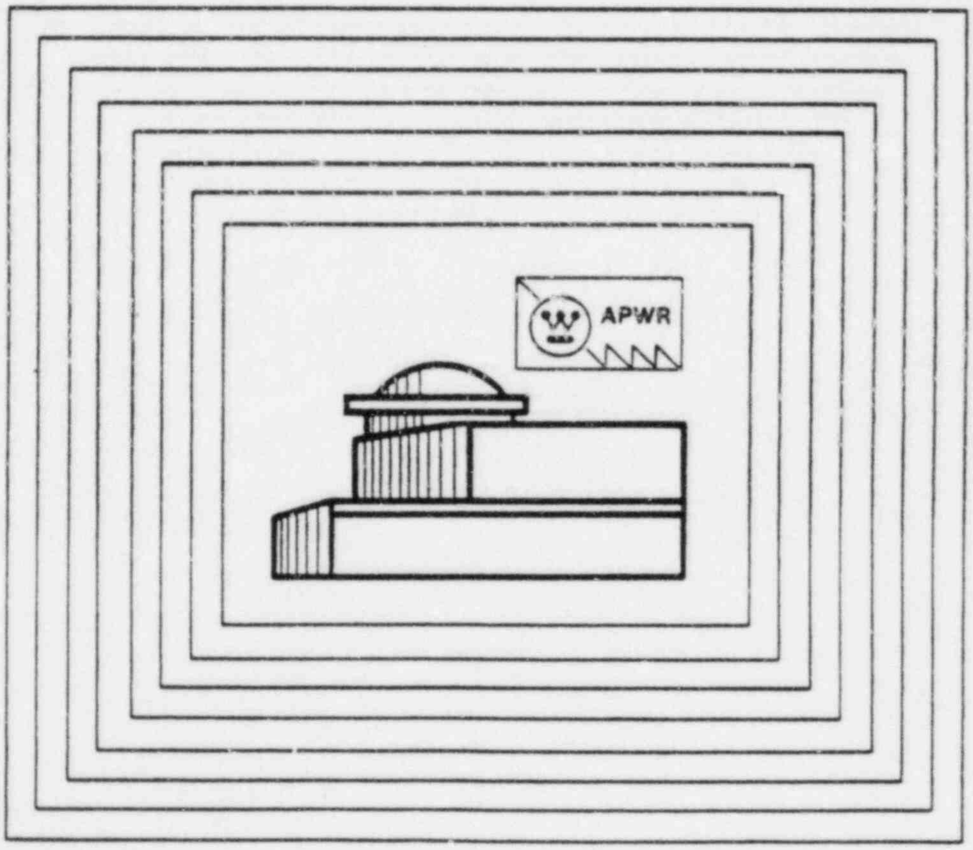
# RESAR-SP/90 PROBABILISTIC SAFETY STUDY

## WESTINGHOUSE ADVANCED PRESSURIZED WATER REACTOR




STANDARD PLANT DESIGN

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont)

LIST OF TABLES

LIST OF TABLES (Continued)

LIST OF TABLES (Continued)

LIST OF FIGURES

LIST OF FIGURES (Continued)

## 0. SUMMARY OF PLANT COREMELT ANALYSIS

This module contains the plant coremelt analysis of the Westinghouse Advanced PWR (WAPWR) design. The point estimate (mean value) plant coremelt analysis is carried out for internal initiating events.

This module will be complemented by three more modules which will contain the core and containment analysis, consequence analysis, and the plant risk and uncertainty analysis.

### 0.1 PLANT DESIGN FEATURES AND SYSTEM RELIABILITIES

#### 0.1.1 PRIMARY SYSTEMS

A. Reactor Coolant System

The RCS of the APWR includes a reactor vessel with greater internal volume than standard W-PWR vessels. The increased quantity of water above the core provides a longer period of time before core uncovery following both a loss of secondary cooling and a small LOCA.

B. Core Reflood Tanks

Four tanks with low pressure nitrogen coverage that inject into the RCS vessel through high resistance lines assist the HHSI in reflooding the core following a large LOCA. These tanks eliminate the need for active low head SI pumps.

C. ISS

Four high head pumps that inject through their own RCS vessel connections provide emergency core cooling for the full range of LOCAs and provide RCS makeup and boration for all non-LOCA events. Only one of these four pumps is required for small LOCAs and "feed and bleed" cooling. No valve realignment is required for initial injection or recirculation.

D. Emergency Water Storage Tank

The water supply for the Emergency Core Cooling System and Containment Spray System is located in the basement of the containment. Thus, no switchover from an injection mode to recirculation mode is required. The EWST also provides a means to reduce the containment cleanup resulting from discharge from the pressurizer relief tank rupture disc, the hot leg vent path, or the SG overfill paths. The location inside the containment provides security and a higher minimum temperature which reduces vessel thermal shocks due to SI.

E. Hot Leg Vents

Two vent lines are provided on the RCS hot legs to provide emergency boration and an alternate bleed path for core cooling and reactor coolant system depressurization. These lines vent into the emergency water storage tank.

F. Interfacing Systems LOCA

The RHR/CSS system piping has been arranged such that the frequency of a rupture of system piping outside containment due to exposure to full RCS pressure has been reduced. The most likely cause of an exposure to RCS pressure is the spurious failure of both series RHR letdown isolation valves. The system is arranged such that should the RHR isolation valves fail the RCS pressure would be relieved through the RHR pump suction line back into containment. An ex-containment rupture is assumed if the normally open RHR pump suction isolation valve is inadvertently closed.

G. Charging Pumps

The APWR charging system is not used to mitigate design basis LOCAs. However, it does have substantial RCS makeup capability, it is ANS-3 with 1-E motors, and it is automatically loaded on the emergency diesels in the case of loss of offsite power without an "S" signal.

H. Back-up Seal Injection.

The CVCS contains a back-up seal injection pump which automatically provides RCP seal cooling in the event of loss of normal seal injection and CCWS thermal barrier cooling. This pump is a control grade positive displacement pump with a DC motor that receives power from a dedicated diesel motor/DC generator set. Power is also available from control grade DC system. The pump does not require AC or DC power (aside from its self-contained diesel generator set) or support systems such as CCWS or HVAC.

I. Alternate Core Cooling Means

In addition to normal alternate core cooling means (SFWS, EFWS) and their back-up (RCS feed/bleed with HHSI), there are several other possibilities. Examples of these are RCS feed and bleed with charging pumps, RCS depressurization and feed and bleed with RHR pumps, and SG feed by main feedwater or condensate pumps. For the most part these means are not considered in the WAPWR PRA analysis. However, for core cooling following a small LOCA with the failure of all four HHSI pumps credit is taken for the operators opening the pressurizer PORV and aligning the RHR pumps to inject into the RCS. In this case the larger APWR RCS and accumulator volumes give the operator the capability of keeping the core from overheating during the depressurization to the RHR pump delivery pressure of ≤ [ ] psig. **(a,c)**

0.1.2 SECONDARY SYSTEMS

A. Emergency Feedwater System

The emergency feedwater system contains four pumps, two electric motor driven and two turbine driven. Any one of the pumps is sufficient to remove decay heat through the S.G. The turbine driven pumps start upon the opening of a steam inlet air-operated fail-open valve. This valve opens upon the loss of air supply or DC power to either of two solenoid valves. System actuation is automatic upon receipt of an S signal or following a loss of start-up feedwater system or is manual. The turbine driven pumps do not require any AC or DC power or any support systems such as CCW or HVAC.

B. Start-up Feedwater System

A single non-safety class pump driven by a 1E motor, taking suction from either the condenser hotwell or a deaerating heater, provides the normal feedwater function following reactor trip. The system bypasses the main feedwater control valves, but shares the main feed isolation valving. Automatic actuation occurs upon low steam generator level. The system is provided to minimize challenges to the Emergency Feedwater System and to minimize thermal transients on the steam generator and piping.

C. Steam Generator Overfill Protection

Each steam generator is provided with an automatic drain system to prevent high steam generator level and possible water passage in the main steam lines. Two safety grade parallel valves are opened upon indication of high-high SG level, and closed on a lower level. The drain path is into the EWST. This system greatly reduces the dependence on operator action to mitigate SGTR.

### 0.1.3 AUXILIARY SYSTEMS

A. Diesel Generators

Two essential service diesel generators are provided for back-up emergency power to safeguards loads following a loss of offsite AC power.

B. Component Cooling Water System/Service Water System

The APWR CCWS and SWS are two subsystem designs that are not interconnected. Therefore, for events such as CCWS or SWS pipe breaks or excessive heat input post-large LOCA only one subsystem can be affected.

## 0.2 WAPWR PLANT ANALYSIS METHODOLOGY

The large event tree, small fault tree approach was utilized in this analysis. A major effort was expended on minimizing the complexity of the analysis in two ways:

a. Identification and standardization of component modular fault trees, allowing full system fault trees to be compiled from a standard set of segments. This facilitates review of the fault trees and assures consistent treatment of like faults between systems and analysts. It also assures consistent use of the data base, with all fault trees developed to the same degree of detail.

b. Minimization of event tree sequences by both reducing the number of events analyzed and the number of sequences addressed by each event tree. Reduction in the events analyzed in the study was facilitated by the WAPWR design, which provides for similar plant response to different initiating events. For example, ECCS operational parameters eliminate the event Medium LOCA, which placed special requirements on older design systems. Similarly, analysis of plant transients includes all anticipated and design basis events that lead to reactor trip but not necessarily to generation of an S signal.

   A further simplification was the minimization, where practical, of event tree sequences. It was the intent of this procedure to minimize the number of sequences whose frequency was about five (5) orders of magnitude below the total frequency for each of the associated core damage categories. This method was not extremely effective, as some sequences with frequencies of $10^{-20}$ still result. Where simplification was possible, a conservative approach to categorization was taken, grouping the sequences with higher-consequence core damage categories than might result if further analysis of the sequence were to be performed.

Further modeling methods and assumptions are described below:

### 0.2.1 SUPPORT STATE MODELING

Engineered Safety features systems have been divided into two groups for this study: front-line systems such as Emergency Feedwater and Integrated Safeguards, and Support systems. This latter group is comprised of the Diesel Generators and Class 1E AC distribution system, the Essential Service Water System, the Component Cooling Water System, and the Integrated Protection System.

The availability of the support systems is explicitly modeled in the event trees. Three possible states are addressed: 1. Both front-line trains of equipment have electric power, cooling water flow, and actuation signals delivered to active components; 2. Only one train of each front-line system has every support system available; and 3. No front-line systems are receiving support from all support systems. Thus, the failure of any support system, be it electric power, cooling water, or actuation results in a plant state with reduced front-line systems available for accident mitigation. These states are modeled by the second node in each event tree, which shows three branches. The event tree structure following each branch reflects the availability of front-line systems, and the reliability of those systems, which is a function of support state, is changed in quantification of the event tree.

### 0.2.2 RECOVERY OF AC POWER

Recovery of AC power sources is modeled in both the short-term and in the long-term. Short-term recovery is modeled as both restoration of offsite power sources and repair of the onsite diesel generators. Short-term recovery is modeled as occurring before dry-out of the steam generators following reactor trip, which is very conservatively assumed to be 40 minutes. If short-term recovery of AC power fails, then long-term recovery of offsite power is modeled. Recovery of the offsite grid after 40 minutes but before core uncovery, which is roughly between two and three hours after reactor trip, will enable the safeguards systems to prevent core damage. Onsite recovery is not addressed in the long-term. Furthermore, operator actions to depressurize the primary system in order to use the accumulators and core reflood tanks, thus delaying core damage, are not addressed.

### 0.2.3 RCP SEAL LOCA

Upon loss of both RCP seal injection and thermal barrier cooling, it is assumed to be equally probable that a consequential seal LOCA resulting in core uncovery and damage will occur as not. This is a conservative assumption since the chance of a seal leak of sufficient magnitude to uncover the core before recovery of offsite power is considered to be small.

### 0.2.4 COMMON CAUSE FAILURE ANALYSIS

The beta factor method was used to model common cause failure of redundant components. A mean value of 0.1 for the failure of a second component given that the first has failed was used for all active pumps and valves in all systems. In order to address the use of four redundant components in many systems, it was assumed that adding two active components in parallel to a normal two component system would only decrease the unreliability of the overall system by an order of magnitude. This method implicitly applies conditional failure probabilities of 0.2 and 0.5 to the third and fourth trains, respectively.

### 0.2.5 TEST AND MAINTENANCE

Test unavailability of systems was based on testing intervals and durations peculiar to the system analyzed, drawing on technical specification requirements of other Westinghouse PWRs.

Maintenance unavailability was derived from previous operating experience at several Westinghouse PWR facilities. The mean frequency of maintenance of system components was assumed to be the average values achieved in these similar plants, thus reflecting differing component reliabilities and utility maintenance practices.

## 0.2.6 ANALYSIS OF OPERATOR ACTIONS

A scoping study of operator actions was performed in this analysis, where the unreliability of the operator under any given set of circumstances was assumed to be no less than $5.0 \times 10^{-3}$. Due to the dominance of the failure to properly diagnose plant conditions, a detailed study of operator acts of omission and commission was not performed. Based on stress levels extant during degraded conditions of the plant, operator unreliability increased with increased complexity of the actions and increased with decreasing time available to carry out those actions. It was also assumed that increased practice under simulator training and detailed procedural preparation would increase the reliability of the operator in certain actions, for example, establishing feed and bleed cooling. However, justification of a reliability in excess of 0.995 was not attempted. As a result, for this study an operator reliability of $5 \times 10^{-3}$ is only assumed for opening the pressurizer PORVs to establish "feed and bleed"; all other operator actions are more complicated, have higher stress, or shorter available time and therefore are assumed to have a reliability of $1 \times 10^{-2}$.

## 0.3 SUMMARY OF PLANT COREMELT QUANTIFICATION

The breakdown of the total plant coremelt frequency by support states (availability of AC power, Service Water/Component Cooling Water Cooling, etc.) indicates that the loss of support sytems (mainly the AC power) contributes significantly to the coremelt frequency:

| | Support State | Coremelt Contribution |
|---|---|---|
| | Support Systems Available: | [ |
| (a,c) | Only One Front Line Train Supported: | |
| | No Front Line Trains Supported: | ] |

(a,c) The total plant coremelt frequency for the WAPWR is [ ]. See Section 4.2.

0.3.1 DOMINANT ACCIDENT SEQUENCES

The dominant accident sequences and their contributions to the total plant coremelt are given below:

| Event Sequence | % Contribution |
| --- | --- |

(a,c)

| Event Sequence | % Contribution |
| --- | --- |

(a,c)

| Event Sequence | % Contribution |
| --- | --- |

(a,c)

### 0.3.2 SUMMARY OF SYSTEM IMPORTANCES

The event tree nodes and support systems also ranked according to their contribution to the total plant coremelt frequency:

| System | Importance |
| --- | --- |

(a,c)

This importance measure can be interpreted as follows: in the above list, if the diesel generator failure probability can be reduced to effectively 0, then the plant coremelt frequency can be reduced by [49%] of its original value. (a,c) Note that this argument only holds for one system at a time; it does not hold for simultaneous changes in reliability of multiple systems.