GE Nuclear Energy

General Electric Company
175 Curtner Avenue, San Jose, CA 95125

June 2, 1993

Docket No. STN 52-001

Chet Poslusny, Senior Project Manager
Standardization Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of the Nuclear Reactor Regulation

Subject: **Important Features Identified by the ABWR PRA**

Dear Chet:

Attached is the subject paper.

Please provide copies of this transmittal to D. Scaletti, J. Moninger, G. Kelly, and R. Palla.

Sincerely,

Jeffrey C. Bachler for JNF

Jack Fox
Advanced Reactor Programs

cc: J. D. Duncan (GE)
Norman Fletcher (DOE)

JF93-181

A050
1/1

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 Fussel-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; and 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.

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 Fussel-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 it's 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 (CDF on the order of 10^{-9}) will have a lower overall significance than features for mitigating events with a higher contribution to CDF.

IMPORTANT FEATURES FROM LEVEL 1 INTERNAL EVENTS ANALYSES

SUMMARY OF ANALYSIS RESULTS

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. The estimated total CDF for all internal events analyzed is 1.6E-7 per year.

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 cut sets 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, cut sets and importance measures identify "features" at the component level. By reviewing the accident sequences and cut sets 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 Fussel-Veseley 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 cut sets contribute 72 percent 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 Fussel-Veseley importance belong to RCIC. If the RCIC were not present in the design, the calculated CDF would be a factor of 12 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 cut sets. It is also among the top twenty in Fussel-Veseley 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.

FEATURES SELECTED

The specific capabilities and features identified as being important to safety are listed in Table 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. In order to meet station blackout requirements, the RCIC must be able to operate for eight hours without AC power. 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 approximately a factor of 12 reduction in the calculation of the estimated CDF.

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. Although the probability of loosing 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 (SSLC)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 (SLC) 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.

Bus Transfer

The electrical power for the condensate pumps are normally supplied from a non-safety related AC bus. The condensate pumps can be supplied with emergency AC power by transferring power from the safety related bus to the non-safety related bus that powers the condensate pumps. In the event that offsite power has been lost and the ECCS systems are not available, the capability to power the condensate pumps from emergency AC power significantly reduces the calculated CDF for this sequence of events.

Three Division 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.

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, with a fault detection probability of 0.95. Undetected faults are identified during periodic (quarterly) surveillance testing, using

the operator initiated, off-line 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 off-line 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 off-line testing was judged to be important in the PRA analysis.

Many features that are included in the level 1 model were determined to be less important than others in the context of these analyses. Several of these are identified in the following paragraphs.

The capability of the Reactor Water Cleanup (CWU) System to provide an additional means of decay heat removal with the reactor at high pressure was judged to be less important than the features selected as "important features." The additional redundancy provided by this capability does not significantly reduce the calculated ABWR CDF. This is due to the high reliability of other means of decay heat removal such as the various modes of operation of the three RHR loops and the containment overpressure protection system which result in a very small contribution of Class II sequences to total CDF without the CWU capability.

The degree of redundancy in SRVs to perform the ADS function was also judged to be less important than other features. Only three SRVs are required to open to depressurize the reactor so that low pressure pumps can provide the necessary cooling. The eight ADS SRVs plus the remaining ten SRVs that can be manually actuated far exceed redundancy requirements for depressurization. ADS failure is dominated by common cause failure of the ADS valves.

Another feature judged to be less important than other features is the automatic initiation of RHR on suppression pool high temperature. Many hours are available to initiate RHR to remove heat from the suppression pool following transients that dump heat to the suppression pool. The reliability of operators to manually initiate this function when required is judged to be very high, therefore this automatic initiation feature does not significantly reduce the calculated CDF.

The capability to manually initiate scram was judged to be less important than the selected features. The ability to manually initiate scram is not an important feature from the standpoint of CDF due to the highly reliable, redundant, and diverse features of the reactivity control systems.

The capability to use the CRD hydraulic system to provide additional water injection into the core was judged to be less important than the selected features. Credit in some sequences for the coolant injection capability of the CRD pumps is of a lesser importance since adequate core cooling is available from other sources to assure a very low core damage frequency.

It was also judged that the high drywell pressure signal for ADS was less important than the selected features. With the incorporation of the drywell high pressure signal bypass timer, the high drywell pressure signal for ADS is less important.

TABLE 1
IMPORTANT FEATURES FROM
LEVEL 1 INTERNAL EVENTS ANALYSES

FEATURE	BASIS
Capability to operate RCIC for eight 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 eight 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.	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 ABWR 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.

FEATURE	BASIS
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 consequently 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.
The capability to make a bus transfer from a safety bus to a non-safety bus and provide power to the condensate pumps with an emergency diesel generator.	The capability to transfer power from a safety bus to a non-safety bus provides the means to use the condensate pumps for core cooling in the event of the loss of offsite power and thus reduces the calculated CDF in the event of such transients.
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 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.

FEATURE	BASIS
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.
Conduct of quarterly testing of the Essential Multiplexing System and the Safety System Logic and Control System.	This testing is conducted to discover faults that are not identified by the continuous self-test feature. The conduct of the quarterly testing substantially increases the reliability of the Essential Multiplexing System and the Safety System Logic and Control System and the subsequent contribution to the low calculated CDF.

IMPORTANT FEATURES FROM SEISMIC ANALYSES

SUMMARY OF ANALYSIS RESULTS

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. The results of the analysis indicate that all hypothesized accident sequences and all accident classes had HCLPFs equal to or greater than 0.60g. This is twice the 0.30g for SSE. All components in the analysis also had HCLPFs equal to or greater than 0.60g.

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.

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 Fussel-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.

FEATURES SELECTED

Table 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 (HCLPF = 1.11g) and the reactor building (HCLPF = 1.12g).

Seismic failure of DC power also is assumed to lead directly to core damage, whether or not emergency AC power survives. 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 battery racks (HCLPF = 1.13g) and the battery chargers (HCLPF = 0.75g). In sequences where AC power is available, both of these components (batteries and chargers) must fail if core damage is to result.

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 (HCLPF = 0.62g) and the SLC system boron solution tank (HCLPF = 0.62g).

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 failure of all divisions of DC power, which by itself can lead to core damage, or failure to scram could provide the additional failure needed (in addition to failure of AC power or service water) to lead to core damage. The limiting components for seismic failure of emergency AC power are the diesel generators (HCLPF = 0.62g), transformers (HCLPF = 0.62g), motor control centers (HCLPF = 0.62g), and circuit breakers (HCLPF = 0.63g). The limiting components for seismic failure of plant service water are the service water pumps (HCLPF = 0.63g), room air conditioners (HCLPF = 0.62g), and the service water pump house (HCLPF = 0.60g).

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 0.60g is a Category I structure having a HCLPF below 0.60g. This would also decrease the HCLPF of accident class IE; ATWS with high pressure melt due to loss of inventory. The lowest HCLPFs for Category I structures are 1.11g and 1.12g. The only system that could, by itself, result in lowering an accident sequence HCLPF below 0.60g is DC power. DC power has two components that must both fail to fail the sequence - the batteries and battery racks (HCLPF = 1.13g) and the battery charger (HCLPF = 0.75g). No single component could cause the HCLPF of any accident sequence to fall below 0.60g, even if its HCLPF were taken to be zero.

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 for ACIWA operation. The ACIWA is seismic category I and 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 should not prevent the pumps from starting and running.

TABLE 2
IMPORTANT FEATURES
FROM SEISMIC ANALYSES

FEATURE	BASIS
Seismic design of the containment and reactor building.	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, battery racks, and battery chargers.	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, 480 volt transformers, circuit breakers, and motor control centers.	In a large 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, 480 volt 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 large 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.

FEATURE	BASIS
Seismic qualification of SLC system boron solution tank and SLC pumps.	In a large 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 is seismic category I and 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.
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.

IMPORTANT FEATURES FROM FIRE PROTECTION ANALYSES

SUMMARY OF ANALYSIS RESULTS

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. Each scenario evaluated was calculated to have a core damage frequency less than 1E-6.

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.

FEATURES SELECTED

Table 3 lists the features selected and the basis for each feature being considered important. These features are those necessary to maintain fire indicated 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 infared 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 provide 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. Core damage frequency, as initially evaluated by the FIVE methodology, for control room fires was over two orders of magnitude greater than that predicted for a divisional electrical fire, and did not pass the FIVE methodology screening criterion. The Remote Shutdown Panel provides capability to shut down the reactor that is physically and electrically independent from the control room. However, initially the Remote Shutdown Panel had the capability for operating only one loop of high pressure injection (HPCFB) and only three safety relief valves for depressurization. Either the HPCFB or the successful operation of all three SRVs was required to prevent core damage in the event of a fire which led to abandonment of the Control Room.

Potential courses of action to reduce the risk from control room fires included 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. The CDF impact of each of these two options was evaluated by the FIVE methodology. Neither option by itself provided sufficient reduction in the CDF to meet the 1E-6 risk screening criterion. In combination, however, the fire risk screening criterion was met. With the incorporation of both options into the capability of the Remote Shutdown Panel, a CDF of less than 1E-6 was demonstrated for the ABWR.

Divisional Separation of ESF and Support Systems

ABWR fire core damage frequency less than the 1E-6 screening criterion was demonstrated based upon the design feature that 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.

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.

TABLE 3
IMPORTANT FEATURES FROM FIRE PROTECTION ANALYSES

FEATURE	BASIS
Fire detection and suppression systems are provided throughout the plant. Fire detection methods include infared and product-of-combustion. 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 events.
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).	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.

FEATURE	BASIS
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.

IMPORTANT FEATURES FROM SUPPRESSION POOL BYPASS AND EX-CONTAINMENT LOCA ANALYSES

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. The total bypass fraction is 3E-5.

Ex-containment LOCAs that bypass the suppression pool were evaluated based on simplified event trees. The total calculated CDF for these LOCAs is 1E-10.

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. A numerical goal of 8E-4 was established based on comparison of offsite exposures with and without a full suppression pool bypass. 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 the numerical goal.

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.

FEATURES SELECTED

Table 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. The change in the bypass fraction if the feature were to fail is discussed below.

DW-WW Vacuum Breakers

Assuming an event leads to pressurization of the wetwell to the extent that the containment rupture disc 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 disc 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. The consequence of a vacuum breaker failing to close was evaluated in the PRA. The total bypass fraction was calculated to be 3E-1 if a vacuum breaker failed to close.

Redundant MSIVs

There are four 28 inch diameter main steam lines (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 28 inch bypass pathway is large compared to other potential bypass pathways. Therefore, the failure of two MSIVs to close in any one steam line 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 steam line could fail to close and, depending on the event, the failure could result in a substantial offsite dose consequence. The total bypass fraction is calculated to be 1E-1 if failure of two MSIVs occurred.

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 disc. Although it is extremely unlikely, the failure of the SRV discharge line during operation of the SRV and the subsequent opening of the rupture disc 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. The bypass fraction would be about 7E-2 if one of the SRV lines failed resulting in the rupture disc opening.

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. Although manual closure of the sample line valves may be possible, if the valves were open the total bypass is calculated to be 4E-3. If the drywell purge lines were open, the total bypass fraction is calculated to be 2E-3.

Blowout panels in the RCIC and RWCU Divisional Areas

Blowout panels are provided in the RCIC and RWCU divisional areas to prevent overpressurization. Failure of the blowout panels during an ex-containment LOCA due to a break in a RCIC or RWCU 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. If a break in one of these areas caused such an impact, the core damage frequency for bypass events could be increased by a factor of 10.

Several plant features treated in the analysis were judged much less important than those discussed above. These are noted in the following paragraphs.

Piping dimensions are judged to be less important to suppression pool bypass evaluations than other features. The flow split fraction is determined by design dimensions of the plant such as piping size and length. While important in the evaluation of suppression pool bypass, the evaluation was based on conservatively low estimates of bypass path resistance. Consequently these features were not considered important within the context of the final system design. Only much larger piping sizes in identified pathways would be of concern, but significant variations are not considered likely.

The level of water in the suppression pool is considered less important than other features. Higher suppression pool level tends to increase the amount of flow which passes through a bypass pathway because of the increased resistance within the suppression pool path. This characteristic is less important to the results because the flow split fraction varies as the square root of the differential pressure and thus the suppression pool level. Since the suppression pool water level is limited by the return line elevation to 1.6m above the normal level of the suppression pool, the maximum effect on the bypass fraction is about 10%.

The closing of the turbine bypass valve is considered less important than other features. If the MSIVs fail to close in one of the steam lines, the turbine bypass valve would normally be expected to close in response to the Turbine Pressure Control System after RPV pressure has reduced below normal operating pressure. Failure of this valve to close is one component of the definition of the main steamline bypass pathway. The feature is considered relatively unimportant in comparison with the reliability of MSIV closure.

The instrument check valves are also less important than other features. All instruments which sense RPV or containment parameters contain in-line excess flow check valves to limit the release in the event of an instrument line break. However due to their small line size, even if the check valves fail to prevent excess flow, the total bypass fraction from instruments would only contribute about 1.5% of the total bypass fraction. Therefore this feature is considered of lesser importance to the results of the bypass evaluation.

Reliable seating of redundant Feedwater and SLC check valves and ECCS discharge check valves is considered to be of lesser importance than other features that prevent or

mitigate suppression pool bypass. Because of the relatively large line size, failure of the redundant feedwater check valves can lead to a bypass if a break occurs in the feedwater, RWCU or LPFL A return lines, both check valves fail to prevent full reverse flow and core damage occurs. Redundant SLC lines also result in a bypass path if the check valves fail to prevent reverse flow and a piping failure occurs. Failure of LPFL B or C discharge check valves could be significant if a break were to occur in the pump discharge. If all check valves failed to seat, the total bypass fraction could be as high as 3E-5 which is still below the goal. Therefore it can be concluded that the check valves are not important to the bypass evaluation as other features.

TABLE 4
IMPORTANT FEATURES FROM
SUPPRESSION POOL BYPASS AND EX-CONTAINMENT LOCA ANALYSES

FEATURE	BASIS
Reliable closing of a DW-WW vacuum breaker	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 containment rupture disc to open. The consequence of a vacuum breaker failing to close and causing the rupture disc to open was evaluated in the PRA.
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 steam line 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 disc to open and result in a pathway directly from the RPV to the environment.
Normally closed sample lines or drywell purge lines.	If sample lines or purge lines are inadvertently left open a bypass pathway can exist.

FEATURE	BASIS
Blowout panels in the RCIC and RWCU divisional areas.	Failure of the blowout panels during an ex-containment LOCA due to a break in a RCIC or RWCU 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.

IMPORTANT FEATURES FROM FLOODING ANALYSES

SUMMARY OF ANALYSIS RESULTS

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. The CDF for events initiated by flooding in the Turbine Building is 4E-9 per year for a low ultimate heat sink (UHS) and 1E-8 per year for a high UHS. The CDF for events initiated by flooding in the Control Building is 4E-9 per year and the Reactor Building is 3E-9. The estimated CDF for events initiated by flooding from all internal flood sources is less than 2E-8 per reactor year.

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 Fussel-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.

FEATURES SELECTED

Table 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 water tight 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 even if some drains are plugged by debris.

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). For a break in a line to the HPCF, it is possible that the CST would initially drain and then the suction could transfer to the suppression pool. The corridor has two sump pumps but the analysis conservatively assumes that the sump pumps do not operate.

Anti-siphon Valves

The reactor service water (RSW) system contains anti-siphon valves 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 valves will terminate RSW flow if the RSW pumps are tripped but the isolation valves in the affected division fail to close. There is one anti-siphon valve at the discharge of each RSW pump in the ultimate heat sink pump house.

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.

Operator Check Watertight Doors are Dogged

The flooding analysis assumes that all watertight doors are closed and dogged to prevent floods from propagating from one area to another. The watertight doors are alarmed to alert the control room operators that a watertight door is open but will not alarm to indicate that a door is not dogged. To guard against a door being left undogged, operators should check the doors every shift to assure that they are closed and dogged.

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. This prevents the possibility a system failure in one division from flooding and failing a different division.

TABLE 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 pumps 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 and 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 valves in RSW systems.	Anti-siphon valves will prevent a control building flood from continuing to siphon water after the pumps have been stopped. Failure of these valves could increase the chances of some floods leading to core damage.

FEATURE	BASIS
Reactor Building sumps on floor B1F have overfill lines to the B3F corridor. Loop seals are provided on the overfill lines.	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.
Operator check on each shift that 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.

IMPORTANT FEATURES FROM SHUTDOWN EVENTS ANALYSES

SUMMARY OF ANALYSIS RESULTS

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 identified by the NRC in NUREG 1449, "Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States" as having potentially high shutdown risk based on past experience with operating plants. The five areas are: decay heat removal, inventory control, containment integrity, reactivity, and 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 decay heat removal, 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. The CDF calculation was then completed to determine if the minimum set met a conditional CDF of 1E-5.

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.

LOGICAL PROCESS USED TO SELECT IMPORTANT DESIGN FEATURES

The analysis systematically evaluated potential risks during shutdown. Normal 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 Fussel-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" (i.e., the five areas identified in NUREG 1449) 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. The condenser hotwell, while it could be used for makeup during shutdown, was not selected because it will more than likely not be available due to maintenance and other systems such as the Residual Heat Removal (RHR) system in the low pressure core flood mode (LPFL) or high pressure core flooder (HPCF) are typically available for inventory control.

FEATURES SELECTED

Table 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 Reactor Water Cleanup (CUW) System was not selected because it cannot remove all the decay heat by itself until 14 days following shutdown. Even then, two divisions of CUW are required which means that two divisions of RSW and RCW are also required.

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.

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 and prevents withdrawing more than on CRD blade during refueling.

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 gases 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.

TABLE 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.

FEATURE	BASIS
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 all 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.
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 prevent ejection of a CRD which could cause criticality.
Refueling Interlocks	When the reactor Mode switch is placed in the REFUEL position, only one CRD blade can be withdrawn at a time and 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 gases before release to the atmosphere.

FEATURE	BASIS
Electrical Power	
Three physically and electrically independent divisions of safety related power.	The three divisions of safety related electric power allows for one division tc 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.