



UNITED STATES  
 NUCLEAR REGULATORY COMMISSION  
 WASHINGTON, D. C. 20555

May 5, 1992

NOTE TO: Jack Duncan, GE  
 FROM: Glenn Kelly, NRR, DREP, PRA *Glenn Kelly*  
 SUBJECT: CLARIFICATION OF NRC REQUEST AND GE COMMITMENT TO PROVIDE WRITE UP  
 TO THE STAFF OF ABWR PRA DESIGN INSIGHTS

During a conference call May 4, 1992, you indicated that you would like to confirm what the staff requested regarding a write up on PRA design insights. At the March meeting between the staff and GE in San Jose, the staff requested that GE provide a discussion of PRA design insights from the ABWR PRA. GE verbally indicated it would provide such a write up. In particular, the staff mentioned the following areas:

- What is the PRA telling us about the ABWR design?
- How was the PRA used to identify potential vulnerabilities and which, if any, were found?
- What is the balance between prevention and mitigation in the ABWR?
- How is the PRA used in RAP?
- How is the PRA used in shutdown risk?
- What does the PRA tell us about what needs to go into ITAAC?
- How is the human error analysis to be included into the control room DAC?
- Compare ABWR vs. BWR dominant sequences and why they go away

I hope this list is helpful to you in responding to staff's request. If you have any questions on this list, please call me.

Introduction for Parts A and B of the ABWR PRA FSER

- \* PRA uses during and beyond Design Certification (An overview of PRA objectives and uses during Certification, preoperation, and operation).
- \* Criteria used to judge acceptability of ALWR Design PRAs in contrast to traditional PRA reviews. (a general discussion)
- \* Road map of PRA relationship with current licensing and future operational activities

Part A: PRA-Based Design Evaluation Insights

A.1: Introduction and Executive Summary

(Special design features that reduce CDF and risk, vulnerabilities, balance of prevention and mitigation, and design robustness)

A.2: ABWR Risk Profile Insights

A.2.1: Level 1 (Internal Events)

A.2.1.1: CDF Leading Sequences (an overview and comparison with operating BWRs with a description of ABWR design features that reduce CDF)

A.2.1.2: Human Error contribution to Risk (comparisons with Operating BWRs PRAs)

A.2.1.3: Insights from uncertainty, sensitivity, and importance analyses.

A.2.1.4: Conclusion (Design Robustness)

A.2.2: Level 2 (Internal Events)

A.2.2.1: Characterization of phenomena challenging Containment Integrity.  
(an overview and comparison with operating BWR PRAs, Discussion of special features of ABWR design)

A.2.2.2: Insights from sensitivity and uncertainty Analyses

- A.2.2.3: Conclusion  
(Design robustness and mitigative features influencing risk)
- A.2.3: Level 3 Consequence Analyses  
(General Overview and discussion of results)
- A.3: External Events Insights  
(Insights about design robustness and risk reducing features in ABWR design as compared to operating BWRs. Discussion of special design features and improvements influencing risk)
  - A.3.1: Seismic
  - A.3.2: Internal Floods
  - A.3.3: Fires
  - A.3.4: Others
- A.4: Shutdown operation:  
(Discussion of design features reducing shutdown risk)
- A.5: Use of PRA by GE in Designing the ABWR
- A.6: PRA Applications
  - A.6.1: DAC/ITAAC and PRA
    - A.6.1.1: Road Map for PRA use
    - A.6.1.2: Examples and General Discussions
  - A.6.2: PRA and the Reliability Assurance Program (Reliability Targets, importance analyses results, living PRA..etc)
  - A.6.3: Severe Accident closure (SAMDA, A/M)
    - A.6.3.1 SAMDAs  
(Discussion/results of GE & staff evaluation of SAMDAs for ABWR)
    - A.6.3.2 Accident Management  
(Discussion of approach to A/M for ABWR, and manner in which each element will be addressed)
- A.7: Conclusion & Overview

Part B:

PRA Quality

(an update of the old Ch. 19 Probabilistic Risk Assessment)

May 5, 1992

NOTE TO: Chet Poslusny  
FROM: Glenn Kelly *GJK*  
SUBJECT: RECEIPT OF FAX FROM GE ON ABWR PRA

Enclosed please find a copy of a fax sent to me on April 7, 1992 by Jack Duncan, GE that provides a proposed write up for "PRA as a Design tool".

Enclosure: as stated

9205190271 920505  
PDR TQPRP EMVGENE  
C PDR





504-1075

GE Nuclear Energy

ABWR

Date 7 APRIL 92

To GLEN KELLY NRC

Fax No. \_\_\_\_\_

This page plus 7 page(s)

From JACK DUNCAN

Code \_\_\_\_\_  
1 Curtner Avenue  
San Jose, CA 95125

Phone (408) 925-6947

FAX (408) 925-1193  
or (408) 925-1687

Subject PPA AS A OPTION TOUR

Message 7 PAGE DRAFT FOLLOWS

LET ME KNOW WHAT

YOU THINK

## PRA AS A DESIGN TOOL — DRAFT

Note: This would go in the main Chapter 19 report after measurement against goals material.

### 19.6.10 Probabilistic Risk Assessment Use as a Design Tool

In addition to its use as a measurement tool to assess the degree to which PRA related goals were satisfied, 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.

#### 19.6.10.1 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, ANM and GE was used to establish the original design. The K6/K7 project followed that effort embracing in more detail the experience of TEPCO, General Electric, Hitachi and Toshiba.

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.

#### 19.6.10.2 Early PRA Studies

PRAs 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 CCS 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 reliability.

A BWR 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

Two studies, namely, 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 alternate 4A 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 multiplexing systems and other 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 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 an annual 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.

### 19.6.10.9 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 floodler 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 ABWR had abundant means of preventing severe accidents and mitigating their consequences and that the goals 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 about one event per million reactor years of operation. 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 virtually eliminate station blackout as a contributor to core damage, decreasing the frequency by an order of magnitude.

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 flooder" which could be relied on with much greater uncertainty to produce the desired favorable effects. Since this was a low cost system (several pipes and thermally activated valves) it was added to the ABWR design.

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 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 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 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 RTR 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 on-site nonsafety power source to feed permanent nonsafety 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) 6.9 kV buses which carry the plant investment protection loads. The CTG automatically starts on detection of a voltage drop to about 70% on its downstream bus. When the CTG is ready to synchronize it automatically assumes the 6.9 kV bus 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. However, the plant can cope with a station blackout without the CTG.

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 floods the lower drywell with water from the suppression pool 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 heatup. The fusible plug valves open when the drywell atmosphere (and subsequently the fusible plug valve) temperature reaches 260°C. 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 the system to the lower drywell to quench the corium, cover the corium and remove corium decay heat. The result will be a reduced drywell temperature and pressure from noncondensable gas generation. There will be less chance of overpressurizing the containment and increasing leakage. 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, this pressure will be relieved through a line connected to the wetwell atmosphere, by relieving the wetwell atmosphere to the plant stack. Providing a relief path from the wetwell airspace precludes an uncontrolled containment failure. Directing the flow to the stack provides a monitored, elevated release. The relief line, designed for 150 psig, contains two rupture disks, in series, which open at a pressure above the design pressure but below the Service Level C capability of the containment. 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 decontamination factor 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 for an indefinite period.

#### (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 operation in the analysis. The other three features have relatively high seismic capacities. The ac-independent water addition system is seismic Category I and has three pumping sources: ac-driven pump, direct diesel-driven pump and a fire truck. The balance of the system consists of pipes and manually operated valves which have relatively high seismic capacity compared to many components in conventional safety systems. 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 its failure should not 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 for necessary valves operation is not available because of transformer failure. The transformer seismic capacity is less than that of the diesels. However, the necessary valves can be operated manually under many of these conditions, and this capability will be reflected in the detailed procedures to be developed from the EPGs.

#### (b) Accident Mitigation

EPGs developed for earlier BWRs call for the operator to fill the containment to the level 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 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 clean-up operations, it would probably be necessary to increase containment water level to an elevation above the top of the active fuel.

### (4) Further Improvements

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

The pressure capability to the drywell head was increased to increase the containment pressure capability. Basaltic concrete was added to the lower drywell 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 to control automatic depressurization valves from the remote shutdown panel was improved.

As a result of the internal flood PRA studies . . . (later, after this work is done).

Several of the key safety functions, previously performed manually were automated (more later after changes are approved).



## (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 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 leads 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.

### 19.6.10.4 Conduct of the PRA Evaluations

In addition the PRA was conducted in accordance with the Key Assumption 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 system and equipment and dependencies arising from common cause failure, human error and support system failure, thus enabling potential vulnerabilities to be identified.

### 19.6.10.5 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 (Appendix 19P) 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.