shutdown capabilities, including operator actions. Since this is an implicit assumption in the FIVE analysis and has been identified as NRC guidance in SECY 90-016 and SECY 93-087 as elements to resolve fire protection concerns, the control of smoke, hot gasses, and fire suppressant is considered an important design feature for fire protection.

If there is a fire in the secondary containment that results in the loss of the HVAC system due to one of the valves at the common HVAC supply or exhaust failing to close, hot gasses will migrate upward in the building through pipe chases and HVAC ducts. Safety-related equipment will continue to operate since they are at the lower levels of the secondary containment and the smoke will migrate away from the lower levels and room coolers will maintain temperature in the subcompartments within acceptable limits. Entrances to the secondary containment are at or near grade, therefore, fire fighting personnel can enter at this level to fight a fire and take any other actions necessary even if one of the common HVAC valves fail to close.

19.4 Important Features from Suppression Pool Bypass and Ex-Containment LOCA Analyses

19.4.1 Summary of Analysis Results

Suppression pool bypass pathways, potential pathways for the release of radioactive material which do not receive the benefits of suppression pool scrubbing, were evaluated. The evaluation included an analysis of the probability of individual bypass pathways existing at the time of a core damage event and the consequence of each path as estimated by the amount of flow accommodated by the pathway. These factors were multiplied to obtain a "bypass fraction" which is a measure of risk.

Ex-containment LOCAs that bypass the suppression pool were evaluated based on simplified event trees.

19.4.2 Logical Process Used to Select Important Design Features

The bypass fraction was used to verify that bypass paths contribute less than 10% of the total offsite risk from internal event sequences and therefore do not present an undue offsite risk. The features that contribute to the prevention or mitigation of containment bypass were systematically reviewed to evaluate their specific contribution to containment bypass. The selection basis used to determine the important features that prevent or mitigate containment bypass was to consider features which, if they were not included in the design, could increase the total bypass fraction above 10% of the total offsite risk.

The core cooling features that could prevent or mitigate containment bypass were systematically reviewed to determine their contribution to total CDF. Those features that would increase the calculated CDF by more than a factor of 2 if they failed or were not included in the design were identified as important features.

19.4.3 Features Selected

Table 19 – 4 lists the features that were identified as important to prevent or mitigate suppression pool bypass events and ex-containment LOCAs. The basis for the selection of the feature is noted in the table.

DW-WW Vacuum Breakers

Assuming an event leads to pressurization of the wetwell to the extent that the containment rupture disk opens, the vacuum breakers would open and then close thereby isolating the drywell from the wetwell. Failure of a DW-WW vacuum breaker to close following the assumed event would provide a significant bypass from the drywell into the wetwell airspace. If the rupture disk is open and one of the vacuum breakers has not closed there would be a direct pathway from the drywell to the wetwell and to the environment.

Redundant MSIVs

There are four main steamlines (MSL), each with two in-series automatic isolation valves. The MSIVs are a pneumatic operated, spring close, fail-closed design actuated by redundant solenoids through two-out-of-four logic. If both MSIVs in any one MSL fail to close there will be a large bypass pathway from the RPV to the Turbine Building. The potential bypass pathway is large compared to other potential bypass pathways. Therefore, the failure of two MSIVs to close in any one steamline would result in a higher consequence from a given postulated event. Although it is extremely unlikely, it is possible that two MSIVs in the same steamline could fail to close and, depending on the event, the failure could result in a substantial offsite dose consequence.

Design and Fabrication of the SRV Discharge Lines

The discharge of the SRVs are piped through the drywell and the wetwell airspace to the suppression pool which is inside the wetwell. To ensure the integrity of the SRV discharge lines, especially in the wetwell region, these lines are designed and fabricated to Quality Group C requirements and the welds in the wetwell region above the surface of the suppression pool are non-destructively examined to the requirements of ASME Section III, Class 2. During an SRV discharge, a break in one of these lines in the wetwell airspace could result in the pressurization of the wetwell and possibly result in the opening of the rupture disk. Although it is extremely unlikely, the failure of the SRV discharge line during operation of the SRV and the subsequent opening of the rupture disk would result in a pathway directly from the RPV to the environment. Depending on the event, the consequence of this postulated sequence could be a substantial increase in the offsite dose consequence.

Normally Closed Sample Lines and Drywell Purge Lines

The sample lines and drywell purge lines are normally closed during plant power operation. Although the valves in the sample and drywell purge lines are normally closed in order to limit the risk of bypass, if one or more of these lines are open when an event initiates a potential bypass path can exist. Depending on the event and the size and number of lines open, a substantial fission product release could result in a significant increase in the consequences of a given event.

Cleanup System Isolation and Connection Elevations

In the event of a break in the CUW system, it is important that the break be isolated. Even though the exposed structures and ECCS equipment are designed for the loads and environment which could follow from an unisolated break, there is some potential for failure. Further, there is some potential for the operator not properly controlling reactor vessel water level during the recovery phase. It is important that the CUW suction line be located approximately 1.8 meters above the top of active fuel and that the RPV drain line connects to the CUW suction line approximately 38 cm above the top of active fuel.

Blowout Panels in the RCIC and CUW Divisional Areas

Blowout panels are provided in the RCIC and CUW divisional areas to prevent overpressurization. Failure of the blowout panels during an ex-containment LOCA due to a break in a RCIC or CUW line could result in the pressurization of a divisional area that could impact equipment in an adjacent area and result in a second electrical division being unavailable. This impacts the core damage frequency for ex-containment LOCAs.

19.5 Important Features from Flooding Analyses

19.5.1 Summary of Analysis

The ABWR flooding analysis evaluated all potential flood sources and through the use of simplified event trees determined the CDF for each building of interest. The three buildings determined to have the potential for flooding to affect safety-related equipment are the Turbine, Control, and Reactor Buildings. The other buildings do not contain safety-related equipment and are not connected to buildings that do. Tunnels from each of these buildings which are routed to the radwaste building are sealed to prevent interbuilding flooding. Therefore, the interbuilding flooding probability through these tunnels was evaluated to be several orders of magnitude lower than direct flooding due to pipe breaks in each building and was not included in the event trees.

19.5.2 Logical Process Used to Select Important Design Features

The ABWR flooding probabilistic risk analysis used simplified event and fault trees to estimate the CDF due to postulated floods. This approach did not result in the calculation of the minimal cutsets which contribute to the CDF. Therefore, there was no calculation of importance parameters such as Fussell-Vesely or Risk Achievement. Therefore, the flooding analysis was systematically reviewed to identify important design features based on other factors. Since importance parameters were not available, the process used to determine the important features was the impact the feature would have on the results of the specific flood in question. If, by completing its function, the component either fully mitigated or prevented the flood or was required to allow some other component to mitigate the flood, then it was selected. Other features, such as sump pumps, that could mitigate some floods but could be backed up by other features were not selected.

19.5.3 Features Selected

Table 19 - 5 lists the features selected and the basis for each feature being considered important. These features met the criteria of either mitigating or preventing flooding or were required to allow some other feature to mitigate flooding.

Physical Separation of the Three Safety Divisions

The three safety division are physically separated by fire rated walls and floors. These walls and floors are also effective flood barriers. Entrances to rooms containing safety-related equipment on the first floor of the reactor and control buildings also have watertight doors. Watertight doors are also on all below-grade entrances to the reactor and control buildings from the service building. Cables penetrating the divisional rooms are sealed to prevent the propagation of fires. These seals are pressure tested and thus also serve as flood barriers.

Floor Drains

The reactor and control buildings are designed to mitigate potential flooding by diverting all flood waters to floors which contain sump pumps by the use of floor drains. The floor drains are sized to handle the largest potential flood source on the upper floors which is the fire protection water system. The floor drains are sized to ensure that water levels on the upper floors will not accumulate to levels high enough to damage important equipment.

Water Level Sensors in the RCW/RSW rooms

Water level sensors are installed in the turbine building condenser pit and the RCW rooms in the control building. These sensors are used to detect flooding in the rooms and send signals to trip pumps and close isolation valves in the affected systems. The sensors are arranged in a two-out-of-four logic. The control building has two sets of sensors (lower and upper) which measure the water level using diverse means to eliminate the potential for common cause failures. The sensors also send signals to the control room to alert the operator to a potential flooding condition so that appropriate manual actions can be taken to isolate the flooding source.

B3F Corridor

The corridor of the Reactor Building first floor has a volume that is sufficient to contain the largest Reactor Building sources which are the suppression pool and condensate storage tank (CST). Penetrations (except for water tight doors) in the divisional walls are at least 2.5 m above the floor level of 8200 mm. The corridor has two sump pumps but the analysis conservatively assumes that the sump pumps do not operate.

Anti-siphon Capability

The reactor service water (RSW) system contains anti-siphon capability (e.g., vacuum breakers, air break) to stop flooding in the event of a break in a RSW line in the reactor component cooling water (RCW) rooms in the control building. The anti-siphon capability will terminate RSW flow if the RSW pumps are tripped but the isolation valves in the affected division fail to close. The anti-siphon capability applies to both the RSW supply and return lines from/to the ultimate heat sink.

Motors and Motor Control Centers

Motors will be drip proof and MCCs will have NEMA Type 4 enclosures.

Ultimate Heat Sink

The ultimate heat sink will be designed such that water cannot gravity drain to the control building in excess of the allowed 4000 meters of RSW pipe from the isolation valves in the pump house (2000 meters each for supply and return).

RSW System

A maximum of 4000 meters of RSW piping is allowed between the RSW isolation valves at the pump house and the control building (2000 meters each for supply and return).

Overfill Lines in B1F Sump

The sumps on floor B1F of the reactor building contain overfill lines that are connected to the first floor of the reactor building (B3F). These overfill lines are designed to direct water to the first floor in the event that the sump pumps fail or cannot keep up with the flood rate. The lines penetrate secondary containment so water loop seals are included to maintain the integrity of the secondary containment.

Floods Originating in Turbine, Control, and Reactor Buildings

The screening analysis indicated that the flooding analysis only needed to address internal flooding from sources in the Turbine, Control, and Reactor Buildings. Other buildings do not contain equipment that can be used to achieve safe shutdown and flooding in those buildings cannot propagate to buildings which contain safe shutdown equipment. Although flooding originating in the Turbine Building could propagate through the Service Building and potentially enter the Control or Reactor Buildings if watertight doors fail or are left open, the analysis does not consider flooding to originate in the Service Building. The analysis addresses the potential for propagating of flooding through the Service Building.

Dogging of Watertight Doors

The flooding analysis assumes that all watertight doors are closed and dogged to prevent floods from propagating from one area to another.

High Pressure or High Temperature Lines Not Routed Across Divisions

The flooding analysis assumes that high pressure or high temperature lines are not routed through floors or walls separating two different safety divisions. Piping penetrations are qualified to the same differential pressure requirements as the walls and floors they penetrate. This prevents the possibility of a system failure in one division from flooding and failing a different division.

19.6. Important Features from Shutdown Events Analyses

19.6.1 Summary of Analysis

A shutdown analysis was completed to evaluate the potential for core damage during shutdown (i.e., Modes 3, 4, and 5). The analysis focused on five areas having potentially high shutdown risk based on past experience with operating plants. The five areas are

(1) Decay heat removal

(2) Inventory control

(3) Containment integrity

(4) Reactivity

(5) Electrical power

Decay heat removal was evaluated probabilistically. The other areas were treated in a qualitative manner. A simplified maintenance model was used to calculate the core damage frequency (CDF) for loss of the operating decay heat removal pump, assuming certain minimum sets of available systems during shutdown. The assumption was that only these minimum sets and support systems were available and other systems were in maintenance. No credit was assumed for these other systems. In practice, not all of these other systems are expected to be in maintenance at the same time.

Several minimum sets were identified which met the CDF criterion. Many other minimum sets could have been evaluated, as well as other system configurations for shutdown conditions. A COL applicant will be able to choose from the configurations evaluated in this study or evaluate other configurations to show compliance to the shutdown CDF criterion.

19.6.2 Logical Process Used to Select Important Design Features

The analysis systematically evaluated potential risks during shutdown. Maintenance activities during shutdown result in more systems being unavailable than during normal operation. The simplified maintenance model assumed many systems were undergoing maintenance at the same time. Since systems are artificially assumed to be out of service and because of the way the analyses were structured, computing importance parameters such as Fussell-Vesely would not result in any meaningful conclusions. Therefore, the shutdown risk study did not lend itself to a quantitative evaluation of the importance of ABWR components for loss of decay heat removal during shutdown.

Since no quantitative measures are calculated to determine the importance of components associated with shutdown risk, the following qualitative basis was used. A component was considered to be important for a specified shutdown risk category if it was capable of preventing or mitigating identified shutdown accident scenarios associated with that category. Using this qualitative basis, the shutdown analysis was systematically reviewed to identify important design features. For example, isolation of the RPV on low water level mitigates loss of inventory control, so it was selected.

19.6.3 Features Selected

Table 19 – 6 lists the features selected as important for each category evaluated along with the reason the feature is important. The list includes both active (e.g., RHR pumps) and passive (e.g., shutdown cooling (SDC) nozzle above TAF) features.

Decay Heat Removal

Three features were selected for events involving loss of decay heat removal: RHR shutdown cooling (SDC), Reactor Service Water (RSW), and the Ultimate Heat Sink (UHS). The RHR system was selected because it is the preferred and normally used

method of decay heat removal during shutdown. The three RHR divisions allow for one division to be in maintenance and a single failure in the operating division. The third division could then be used to cool the core. The RSW and the UHS were selected because of their fundamental support functions for all the decay heat removal systems.

The shutdown study concluded that boiling was an effective, although not preferred, method of decay heat removal for all modes including Mode 5 with the RPV head removed. In this case, injection systems such as HPCF are considered to be decay heat removal systems as they function to keep the core covered. Since these systems are primarily used for inventory control, they are included in that category.

Inventory Control

Four injection systems were selected: RHR(LPFL), CRD, HPCF, and AC-independent water addition (ACIWA). All of these systems are capable of ensuring that the core remains covered. Use of RHR(LPFL) and ACIWA require depressurization if the RPV pressure is high. The other features selected under Inventory Control either prevent or mitigate RPV drain down scenarios. Closure of all valves in lines connected to the RPV on low water level ensures that the core is not uncovered due to breaks in lines connected to the RPV or diversion of water from the RPV by the RHR or CUW systems. The permissives and inhibits associated with the RHR mode switch ensures that the proper valve line up is used for various modes of RHR operation. This minimizes the potential for diversion of water from the RPV. The RHR interlocks ensure that the low pressure RHR piping connected to high pressure systems is not inadvertently exposed to high pressure which could result in a LOCA. RPV level sensors inform the operator of the RPV level and actuate systems such as HPCF and RPV valve isolation to ensure that the core remains covered. A plug installed on the RIP diffuser during maintenance ensures that reactor coolant cannot leak out the RIP housing when the RIP motor, shaft, and bottom cover plate are removed.

Reactivity Control

Three reactivity control features were selected: RPS high flux trip (set down), CRD brake, and refueling interlocks. The RPS high flux trip (set down) protects the core from inadvertent power excursions during shutdown by inserting any withdrawn control rods if the power level reaches a preselected setpoint. The CRD brake prevents ejection of a CRD blade which could result in excessive power and core damage. When in the REFUEL mode, refueling interlocks prevent hoisting another fuel assembly over the RPV if a CRD blade has been removed.

Containment Integrity

Containment integrity during Mode 3 and in part of Mode 4 is preserved by automatic isolation of secondary containment on a high radiation signal. This will prevent or at least delay a potential release of radioactivity to the environs. The standby gas treatment

system (SGTS) can function to process gasses before release to the atmosphere to reduce potential contamination.

Electrical Power

The features selected for electrical power include the three divisions of safety-related power physically and electrically independent, the four sources of onsite power (3 emergency diesel generators (EDGs) and the combustion turbine generator (CTG)), and the two independent offsite power sources. The electrical power systems include redundancy and diversity of sources. This allows some power sources to be in maintenance during shutdown and still have adequate sources to provide power when needed. Even if all offsite power is lost, the four onsite power sources can be used to power any safety or non-safety bus. This means that the ABWR can use alternate sources of decay heat removal (e.g., condensate pump) with only onsite power sources.

19.7 ABWR Features to Mitigate Severe Accidents

The ABWR has been designed to prevent the occurrence of a core damage accident. In the extremely unlikely event of a core damage accident, the ABWR containment has been designed with specific mitigating capabilities. These capabilities not only mitigate the consequences of a severe accident but also address uncertainties in severe accident phenomena. The capabilities are listed below along with a discussion of the specific severe accident phenomena that the mitigation devise is addressing. The severe accident issues addressed are consistent with the issues discussed in SECY 90-016.

AC-Independent Water Addition System

This system not only can play an important role in preventing core damage, it is the primary source of water for flooding the lower drywell should the core become damaged and relocate into the containment. The primary point of injection for the system is the LPFL header inside the vessel. Flow can also be delivered through the drywell spray header to the upper drywell. The drywell spray mode of this system not only provides for debris cooling, but it is capable of directly cooling the upper drywell atmosphere and scrubbing airborne fission products. This system has sufficient capacity to cover the core debris ex-vessel and provide debris cooling and scrub fission products released as a result of continued core-concrete interactions.

The system operating in the drywell spray mode will also reduce the consequences of a suppression pool bypass or containment isolation failure. This is due to the fission product removal function performed by this mode of operation. Fission products will be scrubbed by the sprays prior to leaving the containment.

The system has been sized to optimize the containment pressure response and slow the rate of containment pressurization. The system is capable of delivering water to the containment up to the setpoint pressure of the COPS system. The flow rate, nominally 0.06 m^3/sec at runout and 0.04 m^3/sec at the COPS setpoint, is sufficient to allow

cooling of the core debris, while maximizing the time until the water level reaches the bottom of the vessel, at which point injection is turned off.

Lower Drywell Flooder

The lower drywell flooder system has been included in the ABWR design to provide alternate cavity flooding in the event of core debris discharge from the reactor vessel and failure of the AC-Independent Water Addition System. The thermally activated flooder valves are actuated by the melting of a fusible plug. The temperature set point for the plug is 533 K. The system consists of ten lines located about 4 m below the normal suppression pool water level discharging into the lower drywell about 1 m above the floor. The expected flooder flow is 10.8 kg/s per valve. Only two of the valves are required to open to remove decay heat energy and the energy from zirconium-water reaction and allow for quenching of the debris. The passive flooder will not open until after vessel failure. By flooding after the introduction of core material, the potential for energetic core-water interactions during debris discharge is minimized. The flooder will cover the core debris with water providing for debris cooling and scrubbing any fission products released from the debris due to core-concrete interactions.

Containment Overpressure Protection

The COPS consists of overpressure relief rupture disks mounted in a line which connects the wetwell airspace to the stack. This system will provide for a scrubbed release path in the event that pressure in the containment cannot be maintained below the structural limit. The system includes two reclosable valves which may be used to re-establish containment isolation as a part of post accident recovery. These valves should be normally open and be designed to fail open.

This controlled release will occur at a containment pressure of 0.72 MPa (90 psig). The outer rupture disk of the COPS has a rupture differential pressure of less than 0.03 MPa. The setpoint of the COPS system is based on the competing goals of minimizing the probability of containment structural failure and maximizing the time of any fission product release. The setpoint was assumed to be reliable to within ±5% of the actuation pressure at nominal temperature. The effect of temperature on the rupture disk should be small, the analysis assessed the variability of about 2% per 56 K (100°F).

The area of the rupture disk is designed to permit the COPS system to be effective in mitigating the pressure increase during an ATWS event in which the operator controls the injection flow. The minimum capacity of the COPS is 28 kg/sec steam flow when the containment is at the actuation pressure. This provides ample margin to steam generation rates related to decay heat generation. Analysis of the blowdown of the containment following rupture disk operation indicates that the pool swell and the blowdown loads will not threaten the piping, and that significant entrainment will not occur.

This system is beneficial for several of the severe accident issues. In cases with continued core-concrete attack, or those with no containment heat removal operational, the containment will pressurize. The COPS provides a controlled release path preventing containment structural failure and mitigating fission product release. The COPS system reduces the effect of uncertainties in severe accident behavior, e.g. debris coolability, in the ABWR design.

Vessel Depressurization

The ABWR reactor vessel is designed with a highly reliable depressurization system. The nitrogen supply and battery capacity are sufficient to allow depressurization after RCIC failure during a long-term station blackout. This system plays a major role in preventing core damage. However, even in the event of a severe accident, the RPV depressurization system can prevent the effects of high pressure melt ejection. If the reactor vessel would fail at an elevated pressure, fragmented core debris could be transported into the upper drywell. The resulting heatup of the upper drywell could pressurize and fail the drywell. Parametric analyses indicate that even in the event of direct containment heating, the probability of early drywell failure is low. The RPV depressurization system further decreases the probability of this failure mechanism.

Lower Drywell Design

The details of the lower drywell design are important in the response of the ABWR containment to a severe accident. Seven key features are described below.

(1) Sacrificial Concrete

The floor of the ABWR lower drywell includes a 1.5 meter layer of concrete above the containment liner. This is to ensure that debris will not come in direct contact with the containment boundary upon discharge from the reactor vessel. This added layer of concrete will protect the containment from possible early failure.

(2) Basaltic Concrete

The sacrificial concrete in the lower drywell of the ABWR will be a low gas content concrete. The selection of concrete type is yet another example of how the ABWR design has striven not only to provide severe accident mitigation, but to also address potential uncertainties in severe accident phenomena. Here, the uncertainty is whether or not the ex-vessel core debris can be cooled by flooding the lower drywell. For scenarios in which water in the lower drywell is unable to cool the core debris, the concrete type selected has approximately 4 weight percent calcium carbonate which will result in a very low gas generation rate. This translates into a long time to pressurize the containment. This is important because time is one of the key factors in aerosol removal.

(3) Pedestal

The ABWR pedestal is formed of two concentric steel shells with webbing between them. The space between the shells is filled with concrete. The thickness of the concrete between the shells is 1.64 m. A parametric study of core concrete interaction was performed which indicated a very small potential for pedestal failure even in the event of continued interaction. Furthermore, any potential failure will not occur for approximately one day.

(4) Sump Protection

The lower drywell sumps are protected by corium shields such that core debris will not enter them. This maximizes the upper surface area between the debris and the water and maximizes the potential to quench the core debris. The shields are made of alumina which is impervious to chemical attack from core-concrete interaction. The walls of the floor drain sump shield have channels which permit water flow, but which will not permit debris flow. The equipment drain sump shield has no such channels. The height and depth of the shields has been specified to ensure that debris will not enter the sumps in the long term.

(5) Increased Floor Area

The floor area of the lower drywell has been maximized to improve the potential for debris cooling. The minimum lower drywell floor area is 79 m^2.

(6) Wetwell-Drywell Connecting Vents

The flow area between the lower and upper drywell has been designed in a way to allow adequate venting of gases generated in the lower drywell. The connecting vents flow area is 11.25 m^2. This is important when considering the steam generation rates associated with fuel-coolant-interactions in the lower drywell. The interconnection between the lower drywell and the wetwell is at elevation -4.55 m, 8.6 m above the floor of the suppression pool. Thus, approximately 2.E6 kg of water must be added from outside the containment for the pool to overflow into the lower drywell.

The path from the lower to the upper drywell includes several 90 degree turns. This tortuous path enables core debris to be stripped prior to transport into the upper drywell minimizing the consequences from high pressure melt ejection. Also important when considering high pressure core melt scenarios, the configuration of the connecting vents will result in the transport of some core debris directly into the suppression pool. This is preferable to transport

into the upper drywell and would result in the debris being quenched with only a slight increase in the suppression pool temperature.

(7) Solid Vessel Skirt

The vessel skirt in the ABWR does not have any penetrations which would allow the flow of water from the upper drywell directly to the lower drywell. This, in combination with other design features described above, ensures a very low probability that water is in the lower drywell before the time of vessel failure. Thus, large scale fuel-coolant interactions are precluded.

Inerted Containment

One of the important severe accident consequences is the generation of combustible gasses. Combustion of these gasses could increase the containment temperature and pressure. The ABWR containment will be inerted during operation to minimize the impact from the generation of these gasses.

Containment Isolation

The ABWR containment design has striven to minimize the number of penetrations. This impacts the severe accident response due to a smaller probability of containment isolation failure. All lines which originate in the reactor vessel or the containment have dual barrier protection which is generally obtained by redundant isolation valves. Lines which are considered non-essential in mitigating an accident isolate automatically in response to diverse isolation signals. Lines which may be useful in mitigating an accident have means to detect leakage or breaks and may be isolated should this occur.

Upgraded Low Pressure Piping

The low pressure piping in the ABWR has been upgraded to withstand higher pressure. This reduces the probability of an interfacing system LOCA and the severe accident consequences associated with such an event.

Drywell-Wetwell Vacuum Breakers

The ABWR contains eight vacuum breakers which provide positive position indication in the control room. Failure of the vacuum breakers to close as designed can potentially lead to increased source terms and early containment failure. The vacuum breakers have been located high in the wetwell to reduce potential loads occurring during pool swell. The analysis assumes that the position switch which provides annunciation in the control room can sense a gap between the disk and the seating surface greater than 0.9 cm. Additionally, the vacuum breakers will be tested during periodic outages to ensure operability. The result of the vacuum breaker design in the ABWR is to reduce the potential for suppression pool bypass.

Residual Heat Removal System

The RHR system is the primary mechanism for the removal of decay heat from the containment. This system is capable of pumping saturated water up to the pressure of the COPS setpoint. Recovery of a single loop of RHR is adequate to remove decay heat in the long term. The RHR system also has a drywell spray function which may be important in preventing high temperature failure of the containment in an accident in which debris is entrained to the upper drywell. The wetwell spray may be used to mitigate the effects of suppression pool bypass.

Overall Containment Performance

The design of the ABWR containment provides for holdup and delay for fission product release should the containment integrity be challenged. The design basis containment leak rate is 0.5% per day at containment design pressure. Leakage is expected to be of this magnitude in a severe accident. Long term containment pressurization is governed by the generation of decay heat and non-condensable gases. The primary source of non-condensable gas generation is metal-water reaction of the zirconium in the core. This is accommodated by a relatively large containment volume and a high containment pressure capability. The mitigating systems discussed above ensure that the decay energy results in steam production. The suppression pool absorbs this energy, resulting in very slow containment response which ensures ample time for fission product removal.

The containment strength was evaluated. The limiting structure is the drywell head. Service Level C was found to be greater than 0.77 MPa (97 psig). This is adequate to withstand the generation of 100% metal water reaction. The median ultimate strength of the containment was found to be 1.025 MPa (134 psig). Ultimate strength capability is important for very rapid containment challenges such as direct containment heating and rapid steam generation. Evaluation of both these phenomena indicate early containment failure from these mechanisms is unlikely.

Key Severe Accident Modeling Parameters

Table 19 - 7 provides a list of key severe accident modeling parameters. This list has been derived from the discussions presented above and from a variety of ABWR severe accident evaluations.

Table 19 -1 Important Features from Level 1 Internal Events Analyses

Feature	Basis
Capability to operate RCIC for two hours without AC power, and ability to override switchover to makeup water source from CST to suppression pool. This defines requirement for station battery capability to provide RCIC control power for two hours.	This system with this capability provides the only means available to provide core cooling with the reactor at high pressure and avoid core damage in the event of a station blackout.
Combustion turbine generator connectable to any of the three safety divisions and capable of powering one complete set of normal safe shutdown loads. No plant support systems are needed to start or run the CTG. Safety-grade loads are to be added manually.	Provides a diverse source of emergency AC power as added defense against loss of offsite power and diesel generator failure events.
Operability of one high pressure core flooder (HPCF) loop independent of essential multiplexing system.	Provides an independent and diverse means of initiating emergency core cooling in the event of postulated common mode failures in the digital safety system logic and control (SSLC).
AC-independent Water Addition System, including a dedicated diesel and manually operable valves, to provide a diverse means of low pressure water injection into the reactor vessel.	Provides an independent and diverse means of achieving emergency core cooling in the event of station power loss or failure of the engineered safety features to provide this function.
Sufficient cooling capacity available in the RCW system to provide seal and motor bearing cooling for ECCS core cooling pumps with one RCW and one RSW system pump in each loop in each division and two RCW heat exchangers in each division operating.	The redundant capability in each RCW/RSW division to successfully support ECCS functions substantially lowers the calculated CDF.
All piping systems, major systems components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) which extend outside the primary containment boundary are designed to the extent practicable to an ultimate rupture strength (URS) at least equal to full RCPB pressure.	The designing of interfacing low pressure systems to URS equal to RCPB pressure reduces the possibility of an intersystem loss of coolant accident and consequantly the possibility of a loss of coolant accident outside the containment.
Redundant and diverse CRD scram capability consisting of both hydraulic and electric run-in capabilities with redundant and diverse scram signals from the RPS and ARI logic.	The CRD scram system provides the first line of defense against ATWS events. In addition, the redundancy and diversity incorporated in the CRD scram system significantly reduces the probability of an ATWS.
Automatically initiated standby liquid control (SLC) system and recirculation pump trip to provide backup shutdown capability in event of failure to insert control rods.	The automatic SLC and recirculation pump trip provides backup shutdown capability to the CRDs which substantially reduce the calculated CDF associated with an ATWS event.

Table 19 –1 Important Features from Level 1 Internal Events Analyses (Continued)

Feature	Basis
Three separated divisions of engineered safety features, each containing both high and low pressure emergency core cooling systems as well as the capability to remove decay heat. The integrity of divisions is important. No high pressure or high temperature piping lines should penetrate walls or floors separating two different safety divisions. Piping penetrations should be qualified to the same differential pressure requirements as the walls or floors they penetrate.	The separated divisions of ESF provides three complete divisions of redundant engineered safety features which are the bases for the low calculated CDF of the ABWR.
Automatic Depressurization System to provide access to low pressure core cooling injection systems.	The ADS provides a reliable means of depressurizing the reactor to permit core cooling with low pressure systems in the event high pressure systems fail.
Three emergency diesel generators, one dedicated to each of the three safety divisions and each capable of powering the complete set of normal safe shutdown loads in its division.	The three emergency diesel generators provide redundant sources of emergency AC power as added defense against loss of offsite power events.
Four divisions of self-tested Safety System Logic and Control instrumentation designed on the basis of two out of four actuation logic.	The four division SSLC provides reliable defense against ATWS events as well as reliable initiation of ESF core cooling and heat removal systems.
Miscalibration of the remote multiplying unit (RMU) and test and maintaining errors are effectively eliminated as a credible source of common-cause failures. Propagation of EMUX failures in one division to other EMUX divisions are similarly eliminated. Finally adequate core cooling may be maintained in the hypothetical event of an entire EMUX system failure.	Reduce the potential for common-cause failures to disable safety systems.
HPCF pump capability to pump 171° C (340° F) water.	Insures continued pumping, even if containment pressure increases to the rupture disk setting.

Table 19 -2 Important Features from Seismic Analyses

Feature	Basis
Seismic design of the containment and reactor building and assurance that future modifications or additions to internal structures meet the requirements of Subsection 3.8 if they are made in the vicinity of safety equipment.	Failure of seismic Category I structures could lead directly to core damage because of possible damage to ESF equipment. The Containment and the Reactor Building are the seismic Category I structures with the lowest HCLPFs.
Seismic qualification of the station batteries and cable trays.	DC power is required for all safety-related instrument and equipment control functions. Failure of the DC power system could lead directly to core damage.
Seismic qualification of the emergency AC power system diesel generators, 480V transformers, circuit breakers, and motor control centers.	In a severe seismic event, it is likely that offsite AC power will be lost and emergency AC power will be the only source of AC power. The components in the emergency AC power system with the lowest HCPLFs are the diesel generators, 480V transformers, circuit breakers, and motor control centers.
Seismic qualification of the plant service water system service water pumps, room air conditioners, and pump house.	In a severe seismic event, it is likely that offsite AC power will be lost and emergency AC power will be the only source of AC power. The plant service water system is required for diesel generator cooling and other cooling functions. The components in the service water system most sensitive to a seismic event are the service water pumps, room air conditioners, and pump house.
Seismic qualification of SLC system boron solution tank and SLC pumps.	In a severe seismic event, the ability to insert control rods may be impaired due to seismic deformation of the fuel channels and the SLC system may be the only means of reactivity control. The most sensitive components in the SLC system are the boron solution tank and the SLC pumps.
Seismic qualification of the ACIWA system including the pumps, valves, and water supply. The collapse of the ACIWA building (shed) should not prevent the pumps from starting and running. All needed valves for system operation can be accessed and operated manually.	ACIWA can provide either vessel injection or drywell spray using equipment that does not require AC power. In addition, support systems normally required for ECCS operation are not required for ACIWA operation. ACIWA is an important system in preventing and mitigating severe accidents.

Table 19 -2 Important Features from Seismic Analyses (Continued)

Feature	Basis
Seismic qualification of the RHR heat exchangers.	Seismic failure of RHR heat exchangers could partially drain the suppression pool and flood the RHR rooms. RHR is needed for decay heat removal and water in the suppression pool would provide fission product scrubbing in the event of core damage.

Table 19 -3 Important Features from Fire Protection Analyses

Feature	Basis
Fire detection and suppression systems are provided throughout the plant. Fire suppression systems include hand held fire extinguishers, water hoses, foam and fire sprinklers. FPS actuation is alarmed in the control room.	The use of these systems (not credited in the analysis) will make core damage frequency much less than the screening value of 1E-6.
The Remote Shutdown Panel with the ability to control HPCFB, four SRVs, and two divisions of RHR.	The Remote Shutdown Panel provides an independent alternative means of achieving safe shutdown of the reactor in the event that the control room becomes uninhabitable due to a fire or other event.
The capability to operate the RCIC from outside the control room and the capability to operate four SRVs from the remote shutdown panel.	The capability to operate a redundant and diverse high pressure injection (RCIC) system and the capability to operate a redundant fourth SRV from outside the control room were required to meet the 1E-6 fire risk screening criterion.
Design and maintenance of divisional separation by three hour rated fire barriers of engineered safety features and their support systems including the intake structure (e. g., electrical power and cooling water). Subsection 9A.5.5 under *Special Cases--Fire Separation for Divisional Electrical Systems* lists the only areas of the plant where there is equipment from more than one safety division in a fire area. These should be the only areas where multiple divisions share the same fire area.	The integrity of the divisional fire barrier separation is required to meet the 1.0E-6 fire risk screening criterion. This assures that a fire in one division will not cause equipment in another division to fail because of fire propagation between divisions.
Routing of piping or cable trays during the detailed design phase will conform with the fire area divisional assignment documented in the fire hazard analysis	This design feature assures that the routing of piping or cable trays will not invalidate the requirement that all safety divisions are separated by three hour fire barriers. The integrity of the divisional fire barrier separation is required to meet the 1E-6 fire risk screening criterion.
Design, maintenance and testing of smoke control systems	The prevention of the spread of smoke, hot gasses, and fire suppressant from one fire division to another is implicit in the FIVE analysis as an important requirement to prevent adversely affecting safe shutdown capabilities, including operator actions.

Table 19 –4 Important Features from Suppression Pool Bypass and Ex-Containment LOCA Analyses

Feature	Basis
DW-WW vacuum breakers.	Failure of a DW-WW vacuum breaker to close provides a significant bypass from the drywell into the wetwell airspace following a drywell LOCA or if RPV failure occurs. This bypass pathway can release fission products directly to the atmosphere if high wetwell pressure causes the contain[illegible] rupture disk to open.
Redundant Main Steam Isolation Valves (MSIVs). The MSIVs are pneumatic operated, spring close, fail-closed designs) actuated by redundant solenoids through two-out-of-four logic.	The MSL is very large compared to other bypass pathways and a failure of both MSIVs in one steamline to close would provide a large bypass pathway from the RPV to the turbine building. Therefore, the failure of the MSIVs to close would have a higher consequence from a given postulated event than other bypass pathways.
The SRV discharge lines are designed and fabricated to Quality Group C requirements and the welds in the wetwell region above the surface of the suppression pool are non-destructively examined to the requirements of ASME Section III, Class 2.	A break in one of these lines in the wetwell airspace could cause the containment rupture disk to open and result in a pathway directly from the RPV to the environment.
Normally closed sample lines and drywell purge lines.	If sample lines or purge lines are inadvertently left open a bypass pathway can exist.
Redundant and seismically qualified CUW system isolation valves, qualified to close under postulated break conditions.	Minimize the potential for an ex-containment LOCA to lead to core damage and potential offsite release.
RPV drain line connection to CUW section line is 38.1 cm (15 in) or more above top of active fuel. CUW suction line connection to RPV is 1.52 m (5 ft.) or more above top of active fuel.	Improve the ability of the operator to properly control RPV water level following and unisolated CUW break.
Blowout panels in the RCIC and CUW divisional areas.	Failure of the blowout panels during an ex-containment LOCA due to a break in a RCIC or CUW line could result in the pressurization of these divisional areas that could impact equipment in adjacent areas and result in a second electrical division being unavailable.

Table 19 –5 Important Features from Flooding Analyses

Feature	Basis
Equipment for each safety division is located within compartments designed to prevent water from a flood from propagating from one division to another. This includes features such as watertight doors and sealed cable penetrations.	Assuming a flood has occurred and other mitigation features have failed, this single design feature prevents flooding in one division from affecting another division.
Floor drains in all upper floors of reactor and control buildings.	Assuming a flood has occurred and other mitigation features have failed, this single feature assures that flood waters on upper floors of the reactor and control buildings will flow to lower floors thereby preventing the failure of important equipment on that floor and allow other features on lower floors to mitigate the flood (e.g., sump pumps, watertight doors).
Water level sensors in RCW/RSW rooms and logic in the control building to alert operator and trip RSW pump and close valves in affected RSW division.	Assuming a flood has occurred, the water level sensors and logic are the only automatic features that can identify and terminate flooding in the RCW rooms.
The reactor building corridor on floor B3F is large enough to contain the largest flood sources in the reactor building (condensate storage tank or suppression pool.	Assuming a flood has occurred and other mitigation features have failed, this feature prevents any flood in the reactor building that flows to the corridor from affecting any safe shutdown equipment in the reactor building by isolating the water in the B3F corridor.
Anti-siphon capability in RSW Systems	Anti-siphon capability will prevent a control building flood from continuing to siphon water after the pumps have been stopped. Failure of this capability could increase the chances of some floods leading to core damage.
Reactor Building sumps on floor B1F have overfill lines to the B3F corridor.	Assuming the failure of the sump pumps or a flood that exceeds the capacity of the sump pumps, these overfill lines prevent flood water in one division from propagating to another division. Loop seals are provided to preserve the integrity of the secondary containment.
Buildings other than the Turbine, Control, and Reactor Building do not contain equipment that can be used to achieve safe shutdown and flooding in those buildings cannot propagate to buildings which contain safe shutdown equipment.	The screening analysis indicated that the flooding analysis only needed to address internal flooding from sources in the Turbine, Control, and Reactor Buildings. If this is not the case, the basic flooding analysis could be invalidated.

Table 19 -5 Important Features from Flooding Analyses (Continued)

Feature	Basis
Watertight doors are closed and dogged.	A watertight door must be dogged to assure that it will provide full protection in the event of a flood.
High pressure or high temperature lines not routed through floors or walls separating two different safety divisions.	This single design feature prevents the failure of one division of a system ultimately resulting in the flooding and disabling of a second division.

Table 19 -6 Important Features From Shutdown Events Analyses

Feature	Basis
Decay Heat Removal	
Shutdown cooling (SDC) mode of the RHR system.	RHR(SDC) is capable of both removing decay heat and ensuring that the core is covered with water. SDC is the normally used and preferred method of decay heat removal (DHR) during shutdown.
Reactor service water (RSW) system.	Failure of the RSW system would disable the principal RHR system. The RSW removes heat from the RHR and other systems and transfers it to the ultimate heat sink.
Ultimate heat sink (UHS).	The UHS rejects decay heat to the environment from the RHR/RCW/RSW systems.
Inventory Control	
The low pressure core flood mode of the RHR system.	The low pressure core flood mode of the RHR system can supply makeup to the reactor with the reactor at low pressure.
The CRD system pumps which can supply water to the core through the CRD purge flow.	The CRD system pumps are capable of providing makeup to the reactor at high and low pressures to ensure the core is covered.
High pressure core flooders (HPCF).	The HPCF is capable of providing makeup to the reactor at high and low pressure to ensure the core remains covered.
AC-independent Water Addition (ACIWA) System.	The ACIWA can supply makeup to the reactor with the reactor at low pressure.
RPV Isolation on low water level.	The isolation of lines connected to the RPV on a low water level signal prevent uncovering the fuel for many potential RPV drain down events.
Permissives and inhibits associated with the RHR Mode Switch).	The permissives and inhibits associated with the RHR Mode switch ensures that valve line ups are correct for most RHR functions thereby preventing inadvertent diversion of water from the RPV.
RHR Valve Interlocks.	The RHR valve interlocks prevent low pressure RHR piping connected to high pressure systems from being exposed to high pressures.
RPV Level Indication.	The RPV level instrumentation informs the operator of RPV level and allows automatic initiation of ECCS pumps and closure of RPV isolation valves on low water level.

Table 19 -6 Important Features From Shutdown Events Analyses (Continued)

Feature	Basis
RIP Diffuser Plug	RIP maintenance during shutdown requires a temporary plug be installed in the RIP diffuser when RIP impeller, shaft and motor are removed. The plug is designed so it can not be removed unless the RIP motor housing bottom cover is in place.
Reactivity Control	
RPS High Flux Trip (Set Down).	The RPS high flux trip automatically inserts withdrawn CRDs at a specified flux level to prevent criticality.
CRD Brake.	The brake system on the CRDs prevents ejection of a CRD which could cause criticality.
Refueling Interlocks.	When the reactor Mode switch is placed in the REFUEL position, no fuel assembly can be hoisted over the RPV if a CRD blade has been removed.
Containment Integrity	
Automatic isolation of secondary containment (Modes 3 and 4).	The automatic isolation of the secondary containment on a specified high radiation signal prevents release of radioactivity to the environs.
SGTS.	The SGTS processes gasses before release to the atmosphere.
Electrical Power	
Three physically and electrically independent divisions of safety-related power.	The three divisions of safety-related electric power allows for one division to be in maintenance and still mitigate a single active failure in another division.
Four onsite sources of AC power (three EDGs and one CTG).	The four sources of onsite AC power backs up offsite power and ensures power will be available to safe shutdown equipment.
Two independent offsite sources of AC power).	Redundant offsite power sources allow for the loss of one offsite power source without losing power for decay heat removal during shutdown.

Table 19 -7 Key Severe Accident Parameters

Parameter Description	Value	Relates to What Feature?
Core Power	3926 MW	Containment Performance
El. of Top of Fuel	9.05 m	Containment Performance
Normal Water Level	13.26 m	Containment Performance
ADS Area	0.07 m^2	Vessel Depressurization
Containment Leak Rate	0.5% per day	Containment Performance
Containment Service Level C	0.77 MPa	Containment Performance
Containment Ult. Strength	1.025 MPa	Containment Performance
Total Zr in Core	72,550 kg	Containment Performance
Sacrificial Concrete		
Calcium Carbonate Content	<4 weight percent	Basaltic Concrete
Height of Layer	1.5 m	Sacrificial Concrete
Pedestal Concrete Thickness	1.64 m	Pedestal
Compartment Volume		
Lower Drywell	1860 m^3	Containment Performance
Upper Drywell	5490 m^3	Containment Performance
Wetwell	9585 m^3	Containment Performance
Floor Area		
Lower Drywell	79 m^2	Lower Drywell
Tolerance of Vacuum Breaker Position Switch	0.9 cm	Vacuum Breaker
Overflow Elevation		
LDW to Wetwell	-4.55 m	Lower Drywell
UDW to Wetwell	7.35 m	Lower Drywell
LDW to UDW vent area	11.3 m^2	Connecting Vents
Lower Drywell Flooder		
Elevation	-10.5 m	Lower Drywell Flooder
Area per valve	0.0081 m^2	Lower Drywell Flooder
Plug Melting Temperature	533 K	Lower Drywell Flooder
Suppression Pool Mass	3.6 x 10^6 kg	Containment Performance
COPS		
Equivalent Flow Diameter of Disk	0.2 m (8 in.)	COPS
Diameter of Piping	0.25 m (10 in.)	COPS

Table 19 -7 Key Severe Accident Parameters (Continued)

Parameter Description	Value	Relates to What Feature?
Setpoint	0.72 MPa (90 psig)	COPS
Tolerance at nom. temp.	5%	COPS
Effect of temp. on setpoint	2% per 100 F	COPS
Firewater Addition System		
Injection Locations	Vessel and Drywell	ACIWA
Maximum Flow Rate	0.06 m^3/sec	ACIWA
Minimum Flow rate at COPS Setpoint	0.04 m^3/sec	ACIWA
Oxygen Concentration	<3.5% By Volume	Containment Inerting