

19.7 PRA as a Design Tool

In addition to its use as a measurement tool to assess the degree to which PRA-related goals were satisfied as summarized in Section 19.6, the PRA was used to substantially influence the design. During the course of the review of this PRA, the NRC requested that the way in which operating experience was factored into the design and the ways in which the PRA influenced the design be described. This description is provided here.

19.7.1 ABWR Design and Operating Experience

The design of the ABWR covered a period of about 12 years, from 1978 to 1990. The world wide experience of several companies including ABB-Atom, Hitachi, Toshiba, ANM, and GE was used to establish the original design. During the design process, methods were employed to ensure that operating experience was factored into the design. These are summarized in Subsection 1.8.3, particularly Table 1.8-22.

In addition to the general design process noted above, three specific design improvements compared to earlier designs were introduced which provide benefits from a PRA perspective:

- (1) The plant is designed for a safe shutdown earthquake (SSE) of 0.3g. Most operating BWRs have an SSE of 0.2g or less. Thus, the ability to withstand earthquakes is improved. Very large margins are expected at low seismic sites.
- (2) The elimination of recirculation piping has substantially reduced the potential for LOCAs, particularly large LOCAs.
- (3) The use of three separated ECCS divisions, provides the benefits shown in the internal events analysis. In addition, this separation reduces ABWR vulnerability to fires and floods.

19.7.2 Early PRA Studies

PRA studies were used extensively in the early design effort for making design decisions. This has resulted in millions of dollars of cost savings without compromising the plant safety. Several key studies are summarized here.

- (1) Core Cooling Systems

A core cooling system optimization study was performed. This study enabled the core cooling and heat removal functions to be combined and the total number of ECCS divisions to be reduced from 4 to 3, resulting in significant cost savings.

A RCIC reliability study was performed. This study enabled the elimination of one high pressure core cooling system by upgrading the RCIC System's reliability.

A risk comparison study was performed. This compared the core damage frequency for BWR/4, 5, and, 6 plants with the ABWR and identified the importance of modifying the ADS logic to initiate on low water level. This change improved the ABWR safety significantly for transient event sequences.

(2) Reactivity Control

Studies of ABWR scram system reliability and scram system unavailability with alternate rod insertion enabled the incorporation of a less expensive ATWS mitigation system in place of an alternate system proposed for an earlier design. This change also results in significant cost savings.

(3) Instrumentation Studies

An ABWR instrument reduction study and reliability assessment enabled the elimination of 60% of the sensor instrumentation in the reactor safety systems without impacting plant safety. Other studies performed have identified significant cost reductions in the ABWR data communication and instrumentation systems.

(4) Control Rod Drive Improvements

The early ABWR ATWS design was based on utilizing the capabilities of the new fine motion control rod drives (FMCRD) to meet the intent of USNRC ATWS Rule 10CFR50.62 for improvement of hydraulic scram reliability. Adoption of the FMCRDs provided improved scram reliability by elimination of the scram discharge volume, which is a potential common mode failure point for current BWRs using the locking piston-type CRDs. The scram reliability goals were met without use of the Alternate Rod Insertion (ARI) valves specified in 10CFR50.62. However, subsequent PRA studies showed that adoption of the ARI valves in the design would provide a further substantial reduction in the probability of ATWS. Since the cost of adding the ARI valves to the design at that time was minor, it was decided that their incorporation into the design was appropriate.

The FMCRD brake mechanism is provided to prevent a rod ejection in the event of a break of the scram insert line. As a result of PRA studies, the design was changed from the centrifugal-type brake used in the early design to the current electro-mechanical-type brake. The PRA studies indicated that the brake design had to be fully testable on a refueling cycle basis to meet the goals for rod ejection frequency. It was determined that the electro-mechanical brake design was easier to test, and would not have any impact on the plant outage critical path.

(5) RIP Trip Study

The reliability of RIP power supply was evaluated. The probability of simultaneous trip of all RIPs was calculated. The objective of this study was to assure that the

probability of an all RIP trip event is low enough to classify such an event as an accident. The study confirmed the 4-bus configuration for the RIP power supply. In addition, motor generator sets were adopted to prevent an all RIP trip event from occurring following a loss of AC power.

19.7.3 PRA Studies During the Certification Effort

As part of the ABWR certification effort, the PRA was further used to improve the design. This effort was first reported in the 1991 Probabilistic Safety Assessment and Management Conference. An AC-independent Water Addition System and a combustion turbine generator were added to reduce the probability of core damage. A lower drywell flooders and a containment over pressure protection system were added to mitigate the effects of core damage in the unlikely event that such damage should occur. The studies which lead to these and other improvements are summarized here.

(1) Initial Probabilistic Risk Assessment

The initial PRA effort for ABWR Certification indicated that the ABWR had abundant means of preventing severe accidents and mitigating their consequences and that the goals (Section 19.6) could be satisfied. However, key insights gained from this effort led to the selection of additional features as described in the following paragraphs.

The core damage frequency from internal events was determined to be extremely small. Although this result was very favorable, the core damage frequency was dominated by station blackout. A simple, “AC-independent water addition system” was added to the design. The cost impact is quite small since only a few small lines and manually operated valves are added. A combustion turbine generator, required by the Electric Power Research Institute Advanced Light Water Reactor Requirements Program was also added to the design. These features significantly decreased the frequency of core damage due to station blackout. As compared to current plants the frequency of these events is extremely low.

In other evaluations, it was determined that if molten core material were present in the lower drywell, it would ablate the reactor vessel pedestal in the region of the wetwell/drywell vents, allowing suppression pool water to enter the lower drywell. This would quench the corium and terminate core-concrete interaction, non-condensable gas generation, and drywell atmosphere heatup; all favorable effects which lessen the potential to fail the containment function. However, it did not seem prudent to take favorable credit for a rather uncertain process. Earlier conceptual studies had identified the concept of a “passive drywell flooders” which could be relied on with much greater certainty to produce the desired favorable effects.

The drywell head was found to be the most probable failure location should the containment be pressurized to a point well above the design pressure. If such an unlikely failure were to occur, fission products could be released without the benefit of suppression pool scrubbing. Fission product retention in BWR suppression pools has been found to be very beneficial in reducing the amount of fission products released from the containment. Even before specific numerical calculations had been performed, the potential benefits of a device that would relieve containment pressure through the suppression pool were apparent. Therefore, a containment overpressure relief feature was added to the design to accomplish this function.

Examination of dominant severe accident sequences indicated several areas in which the Emergency Procedure Guidelines or plant operating procedures could be improved for the ABWR. Prevention of accidents can be improved in seismic initiated loss of offsite power events by instructing the operator to manually operate heat removal system valves if transformer loss has made power operation of those valves impossible. Accident mitigation can be improved for the ABWR accident sequences in which corium has penetrated the reactor vessel by filling the drywell with water to the level of the bottom of the reactor vessel, rather than to the top of the active fuel as done for earlier BWRs.

(2) Feature Descriptions and Resulting Benefits

As a result of the studies summarized above, four new features were added to the design to enhance the plant's performance under severe accident conditions. The added features are described in the following paragraphs.

(a) AC-Independent Water Addition

Two fire protection system pumps are provided on the ABWR: one pump is powered by AC power, the other is driven directly by a diesel engine. A fire truck can provide a backup water source. One of the fire protection standpipes is cross-connected to the RHR injection line to the reactor vessel through normally closed, manually operated valves. From this line, fire protection water can be directed to the reactor vessel after the reactor vessel has been depressurized. Fire protection water can also be directed to the drywell spray header to reduce upper drywell pressure and temperature. Should drywell head failure occur (an extremely unlikely event, especially given the containment overpressure protection feature discussed below), use of drywell spray also reduces the release of volatile fission products from the containment.

(b) Combustion Turbine Generator

A combustion turbine generator (CTG) starts automatically. It is automatically loaded with selected investment protection loads. Safety-grade loads can be

added manually. This provides diverse power if none of the three safety-grade diesel generators are available.

The CTG is a standby non-safety power source to feed plant investment protection loads during loss-of-offsite power events. It is not seismically qualified. The unit also provides an alternate AC power source in case of a station blackout event.

The CTG is designed to supply standby power to the three turbine building (non-Class 1E) 4.16 kV buses which carry the plant investment protection loads. The CTG automatically starts on detection of a 30% voltage drop on the 4.16kV bus. The 4.16kV bus is tripped and the CTG sequentially assumes the loads.

CTG failure will not affect safe shutdown of the plant. The unit is not required for safety but is provided to assist in mitigating the consequences of a station blackout event.

The CTG can supply power to nuclear safety-related equipment if there is complete failure of the emergency diesel generators and all offsite power. Under this condition, the CTG can provide emergency backup power through manually-actuated Class-1E breakers in the same manner as the offsite power sources. This provides a diverse source of onsite AC power.

(c) Lower Drywell Flooder

The lower drywell flooder allows water from the suppression pool to enter the lower drywell during severe accidents where core melting and subsequent vessel failure occur. Several pipes run from the vertical pedestal vents into the lower drywell. Each pipe contains a fusible plug valve connected by a flange to the end of the pipe that extends into the lower drywell. In the unlikely event that molten corium flows to the lower drywell floor and is not covered with water, the lower drywell atmosphere will rapidly heat up. The fusible plug valves open when the drywell atmosphere (and the fusible plug valve) temperature reaches 260°C (500 F). The fusible plug valve is mounted in the vertical position, with the fusible metal facing downward, to facilitate the opening of the valve when the fusible metal melting temperature is reached. When the fusible plug valves open, suppression pool water will be supplied through pipes to the lower drywell to quench the corium, cover the corium, and remove corium decay heat. The result will be a reduced interaction between corium and drywell floor concrete which, in turn, will reduce drywell temperature and pressure from non-condensable gas generation. There will be less chance of overpressurizing the containment and causing radionuclide

leakage to the atmosphere. The lower drywell flooder is a passive injection system. No operator action is required.

(d) Containment Overpressure Protection System

If an accident occurs which increases containment pressure to a point where containment integrity is threatened, the pressure will be relieved to the atmosphere by a line connecting the wetwell to the plant stack. Providing a relief path from the wetwell vaporspace precludes an uncontrolled containment failure. Directing the flow to the stack provides a monitored, elevated release. The relief line, designed for 1.136 MPa, contains a rupture disk which opens at a pressure above the design pressure but below the Service Level C capability of the containment. The relief line also includes a second rupture disk, set at a very low value. This allows the discharge path to be inerted. If overpressure occurs, the rupture disks will open and pressure is relieved in a manner that forces escaping fission products to pass through the suppression pool. Relieving pressure from the wetwell, as opposed to the drywell, takes advantage of the fission product scrubbing provided by the suppression pool. After the containment pressure has been reduced and normal containment heat removal capability has been regained, the operator can close two normally open air-operated valves in the relief path to reestablish containment integrity. Initiation of the pressure relief system is totally passive. No power is required for initiation or operation of the pressure relief function.

(e) Seismic Capability of Added Features

After the above added design features were further developed, additional PRA studies were performed focusing on seismically-initiated events. The combustion turbine generator is not seismically qualified so no credit was taken for its operation in the analysis. The other three features have relatively high seismic capacities. The AC-independent water addition system including the direct diesel-driven pump and the associated piping and manual valves have a seismic HCLPF of 0.5g. The lower drywell flooder is virtually invulnerable to a seismically induced failure (pipes and valves whose likely failure mode would probably introduce water to the lower drywell). The overpressure protection system is Seismic Category I, and a seismically-induced failure is not likely to prevent the relief function provided by the rupture disks.

(3) Emergency Procedure Guideline Improvements

Emergency Procedure Guidelines (EPGs) were improved in several areas. Two examples are described here.

(a) Accident Prevention

In a high fraction of seismically initiated station blackout sequences, diesel generators are available to supply power to pumps in the heat removal system but lower voltage power necessary for operation of MOVs may not be available because of transformer failure. The transformer seismic capacity is less than that of the EDGs. However, the necessary valves can be operated manually and this capability will be reflected in the detailed procedures to be developed to supplement the EPGs.

(b) Accident Mitigation

EPGs developed for earlier BWRs call for the operator to fill the containment to the level of the top of the active fuel if the reactor vessel water level cannot be determined or cannot be maintained above the top of the active fuel. For an ABWR plant which has undergone a severe accident, this strategy can be improved. Filling the containment to a lower level than the TAF is appropriate for two reasons. First, noncondensable gases in the containment are compressed to a lesser degree and containment pressure is reduced compared to the earlier strategy. Second, filling the containment to a lower level avoids flooding the containment overpressure protection system and the potential for subsequent damage to system piping if the rupture disk setpoint pressure is reached. Therefore, the operator is directed to fill the containment to the level of the bottom of the reactor vessel. In the very long term, for post accident recovery and cleanup operations, it would probably be necessary to increase containment water level to an elevation above the top of the active fuel.

In the process of preparing the PRA, human actions were summarized and sensitivity studies were performed. An overview of this process is provided in Section 19.11.

(4) Further Improvements

Subsequent to the above described improvements, several other improvements were identified and incorporated into the design.

The pressure capability of the drywell head was enhanced to increase the containment pressure capability. Basaltic concrete was added to the lower drywell cavity floor to reduce the potential for non-condensable gas generation which could result if core damage occurs.

As a result of the fire PRA studies (Appendix 19M), the capability of controlling automatic depressurization of the RPV from the remote shutdown panel was improved.

Based on studies of the potential effects of failures in Safety System Logic and Control, surveillance testing of microprocessor-based controllers was increased in

frequency to quarterly to improve the ability to detect failures which are not detected by the continuous self-test feature.

As a result of the internal flood PRA studies, several improvements or additional design details were developed to reduce the potential for internal flooding to pose a significant threat. These additional features, which are shown in Table 19R-7, include the following:

- condenser bay water level sensors to terminate serious flooding in the turbine building;
- control building floor water level sensors to terminate major potential flooding sources;
- and floor drains, sump overflow lines, and water tight doors in the reactor building and reactor service water pump house to prevent floods from having significant impact.

Based on a detailed PRA evaluation of a reactor water clean up (CUW) system pipe break outside primary containment, a remote manual shutoff valve was added to the system. This valve is located upstream of the inside containment CUW isolation valve and is intended to terminate outside containment CUW line breaks if the two automatic isolation valves fail to close following a line break. The operator can close the valve from the control room. This valve reduces the probability that the operator would have to control RPV water level lower than the normal range for postulated CUW line breaks.

Consideration of severe accident phenomena indicated the ability to cool the core debris in the lower drywell could be compromised if a significant debris mass were to enter the containment sumps. If the core debris were not quenched, continued core concrete interaction with its resultant noncondensable gas generation could lead to containment pressurization even with successful containment heat removal. To prevent this possibility, a protective barrier around the sumps was added to the design. This barrier prevents the intrusion of molten debris into the containment sumps in the event of a severe accident while allowing water to enter the sumps during normal operation.

Several key safety functions, previously performed manually, were automated.

(5) Summary

Probabilistic Risk Assessment studies conducted for the Advanced Boiling Water Reactor during the certification effort provided valuable insights to plant performance under transient and accident conditions. Although the studies indicated that the established safety goals could be satisfied, an AC-independent water addition

system and a combustion turbine generator were added to the design to substantially reduce the probability of a sequence of events which lead to core damage. To reduce the potential consequences of a core damage event, should one occur, a passive means of flooding the drywell with water and a passive containment over pressure relief system were added to the design. EPGs were also improved to further enhance the capability to prevent accidents from occurring and to mitigate subsequent consequences.

The studies discussed above were conducted by examining the plant design and operation from many different perspectives and thus are judged to constitute a thorough search for design and procedure “vulnerabilities.” No prescriptive attempt was made to define the term vulnerabilities in this context. It was judged the better approach to give engineers experienced in many disciplines a wide latitude in identifying potential weaknesses and then dealing with each issue as it was raised case by case.

19.7.4 Conduct of the PRA Evaluations

The PRA for the original ABWR certification was conducted in accordance with the Key Assumptions and Groundrules developed under the Advanced Light Water Reactor Program. This document was developed with input from many individuals experienced in PRA.

PRA models consisted of fault trees and event trees as described in the “PRA Procedures Guide”, NUREG/CR-2300. Detailed plant models included plant systems and equipment and dependencies arising from common cause failure, human error and support system failure, thus enabling potential vulnerabilities to be identified.

19.7.5 Evaluation of Potential Design Improvements

PRA techniques were used in the evaluation of whether there are additional potential design modifications which would be cost-beneficial to implement and in the technical support of the evaluation of Severe Accident Mitigation Design Alternatives (SAMDA) for compliance with the National Environmental Protection Act (NEPA). Evaluations used the PRA event trees as a guide for estimating conservative benefits from a variety of potential modifications.