Licensing Framework

The ABWR licensing basis generally follows the USNRC regulations and regulatory guides. This framework is the model which has been adopted in a number of countries, including Japan and Taiwan (which have also approved ABWR). In particular, Regulatory Guide 1.70, Rev 3, is used as the basis for documenting the safety analyses and the Standard Review Plan (SRP) is used by the USNRC in reviewing the design.

The events to be analyzed within the design basis are only loosely coupled to a probabilistic basis, and can be considered to be deterministic, both in the event description and in the acceptance criteria. Key points of this policy are:

- The assumption that Anticipated Operational Occurrences (transients) are caused by a single equipment failure or single operator error
- Use of the single active failure (N-1) criterion for postulated accidents
- Certain prescribed hardware and analyses to mitigate special events, such as Anticipated Transients Without Scram (ATWS)

There are no specific US regulations governing severe accidents, but a special set of review guidelines for severe accidents was promulgated by the USNRC in the form of several documents (SECY 90-016, SECY 93-087). These formed the basis for the safety review of the severe accident features provided in ABWR. The ABWR is the first plant to have undergone a specific review for severe accident mitigation and received approval from the USNRC.

Safety Design Approach

The ABWR safety design approach was to provide safety features which meet the regulations, but also to use PRA techniques to guide the feature selection. Insights gained from the PRAs were also used to improve plant technical specifications, emergency procedure guidelines, the control room interface, and the integrated reliability assurance program. These insights will be used throughout the lifetime of the plant to ensure that plant operations maintain a high level of safety.

The ABWR safety design approach looked at four key areas for safety improvement:

- Operational transients
- Design basis accidents
- Special regulatory mandated events
- Beyond design basis accidents, including core melt, commonly called severe accidents

Since improved operations lead directly to improved safety through reduced challenges to safety systems, the ABWR introduced a number of improvements in this area:
• Increased redundancy and diagnostics for I&C control and protection systems so that single failures do not lead to scrams

• The use of 99% trip avoidance statistical design for separating nominal and analytical instrument set points

• Increased redundancy in key hardware, such as recirculation and feedwater pumps

PRA techniques were used to guide the ECCS architecture. For example, significant improvement in core damage frequency (CDF) was obtained in going from 2 divisions to 3 divisions. However studies showed little value in going to 4 divisions, due to common mode failure considerations. Therefore, for design basis accident mitigation the ECCS architecture chose a 3-division approach with a high pressure and a low pressure flooder in each division and heat removal in each division. Each division also contains all supporting services, such as emergency diesel generators. Although it is conceptually possible to meet a deterministic N-2 failure criterion with 3 divisions, PRA studies indicated station blackout to be the dominant safety threat. Therefore, in one division the high pressure flooder was made steam driven. In practice, the ABWR is nearly N-2, with only one out of hundreds of possible N-2 combinations not able to provide core safety.

Containment design for the ABWR uses a double barrier approach, with a low leakage inerted pressure suppression primary containment pressure boundary surrounded by a slightly negative pressure processed atmosphere secondary containment. The US NRC granted regulatory credit for holdup of containment leakage past the MSIVs in the steamlines and main condenser in offsite dose evaluations. This change to past design practice was made to gain consistency in approach between ABWR and current practices of US operating BWRs.

For external threats, such as seismic events, the ABWR is designed to a site envelope (see Appendix A) conservative enough to cover at least 90% of the potential sites in the USA. In this way, a utility can compare its specific site to the envelope, and if the site is within the analyzed conditions, no further safety analysis will be required.

For the key new features, particular attention was paid to insure that their introduction did not lead to new safety issues. For the recirculation system design, redundant power supplies are used and M-G sets with flywheels are included to insure a slow flow coastdown in case of loss of power. The all recirculation pumps trip event is reclassified as an infrequent operational occurrence, with time-temperature acceptance criteria instead of MCPR. The justification for this change is the low probability of simultaneous loss of power at all 10 RIPS. The pump attachments to the reactor vessel were designed so as to make impossible a pump shaft blowout in case of a pressure boundary failure in a pump housing.

For the FMCRD, the drives are supported from the core plate to avoid a drive ejection on pressure boundary failure. In addition, an electromechanical brake which is engaged at all times except during rod movement was added to avoid rod runout on pressure boundary failure. Safety grade limit switches are included in the design to detect rod separation from the drive - this eliminates the possibility of a reactivity event from a rod drop accident. Finally, diverse C&I systems to monitor rod movement eliminated rod withdrawal error transients.

For all design basis events the response was designed to be fully automatic, with no operator action needed to accomplish any of the safety functions - reactor trip,
core cooling, containment isolation, heat removal and radiation protection of the public.

Certain special regulatory mandated events were also addressed directly in the design. ATWS mitigation is completely automated and includes the following features:

- Trip of 4 out of 10 recirculation pumps on high reactor pressure
- Diverse C&I scram (Alternate Rod Insertion) signal for rapid hydraulic-driven rod insertion
- FMCRD electric run-in following a scram signal
- Recirculation flow runback to reduce power
- Feedwater pump trip after two minutes, if necessary, to further reduce power
- Liquid poison injection via the SLCS after 3 minutes, if power is still not down

Station Blackout mitigation includes (in addition to the steam driven RCIC) an alternate onsite diverse AC power source - a Combustion Turbine Generator (CTG) for the standard design. The CTG is a standby onsite non-safety power source designed to feed permanent non-safety loads during loss of offsite power (LOOP) events. Implementation at multiple unit sites has taken alternate approaches: swing EDG at Lungmen, emergency power sharing at Kashiwazaki-Kariwa.

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.

Since active systems form the basis for safety protection for transients, design basis accidents and special events (prevention), the ABWR has provided primarily passive severe accident mitigation features to protect the containment from over-pressurization and to limit the consequences to the public even if the pressure were to exceed the design pressure. The philosophy behind this approach is that the only way a severe accident could occur is by complete failure of the active systems.

**Design Basis Transient and Accident Performance**

Transient performance, in the safety sense, becomes translated into fuel performance and operating margins. The primary BWR measures are Minimum Critical Power Ratio (MCPR) and maximum linear heat generation rate (MLHGR). These design parameters vary, depending on the specific fuel design being used (e.g., 8x8, 9x9 or 10x10); however, the ABWR reactor was designed to assure flexibility of use of advancing fuel technologies while maintaining the capability of at least 15% operating margins to fuel limits if desired by the utility, as required by the US utility sponsored Utility Requirements Document. A wide variety of transient analyses have been performed with different fuel designs to demonstrate that the above requirement can be met, even with longer fuel operating cycles up to 2 years in length.

With the elimination of large pipes attached to the RPV below core elevation, the ABWR has no core uncover and SA LOCA loss of cooling accident (DBA LOCA). Thus there is no concern over peak fuel clad temperature (PCT) after DBAs. The peak pressure in the containment after
DBA has been shown to have 15% margin relative to the design pressure of 0.31 MPa (45 psig). Thus the ABWR represents a very robust design for the traditional design basis accidents.

**Severe Accident Mitigation**

Although demonstration of performance for the traditional set of design basis transients and accidents is important, in recent years regulatory emphasis has shifted toward performance for beyond design basis events, classified as “severe accidents”. The ABWR capability to prevent severe reactor accidents from occurring and the capability to withstand a severe accident in the extremely unlikely event that one should occur were evaluated with several probabilistic risk assessments (PRAs) during the design process. The final evaluation indicates that events resulting in damage to the reactor core are extremely unlikely, but that even if such events were to occur, passive accident mitigation features would limit the offsite dose such that the effect on the public and surrounding land would be insignificant.

**ABWR Probabilistic Risk Assessment (PRA)**

A comparison of the internal events PRA for the ABWR to PRAs performed for other reactors clearly demonstrates the overall improvement in safety (see Figure 10-1). The US NRC risk goal for the frequency of core damage events in new reactors is one in 100 thousand years. The CDF for the ABWR was found to be less than 2 per ten million years. This represents more than a factor of 10 improvement as compared to the previous BWR designs, and a factor 100 improvement as compared to most light water reactors (see Table 10-1).

Probabilistic methods were also applied to events initiated externally: tornado, flood, fire and earthquake. The important design features to ensure plant safety for each of these events were identified in a manner similar to that for the internal events PRA.

The frequency of core damage due to a tornado was found to be extremely low because all safety components are located in the concrete Reactor Building, and the three divisions of emergency diesel generators reduce the probability of a Station Blackout (SBO) due to failure of AC power.

The Reactor Building is designed to physically separate the safety divisions. In addition, drains in the upper floors of the Reactor Building were included in the design to direct water away from electrical equipment towards the lower floor of the building, where water can accumulate without damaging safety equipment. As a result, a flood cannot damage more than one safety division. Therefore, the core damage frequency associated with flooding was found to be a very small fraction of the NRC Safety Goal.
CHAPTER 10 — SAFETY EVALUATIONS

The evaluation of fires was based on the Fire-Induced Vulnerability Evaluation methodology developed by the Electric Power Research Institute (EPRI). This conservative methodology provides procedures for performing quantitative screening analyses of fire risk. No risk significant fires were identified for the ABWR design due in part to the complete divisional separation of all safety systems and the ability to initiate and control safety systems from the remote shutdown panel.

The risk of seismic events was evaluated using seismic margins method. The ABWR was designed for a Safe Shutdown Earthquake (SSE) of 0.3g for an envelope of possible soils. In the margins method, the margins implicit in the system designs are evaluated to determine a somewhat conservative estimate of the actual capacity of each system. Then, using fault trees and event trees similar to those developed for the internal events analysis, the system capacities are combined to determine the overall plant capacity. The ABWR was shown to have a factor of more than two margin to the design SSE. This ensures that there is very little possibility of a core damage event as a result of an earthquake.

The risk of core damage occurring during refueling and maintenance operations was also evaluated probabilistically and found to be a small fraction of the overall core damage risk. This is primarily due to the large body of water overlying the core during refueling operations.

### ABWR Features to Mitigate Severe Accidents

As a result of PRA evaluations and other implied requirements in the USNRC severe accident review guidelines, several new features were added to the ABWR design. Five of the primary features are described; the first four of these are passive.

#### Inerted Containment

The ABWR containment is normally inerted with nitrogen containing < 3.5% oxygen (see discussion of the Atmospheric Control System in Chapter 4). Therefore any potential for hydrogen burning or detonation after a severe accident is avoided.

#### 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 (see Figure 8-6). 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 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,

<table>
<thead>
<tr>
<th>Event</th>
<th>Frequency/yr</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station Blackout</td>
<td>$1.1 \times 10^{-7}$</td>
<td>71</td>
</tr>
<tr>
<td>Transients</td>
<td>$4.5 \times 10^{-8}$</td>
<td>29</td>
</tr>
<tr>
<td>LOCA</td>
<td>$6.9 \times 10^{-10}$</td>
<td>&lt;1</td>
</tr>
<tr>
<td>ATWS</td>
<td>$2.7 \times 10^{-10}$</td>
<td>&lt;1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>$1.6 \times 10^{-7}$</td>
<td></td>
</tr>
</tbody>
</table>

*Table 10-1. ABWR Internal Events CDF*
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 less pressure from non-condensable 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.

**Corium Shield**

The bottom of the lower drywell contains two features to mitigate against continued core-concrete reactions after quenching by the passive lower drywell flooders. The first of these is the use of non-limestone aggregate concrete (so-called basaltic concrete). This minimizes any further production of carbon-based noncondensibles, such as CO and CO₂. In addition, the drywell sumps are covered with refractory oxide bricks to prevent intrusion of molten corium into the sumps.

**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 ~ 1 MPag, 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 (see Figure 4-7). 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.

**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. Figure 4-5 shows the piping arrangement.

An integrated view of how the passive severe accident mitigation features work together is shown in Figure 10-2. Analyses of the dominant severe accident sequence, which is a low pressure core melt following a Station Blackout, shows that the COPS pressure will not be reached for more than 24 hours. In addition, the conditional containment failure probability, defined as the loss of containment as a fission product barrier, was calculated to be 0.2%, far less than the goal of 10% set by the U.S. Utility Requirements Document and USNRC guidelines.
In summary, the detailed PRA of the ABWR design demonstrates that both the core damage frequency and the offsite risk goals established by the US NRC are met with substantial margin. The ABWR represents a substantial improvement in safety as compared to earlier plant designs. The high degree of safety is attributable to the many improved features in the design and to the use of PRA in the design process.

For a nominal U.S. site, the offsite dose as a function of probability is given in Figure 10-3. It can be seen that large releases do not occur even at the one in a billion probability level.

**Summary**

For a nominal U.S. site, the offsite dose as a function of probability is given in Figure 10-3. It can be seen that large releases do not occur even at the one in a billion probability level.