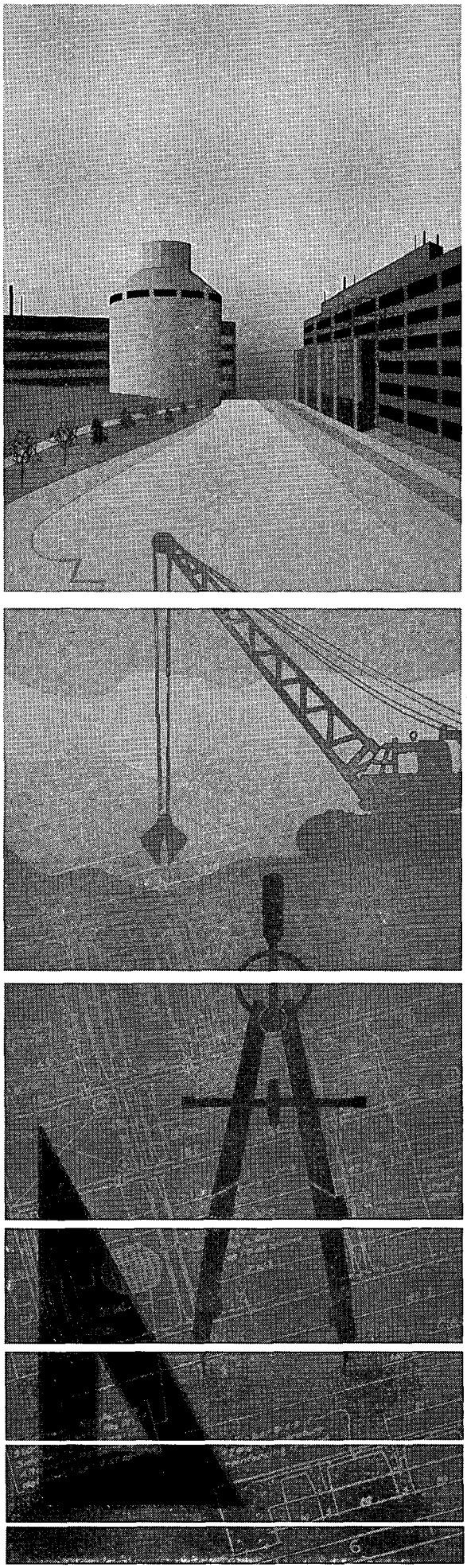


# Final Safety Evaluation Report

Related to Certification of the
AP600 Standard Design

## Volume 2

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

September 1998

# AVAILABILITY NOTICE

## Availability of Reference Materials Cited in NRC Publications

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy,* of the *Code of Federal Regulations,* may be purchased from one of the following sources:

1. The Superintendent of Documents
   U.S. Government Printing Office
   P.O. Box 37082
   Washington, DC 20402–9328
   <http://www.access.gpo.gov/su_docs>
   202–512–1800

2. The National Technical Information Service
   Springfield, VA 22161–0002
   <http://www.ntis.gov/ordernow>
   703–487–4650

The NUREG series comprises (1) technical and administrative reports, including those prepared for international agreements, (2) brochures, (3) proceedings of conferences and workshops, (4) adjudications and other issuances of the Commission and Atomic Safety and Licensing Boards, and (5) books.

A single copy of each NRC draft report is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer
Reproduction and Distribution
Services Section
U. S. Nuclear Regulatory Commission
Washington, DC 20555–0001
E–mail: <GRW1@NRC.GOV>
Facsimile: 301–415–2289

A portion of NRC regulatory and technical information is available at NRC's World Wide Web site:

<http://www.nrc.gov>

All NRC documents released to the public are available for inspection or copying for a fee, in paper, microfiche, or, in some cases, diskette, from the Public Document Room (PDR):

NRC Public Document Room
2121 L Street, N.W., Lower Level
Washington, DC 20555–0001
<http://www.nrc.gov/NRC/PDR/pdr1.htm>
1–800–397–4209 or locally 202–634–3273

Microfiche of most NRC documents made publicly available since January 1981 may be found in the Local Public Document Rooms (LPDRs) located in the vicinity of nuclear power plants. The locations of the LPDRs may be obtained from the PDR (see previous paragraph) or through:

<http://www.nrc.gov/NRC/NUREGS/SR1350/V9/lpdr/html>

Publicly released documents include, to name a few, NUREG-series reports; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigation reports; licensee event reports; and Commission papers and their attachments.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852–2738. These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
<http://www.ansi.org>
212–642–4900

NUREG–1512
Vol. 2

# Final Safety Evaluation Report Related to Certification of the AP600 Standard Design Docket No. 52-003

## Chapters 15–24

Manuscript Completed: August 1998
Date Published: September 1998

**Division of Reactor Program Management**
**Office of Nuclear Reactor Regulation**
**U.S. Nuclear Regulatory Commission**
**Washington, DC 20555–0001**

NUREG-1512, Vol. 2 has been
reproduced from the best available copy.

## ABSTRACT

This final safety evaluation report (FSER) documents the technical review of the AP600 standard nuclear reactor design by the U.S. Nuclear Regulatory Commission (NRC). The application for the AP600 design was submitted on June 26, 1992 by Westinghouse Electric Corporation in accordance with Subpart B, "Standard Design Certifications," of Part 52 of Title 10 of the Code of Federal Regulations (10 CFR Part 52), and Appendix O, "Standardization of Design: Staff Review of Standard Designs."

The AP600 nuclear reactor design is a pressurized water reactor with a power rating of 1933 MWt with an electrical output of at least 600 MWe. The AP600 design contains many features that are not found in current operating reactor designs. For example, a variety of engineering and operational improvements provide additional safety margins and address the Commission's severe accident, safety goal, and standardization policy statements. The most significant improvement to the design is the use of safety systems that use passive means (such as gravity, natural circulation, condensation and evaporation, and stored energy) for accident prevention and mitigation. These passive safety systems perform safety injection, residual heat removal, and containment cooling functions.

Unique features of the AP600 design include an enhanced reactor core design, larger reactor vessel, larger pressurizer, an in-containment refueling water storage tank, automatic depressurization system, revised main control room design with a digital microprocessor-based instrumentation and control system, hermetically-sealed canned reactor coolant pump motors mounted to the steam generator, and increased battery capacity. In addition, the facility is designed for a 60-year life, and employs modular construction techniques in its design.

On the basis of its evaluation and independent analyses, the NRC staff concludes that Westinghouse's application for design certification meets the requirements of Subpart B of 10 CFR Part 52 that are applicable and technically relevant to the AP600 standard design. A copy of the report by the Advisory Committee on Reactor Safeguards required by 10 CFR 52.53 is provided in Appendix G.

## CONTENTS

Page

Page

## LIST OF TABLES

## LIST OF FIGURES

# 15 TRANSIENT AND ACCIDENT ANALYSES

## 15.1 Introduction

In Chapter 15 of the AP600 Standard Safety Analysis Report (SSAR), Westinghouse discusses the design-basis analyses of various transients and accidents. The applicant uses the results of these analyses in the SSAR to show the conformance of the AP600 advanced passive plant design with general design criterion (GDC) 10 for fuel design limits, GDC 15 for the reactor coolant pressure boundary (RCPB) pressure limits and the 10 CFR 50.46 requirements for the performance of the emergency core cooling system (ECCS).

The staff has reviewed the AP600 transient and accident analyses in the SSAR, in accordance with Chapter 15 of the NRC's Standard Review Plan (SRP), NUREG-0800.

### 15.1.1 Event Categorization

The applicant assigned the initiating events to the following categories in accordance with Chapter 15 of the SRP:

(1) increased heat removal from the primary system
(2) decreased heat removal by the secondary system
(3) decreased reactor coolant system flow rate
(4) reactivity and power distribution anomalies
(5) increase in reactor coolant inventory
(6) decrease in reactor coolant inventory
(7) anticipated transients without scram (ATWS)

The first category, increased heat removal from the primary system, includes a new event involving inadvertent operation of the passive residual heat removal (PRHR) heat exchanger (HX). As such, it is a broader categorization than the SRP category of increased heat removal by the secondary system.

The applicant also grouped the design-basis events according to their anticipated frequency of occurrence identified as Condition I normal operation and operational transients; Condition II faults of moderate frequency; Condition III infrequent faults; and Conditions IV limiting faults. The applicant's event frequency grouping is consistent with the guidelines of Regulatory Guide (RG) 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Plants," and the criteria of American Nuclear Society (ANS) 18.2-1973, "Nuclear Safety Criteria for the Design of Stationary Pressurized-Water Reactor Plants." Condition I events occur frequently and should be considered from the point of view of their effect on the consequences of Conditions II, III, and IV events. Condition II events are those that may occur during a calendar year for a particular plant. Condition III events are those that may occur during the life of a particular plant. Condition IV events are postulated but not expected to occur during the life of a plant.

The SRP divides the events into anticipated operational occurrences (AOOs) and postulated accidents. 10 CFR Part 50, Appendix A, defines AOOs as conditions of normal operation and those transients that are expected to occur one or more times during the life of a plant; therefore, AOOs encompass the normal, moderate frequency and infrequent events of Conditions I through III. Chapter 15 of the SRP does not specify a category of infrequent incidents but does provide specific acceptance criteria for those events that cannot be categorized as infrequent. Thus, the event frequency categorization of the SSAR is consistent with the Commission's licensing approach.

In Section 15.0.1 of the SSAR, Westinghouse lists the design-basis events analyzed under Conditions II, III, and IV. These events are generally consistent with current licensing practice. However, the complete loss of forced reactor coolant flow event is listed in the SSAR as a Condition III infrequent fault. This is inconsistent with the current licensing practice of classifying the complete loss of RCS flow as a Condition II event with the acceptance criteria that the departure from nucleate boiling ratio (DNBR) does not exceed the specified limit. Nonetheless, the applicant analyzed this event as presented in SSAR Section 15.3.2 to satisfy the acceptance criteria for a Condition II event. Thus, the staff concludes that the applicant's approach for the analysis of this event is acceptable.

15.1.2 Non-Safety-Related Systems Assumed in the Analysis

For the design-basis analysis, only safety-related systems or components are allowed to be used to mitigate the events. In Westinghouse letter ET-NRC-93-3804, dated January 22, 1993, the applicant's response to the staff's request for additional information (RAI) 440.31 stated that non-safety-related systems or components are assumed to be operational in the following situations:

(a) when assumption of a non-safety-related system results in a more limiting transient,

(b) when a detectable and non-consequential random, independent failure must occur in order to disable the system, and

(c) when non-safety-related components are used as backup protection.

Case (a) is an acceptable assumption, and is also a staff requirement.

For Case (b), the applicant assumed continued operation of the main feedwater control system (MFCS) in the design-basis analyses of those events not related to feedwater system malfunction, loss of ac power, or turbine trip. For example, an event involving withdrawal of a rod cluster control assembly (RCCA) is analyzed from an at-power condition. Before the initiating fault causing the RCCA withdrawal, the MFCS should be operating and maintaining steam generator inventory. If a failure exists in the MFCS, it should be detectable in the control room by alarms or abnormal control system performance before the start of the RCCA withdrawal event. The staff concludes that the assumption of MFCS continued operation is acceptable since a failure in the MFCS is not a consequence of the initiating event, and the probability of a random, independent failure occurring in the MFCS within the time frame of the initiating event is extremely low.

For Case (c) as discussed in WCAP-14477, "The AP600 Adverse System Interactions Evaluation Report," and summarized in SSAR Table 15.0-8, the applicant credited the following non-safety-related components as backup protection in design-basis analyses:

- the main feedwater pump trip in the analysis of an increased feedwater flow event
- the pressurizer heater block in the analyses of loss of normal feedwater, inadvertent operation of core makeup tanks (CMTs), malfunction of the chemical and volume control system (CVS), steam generator tube rupture (SGTR), and small-break loss-of-coolant accidents (SBLOCA)
- main steam isolation valve (MSIV) backup valves, and main steam branch isolation valves, in the analyses of inadvertent opening of SG safety valves, steamline break, and SGTR events (The MSIV backup valves include the turbine stop or control valves, the turbine bypass valves, the main steam to auxiliary steam header valve, and the moisture separator reheat steam supply control valve. The non-safety-related main steam branch isolation valves include the MSIV bypass valves and steamline condensate drain isolation valves.)

During the course of the review, the staff asked the applicant to address its compliance with 10 CFR 50.36, which specifies the criteria for the systems that are subject to technical specification (TS) limiting conditions for operation (LCOs). Specifically, 10 CFR 50.36(c)(2)(ii)(C) requires, in part, that a TS be established for a structure, system, or component (SSC) that is assumed to function or actuate in a design-basis analysis for mitigation of specified events. The applicant complied with the 10 CFR 50.36 requirements by providing TSs to include non-safety-related systems that are credited as backup systems in the licensing design-basis analyses in its response to comment (4) of Westinghouse letter DCP/NRC 0970, dated August 29, 1997. The revised TSs include changes to TS Table 3.3.2 for the main feedwater pump trip and pressurizer heaters trip actuation device, TS 3.6.3 for the main steam branch isolation valves, and TS 3.7.2 for the MSIV backup valves. The added TSs apply to all non-safety-related systems identified as credited in the design-basis analyses. These TSs are consistent with the Standard TSs and are acceptable.

The staff concludes that crediting these non-safety-related backup protection systems and components in the design-basis analyses is acceptable for the following reasons:

(1) The trip mechanisms of the feedwater pump trip breakers and pressurizer heater trip breakers are simple, and the likelihood of the breaker function failure is low.

(2) The operating data show that the turbine stop and control valves are reliable, and taking credit of the turbine valves in the design-basis analyses for backup protection is consistent with the staff position stated in NUREG-0138, "Staff Decision of Fifteen Technical Issues Listed in Attachment to November 3, 1976, Memorandum from Director, NRR to NRR Staff."

(3) The applicant has included surveillance requirements and limiting conditions for operation in the TSs to ensure the reliability of the following systems or components:

(i) feedwater pump trip breakers and redundant pressurizer heater trip breakers
(ii) the main steam branch isolation valves
(iii) the MSIV backup valves

15.1.3 *Chapter 15 Loss-of-Offsite-Power Assumptions*

In the original Chapter 15 analyses, the staff found that the applicant did not consistently postulate the unavailability of offsite power as part of the events. The staff took the position that a loss of offsite power (LOOP) should not be considered a single failure, and should be assumed in Chapter 15 of the SSAR for each event without changing the event categorization. Consequently, the staff asked the applicant to ensure that each of the transient and accident analyses in Chapter 15 of the SSAR conformed to the staff's position. The staff also asked the applicant to reanalyze the Chapter 15 cases where the existing analyses did not conform to this position.

The applicant agreed not to treat LOOP as a single failure in response to comment (3) of Westinghouse letter DCP/NRC 0982, dated August 8, 1997, and included the results of the reanalyses in Revision 13 to Chapter 15 of the SSAR. In the case of events involving a turbine trip, the applicant assumed that a LOOP and the resulting coastdown of the reactor coolant pumps occurs 3 seconds after the turbine trip. The basis for the 3-second delay is provided in Section 8.2.2 of the SSAR. That section describes the electrical design features of the AP600, the electrical system response to a turbine trip, and the COL applicant interfaces that support the 3-second assumption. Among others, the AP600 design provisions include the following electrical features that support the 3-second delay:

- use of an output generator circuit breaker and reverse power relay with at least a 15-second delay before tripping the breaker following a turbine trip (this allows the generator to provide voltage support to the grid and maintain adequate voltage to the reactor coolant pumps (RCPs) for significantly longer than the assumed 3-seconds)

- the COL applicant interface item in Table 1.8-1 of the SSAR that transient stability must be maintained and the RCP bus voltage must remain above the voltage required to maintain the flow assumed in Chapter 15 analyses for a minimum of 3 seconds following a turbine trip (this ensures that, for the applicant's unique grid system configuration, a grid instability condition following a turbine trip will take at least 3 seconds before it results in a loss of power to the RCPs)

- the COL applicant interface item in Table 1.8-1 that the protective devices controlling the switchyard breakers are set with consideration for preserving the plant grid connection following a turbine trip (this is especially important in generator output circuit breaker designs to ensure that the backfeed offsite circuit through the generator main stepup transformer is not interrupted by opening of the switchyard breakers following a turbine trip)

- no automatic transfers of RCP buses are used in the design (this precludes bus transfer failures following a turbine trip)

- if a turbine trip occurs when the grid is not connected to the plant, the main generator will be available to power the RCPs for at least 3 seconds before the generator output breaker is tripped on generator under-voltage or exciter over-current

The staff has reviewed the information on the AP600 electrical design, as well as the COL requirements. On that basis, and as described above, the staff has reasonable assurance that the RCPs can receive power for a minimum of 3 seconds following a turbine trip (see Section 8.2.3.6 of this report). The staff has also reviewed the SSAR Chapter 15 analyses and found that the applicant considered LOOP in all of the analyzed events and applied the acceptance criteria specified in the related SRP sections for events with and without LOOP. Therefore, the staff concludes that the applicant's approach is acceptable.

15.1.4 Analytical Methods

The analytical methods used for transient and accident analyses are normally reviewed on a generic basis. The methods for transient and accident analyses include the following computer codes:

- LOFTRAN: As documented in WCAP-7907-P-A, the NRC previously approved this code to allow Westinghouse to analyze system responses to non-LOCA events for conventional Westinghouse pressurized-water reactors (PWRs). LOFTRAN simulates a multi-loop system using a model containing a reactor vessel, hot and cold leg piping, steam generators, and pressurizer. The code also includes point kinetics and reactivity effects of the moderator, fuel, boron, and control rods. The secondary side of the steam generator uses a homogeneous, saturated mixture for analyses of thermal transients and a water level correlation for indication and control. When the applicant applied the LOFTRAN code to the AP600 safety analyses, it modified the code to incorporate features representative of the AP600 design which are important to modeling the non-LOCA transient analyses. The LOFTRAN modifications are documented in WCAP-14234, "LOFTRAN and LOFTTR2 AP600 Applicability Document." To verify the modified LOFTRAN code, the applicant provided test data comparisons in WCAP-14307, "AP600 LOFTRAN-AP and LOFTTR2-AP Final Verification and Validation Report." The staff has reviewed and accepted the modified LOFTRAN code and provided its evaluation of the code in Section 21.6.1 of this report.

- LOFTTR2: As documented in WCAP-10698-P-A, and supplemented by WCAP-10759-A and WCAP-11002, the NRC-approved code is used to analyze an SGTR event for conventional Westinghouse PWRs. LOFTTR2 is a modified version of LOFTRAN with a more realistic break flow model, a two-region steam generator secondary side, and an improved capability to simulate operator actions during an SGTR event. The version of LOFTTR2 applied to the AP600 SGTR analyses incorporated the LOFTRAN changes to simulate passive safety features for the AP600 design. These changes are documented in WCAP-14234. The staff has reviewed and accepted the application of the modified LOFTTR2 code to the AP600 for SGTR analyses and provided its evaluation in Section 21.6.1 of this report.

- TWINKLE: This multi-dimensional spatial neutronic code uses an implicit finite-difference method to solve the two-group transient neutronic equations in one, two,

and three dimensions. TWINKLE has been used to calculate the kinetic response of a reactor for transients, such as the RCCA bank withdrawal from subcritical conditions and RCCA ejection events, which cause a major perturbation in the spatial neutron flux distribution. The code is documented in WCAP-7979-P-A and had been approved by the NRC for operating Westinghouse plants. Since the AP600 fuel design is similar to that of operating Westinghouse plants, i.e., falls within the NRC-approved applicable range of the code, the application of the TWINKLE code to the AP600 for analysis of kinetic responses is acceptable.

- THINC: As documented in WCAP-7956-P-A and WCAP-8054-P-A, the NRC has approved this code for the core thermal-hydraulic analyses, determining coolant density, mass velocity, enthalpy, vapor void, static pressure, and the DNBR distribution along parallel flow channels within the reactor core under normal operational and transient conditions. Since the AP600 core design is similar to that of operating Westinghouse plants, i.e., falls within the NRC-approved applicable range of the code, the application of the THINC code to the AP600 thermal-hydraulic calculations is acceptable.

- FACTRAN: As documented in WCAP-7908-A, the NRC has approved the FACTRAN code for calculations of the transient heat flux at the surface of a rod. Since the AP600 fuel rod design is similar to that of operating Westinghouse plants, i.e., falls within the NRC-approved applicable range of the code, the application of FACTRAN to the AP600 heat flux calculations is acceptable.

- NOTRUMP: This code consists of the modeling features that meet the requirements of Appendix K to 10 CFR Part 50. As documented in WCAP-10079-A and WCAP-10054-A, the NRC previously approved the NOTRUMP code for SBLOCA analyses. The modified version of the NOTRUMP code for the AP600 application is documented in WCAP-14807, "NOTRUMP Final Verification and Validation Report." The staff has reviewed the application of the modified NOTRUMP code to the AP600 for SBLOCA analyses and provided its evaluation in Section 21.6.2 of this report.

- WCOBRA/TRAC-LBLOCA: As documented in WCAP-12945, this "best estimate" code has been approved by the NRC for large-break loss-of-coolant accident (LBLOCA) analyses. The modified version of the WCOBRA/TRAC code for the AP600 application is documented in WCAP-14171, "WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident." Its auxiliary code, HOTSPOT, is updated for the AP600 and documented in Westinghouse letter NSD-NRC-97-5171 dated June 10, 1997. The staff has reviewed and accepted the application of the modified WCOBRA/TRAC to the AP600 for LBLOCA analyses and provided its evaluation in Section 21.6.3 of this report.

- WCOBRA/TRAC-LTC and WGOTHIC: WCOBRA/TRAC is also used in the SSAR for the post-LOCA long-term cooling (LTC) analyses. The code verification for the long-term cooling analyses is documented in WCAP-14776, "WCOBRA/TRAC, OSU Long-Term Cooling Final Validation Report." The WGOTHIC code, documented in WCAP-14407, "WGOTHIC Application to AP600," is used to calculate containment boundary conditions for LBLOCA and post-LOCA long-term cooling. The staff has reviewed and accepted WCOBRA/TRAC and WGOTHIC for long-term cooling calculations. The staff's evaluations of these codes are provided in Sections 21.6.4 and 21.6.5 of this report, respectively.

Several of the computer codes used to analyze the Chapter 15 design-basis transients and accidents (e.g. LOFTRAN, NOTRUMP, and WCOBRA/TRAC) were under development when the staff's draft safety evaluation report (DSER) was issued. DSER Open Item 15.2-1 stated that the applicant should resubmit the Chapter 15 analyses with updated versions of the codes that have been verified and validated. Westinghouse has updated, verified, and validated these codes (as discussed in Chapter 21 of this report) and reanalyzed the Chapter 15 transients and accidents with the updated versions of the codes. Therefore, Open Item 15.2-1 is closed.

In the DSER, the staff identified Open Item 15.2-2, which stated that, because the mitigation of the design-basis accidents relies to a large extent on gravity, the differences in the elevations of various systems and components and the piping configurations that affect pressure drops are important factors in the mitigation capability; therefore the applicant should address the sensitivities of various system elevations and configurations (by sensitivity studies for example) to support the ITAAC implementation. In its response by a letter (NSD-NRC-97-5090) dated May 6, 1997, Westinghouse stated that the AP600 passive system designs have been analyzed with consideration for variations in parameters such as pipe routing, friction factors, equipment manufacturing variations and plant construction tolerances. These variations are bounded on both the minimum and maximum side for use in the SSAR safety analysis. The inspection, test, analysis, and acceptance criteria (ITAAC) are consistent with the performance variations used in the SSAR safety analysis. The staff finds the use of bounding values of safety analysis as ITAAC acceptance criteria to be acceptable. Discussion of ITAAC is provided in Section 14.3 of this report. Open Item 15.2-2 is closed.

## 15.2 Transient and Accident Analyses

The applicant presented the results of transient and accident analyses for the AP600 design in Chapter 15 of the SSAR. This section discusses the staff's evaluation of the analyses results and the applicant's responses to the staff RAIs. The staff's evaluation of the radiological consequences for various postulated events is presented in Section 15.3 of this report.

### 15.2.1 Increase in Heat Removal from the Primary System

In SSAR Section 15.1, the applicant presented the results of its analysis of the events involving an increase in heat removal from the primary system. The staff's evaluation of the analytical results is provided in the sections below.

#### 15.2.1.1 Decrease in Feedwater Temperature (SSAR Section 15.1.1)

Decrease in feedwater temperature, a moderate-frequency event, may be caused by failure of a low- or high-pressure heater train. A reduction in feedwater temperature decreases reactor coolant temperature, which, in turn, causes an increase in core power because of the effects of the negative moderator coefficient of reactivity. The applicant's analysis for the limiting case is based on initial full-power conditions with a decrease of feedwater temperature caused by loss of one string of low-pressure feedwater heaters. The decrease in feedwater temperature results in an increase in core power of less than 10 percent of full power. The results are bounded by an excessive increase in secondary steam flow (a moderate-frequency event), which results in a power increase of 15 percent. The staff's review of the event with an

excessive increase in secondary steam flow is discussed below in Section 15.2.1.3 of this report.

15.2.1.2 Increase in Feedwater Flow (SSAR Section 15.1.2)

Increase in feedwater flow events may be caused by system malfunctions or operator actions that result in an inadvertent opening of a feedwater control valve. The excessive feedwater flow reduces reactor coolant temperature, which, in turn, causes a power increase because of the effects of the negative moderator coefficient of reactivity. Continuous addition of excessive feedwater is prevented by the steam generator "High-2" water level signal trip, which closes the feedwater isolation valves and feedwater control valves and trips the turbine, main feedwater pumps, and reactor.

The applicant used three codes to perform the analysis for this event. The specific codes used are LOFTRAN for the transient response calculation, FACTRAN for the heat flux calculation, and THINC for the DNBR calculation.

For the no-load condition, the applicant assumed a feedwater control valve malfunction results in a step increase in flow to one steam generator from 0 to 115 percent of the nominal full-load value for one steam generator. The feedwater temperature is assumed to be at a low value of 4.4 °C (40 °F). In the response to RAI 440.717 provided by Westinghouse letter DCP/NRC 1109, dated October 29, 1997, the applicant made a comparative assessment for this event initiated from the zero-power condition. The assessment shows that this event is bounded by an uncontrolled RCCA bank withdrawal from a subcritical or low-power startup condition because of a lower reactivity insertion rate than the uncontrolled RCCA bank withdrawal event due to the effects of the negative moderator coefficient of reactivity. The analysis of an uncontrolled RCCA bank withdrawal event has been reviewed and approved by the staff in Section 15.2.4.1 of this report.

The applicant's analysis for the limiting case is based on initial full-power conditions with a increase of feedwater flow caused by malfunction of one feedwater control valve to its maximum capacity, resulting in a step increase to 115 percent of nominal feedwater flow to one steam generator. A reactor trip and an associated turbine trip are actuated on a steam generator "High-2" level trip signal. In addressing the issue of a LOOP, the applicant assumed that a LOOP and the resulting coastdown of the RCPs occurs 3 seconds after the turbine trip.

The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event. From the viewpoint of a steam generator overfilling, the worst case is a failure of the feedwater control valve in the affected steam generator to close combined with a single failure of the feedwater isolation valve to close. In this case, the analysis credits a steam generator "High-2" level trip signal to trip feedwater pumps and terminate the excessive feedwater flow. The staff notes that the feedwater pump trip is a non-safety-related system. The staff has reviewed and approves the use of the feedwater pump trip to terminate the excessive feedwater flow as discussed in Section 15.1.2 of this report.

The results of the analysis demonstrate that the limiting full-power case meets the acceptance criteria for this moderate-frequency event. Specifically, the calculated peak RCS pressure is below 110 percent of the RCS design pressure, and the calculated DNBRs for the transient

remains above the minimum DNBR defined in SSAR Section 4.4, thus satisfying the acceptable criteria defined in Section 15.1.2 of the SRP. Therefore, the staff concludes that the analysis is acceptable.

15.2.1.3 Excessive Increase in Secondary Steam Flow (SSAR Section 15.1.3)

Excessive increase in secondary steam flow may be caused by an operator action or an equipment malfunction in the steam dump control or turbine speed control. A rapid increase in steam flow results in a power mismatch between the reactor core power and the steam generator load demand.

The applicant analyzes four cases involving a 10-percent step load increase from rated load, using the LOFTRAN code, and assuming:

(1) minimum moderator feedback and manual reactor control
(2) maximum moderator feedback and manual reactor control
(3) minimum moderator feedback and automatic reactor control
(4) maximum moderator feedback and automatic reactor control

To demonstrate the capability of the plant for the cases with automatic rod control, the applicant took no credit for delta T trips on overpower and overtemperature. The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event, and determined that no single active failure in these systems or equipment would adversely affect the consequences of the event.

For the four excessive load increase cases discussed above, reactor and turbine trips are not predicted to occur. In consideration of the effects of a LOOP, the applicant assumed that a reactor trip and an associated turbine trip occur at the time of peak power. The LOOP is assumed to occur 3 seconds after the turbine trip.

The results of the analysis show that the calculated peak RCS pressure is less than 110 percent of the design pressure, and the calculated minimum DNBR does not violate the safety DNBR limits. Since the analysis uses acceptable methods and the results meet the acceptance criteria of SRP Section 15.1.3 for this moderate-frequency event, the staff concludes that the analysis is acceptable.

15.2.1.4 Inadvertent Opening of a Steam Generator (SG) Relief or Safety Valve (SSAR Section 15.1.4)

An inadvertent opening of a steam generator relief, safety, or steam dump valve may result in an increase in steam flow. The excessive cooldown increases positive reactivity in the presence of a negative moderator temperature coefficient.

To assess the effects of the negative moderator temperature coefficient, the applicant's analysis assumes the most negative moderator temperature coefficient corresponding to the end-of-life rodded core with the most reactive RCCA in its fully withdrawn position. Offsite power is assumed to be available to maximize the cooldown effect. The applicant has performed a comparative assessment. Since the initial SG water inventory for the no-load case

is greater, the magnitude and duration of the RCS cooldown resulting from steam releases is greater, and the associated positive reactivity addition is, therefore, also greater. Consequently, the applicant has determined that zero-power conditions are more limiting than at-power conditions for this postulated event. Since the turbine is initially in the trip condition for the plant at the zero-power, the consequential LOOP following the turbine trip is not considered a credible event and, therefore, is not modeled in the analysis.

The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event, and identified that the limiting single failure is a failure of one CMT discharge valve to open. In modeling the CMTs and accumulators, including the assumption of a failure of one CMT discharge valve to reflect the limiting single failure, the applicant minimized the capability to add borated water. The applicant also makes the following assumptions to maximize the cooldown effects:

- The maximum capacity for any single steam dump, relief, or safety valve is assumed as the initial steam flow.
- The Moody model, without consideration of the piping friction losses, is used to calculate the steam flow.
- The lowest startup feedwater temperature is assumed.
- Four reactor coolant pumps are initially operating.
- No moisture is assumed in the blowdown steam.
- Manual actuation of the passive residual heat removal system is assumed at the initiation of the event.

The applicant uses the LOFTRAN code to analyze the event. Based on the above discussion, the values used for input parameters are conservative. The results of the analysis show that the RCS pressure remains below 110 percent of the design pressure and the calculated minimum DNBR remains above the allowable safety limit DNBR, thereby satisfying the acceptance criteria in Section 15.1.4 of the SRP. Therefore, the staff concludes that the analysis is acceptable.

15.2.1.5 Steam System Piping Failure (SSAR Section 15.1.5)

A steamline break (SLB), a limiting-fault event, is defined as a pipe break in the main steam system. The steam release during an SLB causes a decrease in the RCS temperature and SG pressure. In the presence of a negative moderator temperature coefficient, the RCS temperature decrease results in an addition of positive reactivity. The SG pressure decrease initiates a reactor trip when low pressure in the SG system produces a safeguards "S" signal. The "S" signal initiates the actuation of the CMTs, which in turn initiates a trip of the RCPs. In addition, the "S" signal isolates all feedwater control and isolation valves and trips the main feedwater pumps. The low cold-leg temperature signal isolates the startup feedwater control and isolation valves. The reactor is ultimately shut down by the borated water from the CMTs.

The applicant uses the LOFTRAN code to calculate the system transient and the THINC code to determine whether departure from nucleate boiling (DNB) has occurred for the core transient conditions calculated by the LOFTRAN code. A double-ended rupture at no-load conditions with no decay heat is analyzed as the limiting case. Because the SGs have integral flow restrictors with a 0.13 $m^2$ (1.4 $ft^2$) throat area, any rupture with a break greater than 0.13 $m^2$ (1.4 $ft^2$), regardless of location, will have the same effect on the system as a 0.13 $m^2$ (1.4 $ft^2$) break, and so, this limiting break area is assumed in the analysis.

Because the average coolant temperature for a core tripped from at-power conditions is higher than at no-load and there is energy stored in the fuel, the RCS for a core tripped from at-power conditions contains more stored energy than at no-load. The additional stored energy reduces the cooldown caused by the SLB. Therefore, no-load conditions are more limiting than at-power conditions. To represent the limiting initial conditions and maximize the cooldown effect, the applicant assumed an initial condition for the SLB analysis of zero power with no stored energy in the fuel.

The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event. For an SLB in which a single failure results in a failure of the MSIV in the intact SG to close, the applicant takes credit for closing the non-safety-related MSIV backup valves (including the turbine-isolation and control valves) to avoid an uncontrolled blowdown from two SGs. This use of the MSIV backup valves in the SLB analyses for backup protection is acceptable as discussed in Section 15.1.2 of this report. In addition, in order to maximize the overcooling effect, the applicant made the following assumptions:

- The most reactive RCCA is in the fully withdrawn position after reactor trip.
- The end-of-life shutdown margin at zero-power, equilibrium xenon conditions exists at the time of the accident is initiated.
- A negative moderator coefficient for the end-of-life rodded core with the most reactive RCCA stuck out is assumed.
- The Moody model, without consideration of the piping friction losses, is used to calculate the steam flow.
- The lowest startup feedwater temperature is assumed.
- Four reactor coolant pumps are initially operating.
- No moisture is assumed in the blowdown steam.
- Manual actuation of the PRHR system is assumed at the initiation of the event.

Offsite power is assumed to be available to maximize the cooldown effect. The results of an SLB with offsite power available bounded the case with a LOOP for the following reasons:

- An initial condition of a LOOP results in an immediate RCP coastdown, which reduces the RCS cooldown effect and the magnitude of the return-to-power by reducing primary-to-secondary heat transfer.

- The plant protection system automatically provides a safety-related signal that initiates the coastdown of the RCPs coincident with CMT actuation. Since this RCP coastdown initiates early during the SLB event, the difference is insignificant in predicting the DNBRs for cases with and without offsite power.

- Because of the passive nature of the safety injection system, the LOOP will not delay the actuation of the safety injection system.

Westinghouse letter DCP/NRC, dated January 8, 1998, which responded to RAI 440.743F, addressed the staff's concern regarding identification of the limiting SLB case. In its response, the applicant analyzed two full-break SLB cases initiated with the reactor at full-power conditions, both with and without a LOOP. Consistent with the results presented in the SSAR, the full-power SLB analysis confirmed that the results for a case with offsite power available bounded the case with a LOOP at time zero. The results also showed that the maximum calculated fission power is sufficiently low, as compared to the value calculated for the zero-power case, that the calculated maximum nuclear power in the region of the stuck rod is less limiting than that calculated for the zero-power analysis presented in the SSAR. For both SLB cases initiated from full power and zero power, the predicted DNBR values meet the safety DNBR limits.

The staff concludes that the analysis for postulated SLBs is acceptable for the following reasons:

- The applicant has used the LOFTRAN code to perform the SLB analysis.

- The values used for input parameters are conservative.

- The results of the SLB analysis has shown that the minimum DNBR remains above the allowable safety limit DNBR, and the peak RCS pressure remains below 110 percent of the design pressure, thus satisfying the acceptance criteria of SRP 15.1.5 for an SLB analysis.

### 15.2.1.6 Inadvertent Operation of the Passive Residual Heat Removal System (SSAR Section 15.1.6)

The inadvertent actuation of the PRHR system may be caused by an operator action or a false actuating signal that opens the valves that normally isolate the PRHR heat exchanger from the RCS. This moderate-frequency event causes an injection of relatively cold water into the RCS and results in an addition of positive reactivity in the presence of a negative moderator temperature coefficient.

To assess the system response to this PRHR event, the applicant considered plant initial conditions both at full-power and zero-power. A comparative assessment shows that the zero-power condition is bounded by the analysis performed for the inadvertent opening of a steam generator relief or safety valve event (discussed in Section 15.2.1.4 of this report). This is because the latter event, a moderate-frequency event, is analyzed assuming the PRHR heat exchanger actuation coincident with SG depressurization. Therefore, the applicant's analysis for the limiting case is based on initial full-power conditions.

The codes used by the applicant to perform this analysis are LOFTRAN for the system response, FACTRAN for the heat flux, and THINC for the DNBRs. A negative moderator coefficient for the end-of-life rodded core is assumed, which will maximize the power increase in the transient. Control systems are assumed to function for the condition that their operation resulted in more severe conditions. Cases both with and without automatic rod control are considered.

The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event, and determined that no single active failure in these systems or equipment will adversely affect the consequences of the event.

In consideration of the effects of a LOOP, the applicant assumed that a reactor trip and an associated turbine trip occur at the time of peak power. A loss of power is assumed to occur 3 seconds after the turbine trip.

The staff finds the assumptions used in the analysis conservative for the reasons stated above, and, therefore, acceptable. The results of the analyses for the limiting full-power case with and without offsite power available show that the RCS pressure remains below 110 percent of the design pressure, and the minimum DNBR remains above the safety limit DNBR, thus satisfying the acceptance criteria of the SRP for moderate-frequency events. Therefore, the staff concludes that the analysis is acceptable.

15.2.2 Decrease in Heat Removal by the Secondary System (SSAR Section 15.2)

The applicant has analyzed transients specified in SRP Section 15.2 for cases resulting from a decrease in heat removal by the secondary system and identified the limiting case with regard to the capability of the RCS boundary and fuel rod cladding to withstand the consequences of transients. The results of the analyses and the staff review are discussed in Sections 15.2.2.1 through 15.2.2.8 below.

15.2.2.1 Steam Pressure Regulator Malfunction or Failure that Results in Decreasing Steam Flow (SSAR Section 15.2.1)

There are no steam generator pressure regulators in the AP600 design whose failure will cause a steam flow transient. Consequently, this event is not applicable to AP600.

15.2.2.2 Loss of External Electrical Load (SSAR Section 15.2.2)

The loss of external electrical load, a moderate-frequency event, may be caused by electrical system failures. Following the loss of generator load, an immediate fast closure of the turbine

control valves will occur. The reactor is protected by the reactor trips on high pressurizer pressure, high pressurizer water level, and overtemperature delta T signals. The pressurizer and the steam generator safety valves may lift to protect the RCS from overpressurization.

This event is bounded by the turbine trip event because the turbine control valves close more slowly than the turbine stop valves close as a result of a turbine trip event. The smaller reduction in heat removal due to a slower termination of steam flow will result in a lower peak RCS pressure. The staff's evaluation of the turbine trip analyses is discussed below in Section 15.2.2.3 of this report.

15.2.2.3 Turbine Trip (SSAR Section 15.2.3)

The turbine trip event may be initiated by signals resulting from a generator trip, low condenser vacuum, loss of lubricating oil, turbine thrust bearing failure, turbine overspeed, manual trip, and reactor trip. Following a turbine trip, the turbine stop valves rapidly close, and steam flow to the turbine abruptly stops. The loss of steam flow results in a rapid increase in secondary system pressure and temperature, as well as a reduction of the heat transfer rate in the steam generators: this in turn causes the RCS pressure and temperature to rise.

The codes used by the applicant to perform the analysis for this event are LOFTRAN for the transient response calculation, FACTRAN for the heat flux calculation, and THINC for the DNBR calculation. Initial core power, reactor power and pressure, and RCS temperature are assumed to be at their nominal values consistent with steady-state full-power operation. Uncertainties in initial conditions are included in the DNBR limit as described in WCAP-11397-P-A, "Revised Thermal Design Procedure." To maximize the RCS overpressurization effects, the turbine is assumed to trip without actuating the rapid power reduction system. This assumption delays the reactor trip until conditions in the RCS result in a trip actuated by other signals. The reactor is assumed to trip by the first reactor trip setpoint reached on high pressurizer pressure, overtemperature delta T, high pressurizer water level, or low steam generator water level trip signals. In addition, no credit is taken for the turbine bypass system. Main feedwater is terminated at the time of turbine trip, with no credit taken for startup feedwater or the PRHR system to mitigate the consequences of the event. The pressurizer safety valves are assumed to be available to reduce the pressure increase during the transient. To consider the effects of a LOOP, the applicant assumed that the power loss occurs 3 seconds after the turbine trip. The applicant also considered the plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these systems or equipment will adversely affect the consequences of the event.

In analyzing the turbine trip event, the applicant considered both minimum and maximum reactivity feedback cases. The applicant also considered the event with and without credit for the effect of pressurizer spray in reducing the reactor coolant pressure. The results of the applicant's analyses show that the most limiting case analyzed is a turbine trip from full-power with minimum moderator feedback. The limiting case assumes no offsite power available and takes no credit for the effect of pressurizer spray in reducing the RCS pressure. The calculated peak RCS pressure during the turbine trip transient is below 110 percent of the RCS design pressure, and the calculated minimum DNBR is within the safety DNBR limit, thus satisfying the acceptance criteria of Section 15.2.3 of the SRP. Therefore, the staff concludes that the analysis is acceptable.

15.2.2.4 Inadvertent Closure of Main Steam Isolation Valves (SSAR Section 15.2.4)

The inadvertent closure of steam isolation valves results in a turbine trip. The consequences of this event are the same as those of the turbine trip event discussed above in Section 15.2.2.3 of this report.

15.2.2.5 Loss of Condenser Vacuum (SSAR Section 15.2.5)

Loss of the condenser vacuum may result in a turbine trip and prevent steam from dumping to the condenser. Since the applicant assumed that the steam dump is unavailable in the turbine trip analysis, no additional adverse effects will result for the turbine trip event caused by loss of condenser vacuum. Therefore, the analytical results reviewed and discussed above in Section 15.2.2.3 of this report for the turbine trip event also apply to the loss of condenser vacuum event.

15.2.2.6 Loss of AC Power to the Plant Auxiliaries (SSAR Section 15.2.6)

The loss-of-ac power, a moderate-frequency event, may be caused by a complete loss of the offsite grid accompanied by a turbine-generator trip. This event is more severe than the turbine trip event because for this event, the decrease in heat removal by the secondary system is accompanied by an RCS flow coastdown, which further reduces the capacity of the primary coolant to remove heat from the core. The reactor will trip upon reaching one of the reactor trip setpoints in the primary and secondary systems as a result of the flow coastdown and decrease in secondary heat removal or as a result of the loss of power to the control rod drive mechanisms.

Following a loss-of-ac power with turbine and reactor trips, plant vital instruments are supplied from the Class 1E batteries and uninterruptible power supplies. As the SG pressure rises following the trip, the non-safety-related SG power-operated relief valves (PORVs) automatically open to the atmosphere. The condenser is not available for turbine bypass because of a loss-of-ac power. If the PORVs are not available, the SG safety valves may lift to remove the decay heat. As the no-load temperature is approached, the SG PORVs (or safety valves) are used to remove the decay heat and maintain the plant at the hot-shutdown condition (if the non-safety-related startup feedwater is available to supply the water to the SGs). The onsite standby power system, if available, will supply ac power to selected plant non-safety loads. If startup feedwater is not available, the PRHR heat exchanger will transfer the decay heat to the in-containment refueling storage tank (IRWST). After the IRWST water reaches saturation (in about 5 hours), steam starts to vent to the containment atmosphere, and condensation that collects on the containment steel shell (cooled by the passive containment cooling system) will return to the IRWST, maintaining the fluid level for the PRHR heat exchanger heat sink.

The applicant used the LOFTRAN code to perform a decay heat removal analysis to calculate the long-term cooling effect. Only safety-related systems are credited in the analyses to mitigate the consequences of the event. In the decay heat removal analysis, assumptions are made to minimize the energy removal capability of the PRHR heat exchanger and maximize the coolant system expansion. Initial reactor power is assumed to be 102 percent of the rated power level. The ANSI 5.1 decay heat data are used to represent the core residual heat

generation rate. A LOOP is assumed to occur after the reactor trip, which is actuated on a trip signal of low steam generator (narrow range) level. The assumption of a LOOP coincident with the reactor trip would minimize the SG water inventory for heat removal at the time of the reactor trip. In addition, the PRHR heat exchanger heat transfer coefficients are assumed to be at low values associated with the low flow rate caused by the RCP trip.

The applicant used the LOFTRAN, FACTRAN and THINC codes with the revised thermal design procedure described in WCAP-11397-P-A, "Revised Thermal Design Procedure," to perform DNBR calculations. In the analysis, initial reactor power, pressurizer pressure, and RCS temperature are assumed to be at their nominal values consistent with steady-state full-power operation. Uncertainties in initial conditions, as described in the revised thermal design procedure, are included in determining the DNBR limit during the transient. The SG safety valves and pressurizer safety valves are assumed to be functional for steam releases, and the CMTs are assumed to actuate when the PRHR HX cooled down the RCS enough to set off a low cold-leg temperature "S" signal.

To consider the effects of a LOOP, the applicant assumed that the power loss and the resulting coastdown of the RCPs occurred 3 seconds after the turbine trip. If the LOOP occurs at the start of the event, the calculated DNBR transient will be the same as predicted for the event involving a complete loss RCS flow, which is initiated by a LOOP at the beginning of the event. The results of the complete loss of RCS flow event are discussed in Section 15.2.3.2 of this report.

The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event, and determined that the worst single active failure is a failure to open in one of the two valves in the PRHR discharge line. The results of the analysis show that the calculated minimum DNBR meets the safety DNBR limit, and the long-term RCS heat removal capacity is sufficient to removal the decay heat. In addition, the results show that the peak RCS pressure does not exceed the RCS pressure limit and the integrity of the RCS is maintained. Thus, the SRP acceptance criteria for the loss-of-ac power are met, and the staff concludes that the analysis is acceptable.

15.2.2.7 Loss of Normal Feedwater Flow (SSAR Section 15.2.7)

A loss of normal feedwater flow, a moderate-frequency event, may be caused by feedwater pump failures, valve malfunctions, or a loss of ac power sources. Following an event involving a loss of normal feedwater, the SG water inventory decreases as a consequence of continuous steam supply to the turbine. The mismatch between the steam flow to the turbine and the feedwater leads to the reactor trip on a low steam generator level signal, which actuates the non-safety-related startup feedwater system (SFWS). As the SG pressure increases following the trip, the SG PORVs will automatically open to the atmosphere. If the SG PORVs are not available, the SG safety valves will lift to remove the decay heat.

As the no-load temperature is approached, the SG PORVs (or safety valves) will remove the decay heat and maintain the plant at the hot-shutdown condition if the SFWS is available to supply the water to the SGs. If the SFWS is not available, the PRHR HX will be actuated, either on a low SG water level (narrow range) coincident with a low startup feedwater rate signal or on a low-low SG water level (wide range) signal. The PRHR can transfer the decay heat to the

IRWST and provide a continuous core heat removal capability following a loss of normal and startup feedwater.

The analysis of this event is performed using the LOFTRAN computer code. Initial reactor power is assumed to be 102 percent of rated power. The relief of steam in the secondary system is assumed to be achieved through the SG safety valves. Upon initiation of the event, the reactor coolant volumetric flow is assumed to be at its normal value. The RCPs are assumed to continue running until they are automatically tripped by CMT actuation on a low cold-leg-temperature "S" signal. In the analysis, only safety-related systems are assumed to function to mitigate the consequences of the events. The PRHR HX is actuated on a low-low SG water level.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that the worst single active failure is a failure of one of the two valves in the PRHR discharge line to open. Based on the foregoing conditions, the calculated peak RCS and steam generator pressures are less than 110 percent of their design values. For the long-term cooling, the analysis demonstrates that the PRHR can remove core decay heat faster than it builds up during the transient.

In Westinghouse letter DCP/NRC 0990, dated August 14, 1997, the response to comment 17 stated that for DNBR calculations, a LOOP is assumed to occur 3 seconds after turbine trip. The impact of the LOOP is to cause a coastdown of the RCPs. The applicant has shown that a loss of normal feedwater transient event followed by the consequential LOOP after turbine trip is the same scenario presented in Section 15.2.6 of the SSAR for the loss-of-ac power analysis. Therefore, the calculated minimum DNBR, greater than the safety DNBR limits, for a loss-of-ac power event is bounding for an event involving the loss of normal feedwater.

Since the analysis uses approved methods and conservative inputs, and shows that the results meet the acceptance criteria of the SRP for the loss of normal feedwater event with respect to the pressure and safety DNBR limits, the staff concludes that the analysis is acceptable.

15.2.2.8 Feedwater System Pipe Break (SSAR Section 15.2.8)

A feedwater line break (FLB) is defined as a break in a feedwater line large enough to prevent the addition of sufficient feedwater to maintain shell-side water inventory in the steam generators.

The FLB may reduce the ability to remove heat generated by the core from the RCS because fluid in the SG is discharged through the break, and the break may be large enough to prevent the addition of main feedwater after the trip. During the event, the PRHR HX will function to prevent substantial overpressurization of the RCS and maintain sufficient liquid in the RCS to provide core coolability. A reactor trip may be actuated on signals of high pressurizer pressure, overtemperature delta T, low SG water level in either SG, low steamline pressure in either SG, and "High-2" containment pressure.

The applicant assumed the break occurs in a feedwater line between the check valve and the SG with a double-ended rupture of the largest feedwater line. This size is identified as the

limiting break case, resulting in the highest peak primary pressure. The double-ended break area assumed is 0.10 $m^2$ (1.12 $ft^2$).

The analysis of this event is performed with the LOFTRAN computer code. Reactor trip is assumed to be initiated when the low SG narrow-range level point is reached on the affected SG. To minimize the heat removal capability of the SG with the ruptured feedwater line, a saturated liquid discharge is assumed for the break fluid until all the water is discharged from the SG with the ruptured feedwater line. The PRHR HX is actuated by the low SG water level (wide range) with a delay time of 20 seconds to allow time for the alignment of PRHR HX valves. In addition, the applicant took no credit for the high pressurizer trip, for charging or letdown, or for energy deposited in RCS metal during the RCS heatup. During an FLB event, the engineered safety features (ESFs) required to function are the PRHR, CMTs, and steam isolation valves.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that the worst single active failure is a failure of one of the two valves in the PRHR discharge line to open. To consider the effects of a LOOP, the applicant assumed that the power loss and the resulting coastdown of the RCPs occurs 3 seconds after the turbine trip.

The staff noted that the non-safety-related pressurizer spray is credited for heat removal to limit the increase in the peak RCS pressure. Also, a low pressurizer safety valve setpoint is assumed in the analysis. Both assumptions could result in a lower peak RCS pressure. The staff asked the applicant to reanalyze the FLB event to quantify the effects of the pressurizer spray and a low pressurizer safety valve setpoint on the results of the FLB event. In Westinghouse letter DCP/NRC 0962, dated July 18, 1997, the response to comment 20 stated that the event was reanalyzed without pressurizer spray operable and with the pressurizer safety valve setpoint at its normal value. The confirmatory analysis shows that the peak RCS is 18.08 MPa (2624 psia), an increase of 27.6 kPa (4 psi) as compared to the SSAR case, and confirmed that the peak RCS pressure is within 110 percent of the design pressure.

The Semiscale test data for FLBs (as discussed in Section 4.3.3.1 of NUREG/CR-4945, dated July 1987) show that the SG heat transfer capacity remains unchanged until the steam generator liquid inventory is nearly depleted. This is followed by a rapid reduction to 0 percent heat transfer with little further reduction in the SG water inventory. In light of these test data, the staff asked the applicant to provide a discussion of the SG heat transfer model used in the FLB analysis and to verify that it is conservative as compared to the Semiscale test data. In Westinghouse letter DCP/NRC 0990, dated August 14, 1997, the response to comment 22 provided a discussion concerning the SG heat transfer model used in the FLB analysis. The SG heat transfer is calculated with the LOFTRAN code and is within the range of the Semiscale test data. To quantify the effects of the differences, the applicant provided the results of the SG heat transfer sensitivity study for the following three cases:

(1) FLB with the SG UA* set to normalized heat transfer from Semiscale 14.3 percent break
(2) FLB with the SG UA* set to normalized heat transfer from Semiscale 50 percent break
(3) FLB with the SG UA* set to normalized heat transfer from Semiscale 100 percent break

* Where U is the overall heat transfer coefficient and A is the heat transfer area

Cases 1, 2, and 3 are FLB cases using the heat transfer for the Semiscale tests for 14.3 percent, 50 percent, and 100 percent feedwater piping breaks, respectively. The calculated peak pressure of cases 1, 2, and 3 are 18.09 MPa (2624 psia), 18 MPa (2612 psia), and 17.36 MPa (2518 psia), respectively. The case with the heat transfer from the Semiscale 14.3 percent break is the limiting case, resulting in a peak pressure of 18.09 MPa (2624 psia). Compared to the peak pressure of 18.06 MPa (2620 psia) for the AP600 SSAR case, the limiting case with the Semiscale heat transfer shows a small increase of 27.6 kPa (4 psi) in the peak pressure.

Since the LOFTRAN calculated SG heat transfer is within the range of the Semiscale data and the sensitivity study shows that the effects of the heat transfer data differences between the Semiscale data and LOFTRAN model on the peak pressure are small, the staff concludes that the SG heat transfer model used in the FLB is acceptable.

The FLB analysis is performed with the LOFTRAN computer code. The results of the analysis show that the peak pressures of the RCS and SG are below 110 percent of the design pressures. For long-term cooling, the analysis demonstrates the core coolability by showing that the PRHR removes the core decay heat faster than it builds up. For DNBR calculations, a LOOP is assumed to occur 3 seconds after turbine trip and causes a coastdown of the RCPs. The applicant has shown that, for the first part of the transient up to the reactor trip and complete insertion of the control rods (where the minimum DNBR occurs), the system response for an FLB event is similar to the loss-of-ac power analysis presented in section 15.2.6 of the SSAR. Therefore, the calculated minimum DNBR, greater than the safety DNBR limits, for a loss-of-ac power is bounding for the FLB event.

Since the applicant uses NRC-approved methods and assumptions that are conservative with respect to maximizing RCS pressure and has shown that the results of the analysis meet the acceptance criteria of the SRP for the FLB break with respect to the pressure and safety DNBR limits, the staff concludes that the analysis is acceptable.

15.2.3 Decrease in Reactor Coolant System Flow Rate (SSAR Section 15.3)

The applicant has analyzed the transients specified in SRP Section 15.3 for cases resulting from a decrease in RCS flow rate. The applicant has also identified the limiting case with regard to ability of the RCS boundary and fuel rod cladding to withstand the consequences of transients. The results of the analyses and the staff's review are discussed in Sections 15.2.3.1 through 15.2.3.4 below.

15.2.3.1 Partial Loss of Forced Reactor Coolant Flow (SSAR Section 15.3.1)

Partial loss of RCS flow, a moderate-frequency event, may be caused by a mechanical or electrical failure in a RCP or by a fault in the power supply to the pumps supplied by an RCP bus. Protection against this event is provided by the low primary coolant flow reactor trip signal in any reactor coolant loop.

The computer codes the applicant used for analyzing the partial loss of flow event are LOFTRAN for the system response, FACTRAN for the heat flux calculation at the core hot spot, and WESTAR (WCAP-10951-A) for the DNBR calculation. The revised thermal design

procedure described in an NRC-approved report (WCAP-11397-P-A) is used to perform DNBR calculations. To maximize the core power and thus minimize the DNBR, the applicant used the least negative moderator temperature coefficient and a large absolute value of the Doppler coefficient. The RCP flow coastdown is calculated based on RCS pressure losses and RCP characteristics. Reactor coolant fluid momentum is neglected to obtain a low coastdown flow, which would result in lower calculated DNBRs.

To consider the effects of a LOOP, the applicant assumed that the power loss and resulting coastdown of the RCPs occur 3 seconds after the turbine trip. The analysis shows that the LOOP will have no effect on the calculated minimum DNBR since a rapid decrease in the heat flux significantly compensates for the decrease in the RCS flow caused by a LOOP following a turbine trip, and the minimum DNBR occurs before initiation of a LOOP.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these system or equipment adversely affects the consequences of the events.

The applicant analyzed an event involving the loss of two RCPs and presented the results in the SSAR. In Westinghouse letter DCP/NRC 0962, dated July 18, 1997, the response to comment 24 discusses other cases with loss of one and three RCPs. The applicant stated that the AP600 design has two electrical buses to supply power to the RCPs, with each of the two buses supplying power to two RCPs. Two RCPs sharing an electrical bus would be from opposing RCS loops. With this electrical design, one equipment fault in the RCPs could result in three different postulated events involving loss of RCPs:

(1) A loss one RCP because of an RCP fault or a breaker fault
(2) A loss of two RCPs in opposing RCS loops because of a bus fault
(3) A loss of four RCPs because of a complete loss-of-ac power to RCP buses.

Since an event involving the loss of three of the four RCPs is not credible, the consequences of the event are not analyzed. Case 3, the loss of four RCPs, is discussed below in Section 15.2.3.2 of this report. Comparing Cases 1 and 2, the core flow would be much lower for an event involving a loss of two RCPs (Case 2) than for an event involving a loss of one RCP (Case 1), assuming both occurred at the time of the reactor trip. Therefore, the results for an event with a loss of two RCPs are limiting and bound those events where only one RCP was lost.

The applicant uses NRC-approved methods and the values for input parameters are reasonably conservative. In addition, the results of the analysis for the limiting cases involving the loss of two RCPs show that with and without offsite power available, the RCS pressure will remain within 110 percent of the design pressure, and the minimum DNBR will remain above the safety DNBR limit. Consequently, the staff finds that the analysis meets the acceptance criteria of SRP Section 15.3.1 regarding the limits for the calculated RCS pressure and the minimum DNBR. Therefore, the staff concludes that the analysis is acceptable.

15.2.3.2 Complete Loss of Forced Reactor Coolant Flow (SSAR Section 15.3.2)

A complete loss of forced flow from RCPs may be caused by a simultaneous loss of electrical power to all RCPs. A LOOP and the resulting loss of all forced reactor coolant flow through the

reactor core causes an increase in the average coolant temperature and a decrease in the margin to DNB. The signals of low RCP speed or the low reactor coolant loop flow will trip the reactor.

For the case analyzed with a complete loss of flow, the method of analysis and the assumptions made for initial conditions and reactivity coefficients are identical to those for a partial loss of flow and are acceptable as discussed in Section 15.2.3.1 of this report. The results of the applicant's analysis show that the peak RCS pressure during the transient will remain below 110 percent of the system design pressure, and the calculated DNBR will remain above the design DNBR safety limit. Thus, the integrity of the RCS pressure boundary is not endangered, no fuel failure is predicted to occur, and core geometry and control rod insertability will be maintained with no loss of core cooling capability. The staff therefore finds that the analysis meets the acceptance criteria of SRP Section 15.3.2 with respect to the integrity of the RCS pressure boundary and the fuel rods. Thus, the staff concludes that the analysis is acceptable.

15.2.3.3 Reactor Coolant Pump Shaft Seizure (Locked Rotor) (SSAR Section 15.3.3) and Reactor Coolant Pump Shaft Break (SSAR Section 15.3.4)

RCP shaft seizure may be caused by an instantaneous seizure of an RCP rotor, and the RCP shaft break may be caused by an instantaneous failure of a RCP shaft. Both events are classified as limiting-fault events.

For both cases, flow through the affected reactor loop drops rapidly, leading to a reactor trip on a low-flow signal. After the reactor trip, energy stored in the fuel rods continues to be transferred to the coolant, causing the coolant temperature to increase and the coolant to expand. At the same time, heat transfer to the shell-side of the SGs drops because the reduced flow results in a decreased SG tube film coefficient and the reactor coolant in the tube-side cools down while the shell-side temperature increases. The rapid expansion of the coolant in the reactor core, combined with reduced heat transfer in the SGs, causes an insurge into the pressurizer and a pressure increase throughout the RCS. The insurge into the pressurizer compresses the steam volume, actuates the automatic spray system, and opens the pressurizer safety valves.

The analyses discussed in SSAR Sections 15.3.3 and 15.3.4 show that the RCP shaft seizure event with a LOOP bounds the RCP shaft break event with a LOOP. This is because the RCP flow coastdown for the shaft seizure event is slightly faster, resulting in a lower minimum DNBR.

The more limiting RCP shaft seizure is analyzed for cases with and without offsite power available. For cases without power available, a LOOP is assumed to occur at the time of reactor trip. A LOOP will cause a simultaneous loss of feedwater flow, condenser inoperability and coastdown of all RCPs. In the analysis, no credit is taken for restoration of offsite power before initiation of shutdown cooling.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these system or equipment adversely affects the consequences of the events. The analysis of this event is performed using the LOFTRAN code for the system response and the FACTRAN code for the heat flux calculation at the hot spot. Initial reactor power and pressure

and RCS temperature are assumed to be at their maximum values consistent with steady-state full-power operation and included allowances for calibration and instrument errors. The reactor trip is actuated on the low reactor coolant flow signal. No credit is taken for the pressure-reducing effects of pressurizer spray, steam dump, or controlled feedwater flow.

The results of the analysis show that the maximum RCS pressure will remain less than 110 percent of the design pressure and less than 18 percent of the fuel experience DNB. For the purpose of calculating dose releases, the applicant assumed that all fuel rods experiencing DNBR failed (18 percent of the fuel). The assumption of fuel failure for the dose calculation is consistent with the guidance of SRP Section 4.4 and, therefore, is acceptable. The staff's evaluation of the radiological calculations is discussed in Section 15.3 of this report.

The applicant uses NRC-approved methods with results that show the peak RCS pressure will remain within 110 percent of the design pressure, and the radiological release will remain within the 10 CFR 50.34(a)(1)(ii)(D)(*1*) limits. Therefore, the staff finds that the analysis for the RCP shaft seizure event meets the acceptance criteria of SRP Section 15.3.3 and is acceptable.

### 15.2.4 Reactivity and Power Distribution Anomalies (SSAR Section 15.4)

In SSAR Section 15.4, the applicant presented the analytical results of events resulting from reactivity and power distribution anomalies. The staff's evaluation of the analytical results is as follows.

#### 15.2.4.1 Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition (SSAR Section 15.4.1)

The applicant analyzed the consequences of an uncontrolled RCCA bank withdrawal from a subcritical or low-power startup condition. Such a transient may be caused by a malfunction of the reactor control or rod control systems.

For the analysis of this transient, the applicant used TWINKLE for the average power generation calculation, FACTRAN for the hot rod heat transfer calculation, and THINC for the DNBR calculation. The analysis assumes a conservatively small (in absolute magnitude) negative Doppler coefficient and the most positive moderator coefficient to maximize the peak heat flux. Power supplied to the RCCA banks is controlled so that no more than two banks can be withdrawn at the same time, and the banks must be withdrawn in their proper sequence. The analysis assumes that the reactivity insertion rate is equivalent to the simultaneous withdrawal of the two highest-worth banks at maximum speed 1.14 m per minute (45 inches per minute). Reactor trip is assumed to occur on the low setting of the power range neutron flux channel at 35 percent of full power. A 10-percent uncertainty has been added to the reactor trip setpoint value. The most limiting axial and radial power shapes, associated with having the two highest-worth banks in their high-worth position, are assumed in the DNBR calculation.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these system or equipment adversely affects the consequences of the event. Since the turbine is initially in the tripped condition for the plant at a subcritical or low-power startup condition, a consequential LOOP following the turbine trip is not a credible event and, thus, is not modeled in the analysis.

The results of the analysis for this event show that the maximum heat flux is much less than the full-power value and that average fuel temperature increases to a value lower than the nominal full-power value. The calculated minimum DNBR is above the safety DNBR limits.

The staff has reviewed the reactivity worths and reactivity coefficients used in the analysis and found their values to be conservative. The staff also reviewed the calculated consequences of this transient and found that they meet the requirements of GDC 10 in that the specified acceptable fuel design limits are not exceeded. The applicant also meets the requirements of GDC 20 in that the reactivity control system can be automatically initiated so that specified acceptable fuel design limits are not exceeded. In addition, GDC 25 is met in that a single malfunction in the reactivity control systems will not cause the specified acceptable fuel limits to be exceeded. Therefore, the staff finds that the analysis satisfies the acceptance criteria of SRP Section 15.4.1 and is acceptable.

15.2.4.2 Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (SSAR Section 15.4.2)

An uncontrolled withdrawal of an RCCA bank in the power operating range, a moderate-frequency event, may be caused by a malfunction of the reactor control or rod control systems. The effect of such an event is an increase in fuel and coolant temperature (as a result of the core-turbine power mismatch). Plant protection is provided by reactor trips, including the high neutron flux trip, overpower and overtemperature trips, and pressurizer pressure and pressurizer water level trips.

The computer codes used for the analysis of this transient are LOFTRAN for the RCS response, FACTRAN for the hot rod heat transfer calculation, and THINC for the DNBR calculation. The applicant also analyzed cases with both minimum and maximum reactivity coefficients, and performed a sensitivity study of the effects of initial power levels (10, 60, and 100 percent power) and reactivity insertion rates (from 1 pcm/s to 110 pcm/s) on the consequences of the event. The staff agrees that this sensitivity study is adequate to identify the limiting case with respect to power level and reactivity insertion rate. The maximum positive reactivity insertion rate is assumed to be greater than that for the simultaneous withdrawal of the combination of the two control banks, which results in the maximum combined worth at maximum speed. The high neutron flux signal is assumed to occur at 118 percent of nominal full power.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these systems or equipment adversely affects the consequences of the event. In addressing the LOOP issue, the applicant assumed that the power loss and the resulting coastdown of the RCP flow occurs 3 seconds after the turbine trip.

The results of the analysis show that the DNBR does not fall below the safety limit in any case. Therefore, fuel integrity and adequate fuel cooling are maintained. The calculated peak RCS pressure will remain less than 110 percent of the design pressure. The staff finds that the analysis meets the acceptance criteria of SRP 15.4.2 with respect to the integrity of the fuel and pressure boundaries and, therefore, is acceptable.

15.2.4.3 Rod Cluster Control Assembly Misalignment (SSAR Section 15.4.3)

RCCA misalignment incidents include a dropped full-length assembly, a misaligned full-length assembly, and withdrawal of a single RCCA during operation at power. Misaligned rods can be detectable by asymmetric power distributions sensed by incore or excore neutron detectors or core exit thermocouples, by rod deviation alarms, or by rod position indicators. The deviation alarm alerts the operator to rod deviation from the group position in excess of 5 percent of span.

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these systems or equipment adversely affects the consequences of the events. To consider the effects of a LOOP, the applicant assumed that a power loss and the resulting coastdown of the RCPs occurs 3 seconds after the turbine trip.

The staff's evaluation of the analyses for a dropped full-length assembly, a misaligned full-length assembly, and withdrawal of a single RCCA during operation at power is as follows.

15.2.4.3.1 Analysis for a Dropped Full-Length Assembly

For an event with one or more RCCAs dropped from the same group, the core power decreases and the core radial peaking factor increases. The reduced core power and continued steam supply to the turbine cause the reactor coolant temperature to decrease. In the manual control mode, the positive reactivity feedback causes the reactor power to rise to the initial power level at a reduced inlet temperature with no power overshoot. In the automatic control mode, the plant control system detects the reduction in core power and initiates control bank withdrawal in order to restore the core power. As a result, power overshoot occurs, resulting in a lower calculated DNBR. The applicant determined that the automatic operating mode bounded the manual operating mode and is the limiting DNBR case. This conclusion is reasonable.

The applicant analyzed the rod drop events in the automatic control mode using the LOFTRAN code for the system response and THINC code for the DNBR calculation. The results show that the calculated minimum DNBR is greater than the safety limit DNBR for any single or multiple RCCA drop from the same group and the peak RCS pressure will remain less than 110 percent of the design pressure. The staff finds that the analysis has satisfied the acceptance criteria of SRP Section 15.4.3 and therefore, concludes that the analysis for the rod assembly drop event is acceptable.

15.2.4.3.2 Analysis for a Misaligned Full-Length Assembly

For rod misalignment situations, the applicant analyzed the two most limiting DNBR cases, including (1) RCCA misalignments in which one RCCA is fully inserted with the rest of the RCCAs at or above their insertion limits, and (2) cases in which a group is inserted to its insertion limit and a single rod in the group is stuck in the fully withdrawn position. In the analysis, the initial reactor power, pressurizer pressure, and RCS temperature are assumed to be at their nominal values consistent with steady-state full-power operation. The radial peaking factor associated with the misaligned RCCA for these two limiting cases was calculated by the applicant. Uncertainties in initial conditions as described in WCAP-11397-P-A, "Revised

Thermal Design Procedure," are included in determining the DNBR limit during the transient. The analysis shows that the minimum DNBR is above the safety DNBR limit. The staff concludes that the analysis is acceptable since it meets the acceptance criteria of SRP Section 15.4.3.

15.2.4.3.3 Analysis for Withdrawal of a Single RCCA

The inadvertent withdrawal of a single assembly requires multiple failures in the control system, multiple operator errors, or deliberate operator actions combined with a single failure of the control system. The single assembly withdrawal is classified by the applicant as an infrequent occurrence for the AP600 design consistent with what the staff approved for Westinghouse operating plants. The transient resulting from such an event is similar to that resulting from a bank withdrawal, but the increased peaking factor caused DNB to occur in the region surrounding the withdrawn assembly. The radial peaking factor associated with the single RCCA withdrawal was calculated by the applicant. Uncertainties in initial conditions as described in WCAP-11397-P-A, "Revised Thermal Design Procedure," are included in determining the DNBR limit during the transient. Westinghouse letter DCP/NRC-0962, dated July 18, 1997, stated in its response to comment 33 that less than 2.5 percent of the rods in the core experienced DNB in such a transient. For the purpose of calculating dose releases, the applicant assumed that 5 percent of the fuel rods are failed. The assumption of fuel failure for the dose release calculation is more limiting than the guidance of SRP Section 4.4, which would only require failure of 2.5 percent of the fuel rods to be considered (i.e., the SRP states that all rods which experience DNB should be assumed to fail). Therefore, the staff concludes that the assumption is acceptable.

For the single rod withdrawal event (an infrequent event), the applicant has meets the requirements of GDC 27 by demonstrating that the resultant fuel damage is limited such that control rod insertability is maintained, and no loss of core coolability results. The DNBR calculation shows that a small fraction (2.5 percent) of the fuel rods may experience cladding perforation. Therefore, the staff concludes that the analysis is acceptable.

15.2.4.4 Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature (SSAR Section 15.4.4)

Starting an idle RCP increases the injection of cold water into the core, which causes a reactivity insertion and subsequent power increase. The applicant has provided an analysis for an event involving the startup of an inactive RCP in SSAR Section 15.4.4.

In the analysis, the applicant assumed initial conditions of maximum core power (70 percent of nominal value corresponding to the three RCP operating conditions), maximum reactor coolant temperature and minimum reactor coolant pressure to minimize the initial DNBR value. The most negative moderator coefficient and the least negative Doppler coefficient are assumed to maximize the power increase rate. Following startup of the idle pump, the inactive pump flow rate is assumed to accelerate linearly to its nominal full flow rate in 4 seconds. The reactor trip is assumed to occur on low coolant pump flow when the power range neutron flux exceeds 84 percent of rated power. The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and

determined that no single active failure in these system or equipment adversely affected the consequences of the events.

The applicant used the LOFTRAN, FACTRAN, and THINC computer codes to perform the analysis for this event. The results of the analysis show that the maximum calculated RCS pressure will remain less than 110 percent of the design pressure and the minimum DNBR will remain above the safety DNBR limit. The staff finds that the results of this analysis are in conformance with the acceptance criteria of SRP Section 15.4.4. Therefore, the staff concludes that the analysis is acceptable.

15.2.4.5 A Malfunction or Failure of the Flow Controller in a Boiling-Water Reactor Loop that Results in an Increased Reactor Coolant Flow (SSAR Section 15.4.5)

This section is not applicable to the AP600 design.

15.2.4.6 Chemical and Volume Control System Malfunction That Results in the Boron Dilution in the Reactor Coolant (SSAR Section 15.4.6)

The main causes of an inadvertent boron dilution are failures of the demineralized water transfer and storage system (DWS) or chemical and volume control system (CVS) because of control operator error or mechanical failure. The CVS is designed to limit the dilution rate to values which allow sufficient time for automatic or operator actions to terminate the dilution before the shutdown margin is lost. The dilution rate is indicated by instrumentation. An inadvertent boron dilution from the DWS through the CVS is terminated by isolating the makeup pump suction line to the DWS storage tank. The applicant has analyzed the boron dilution event for all modes of operation. The analytical method used by the applicant is consistent with NRC-approved methods for the Westinghouse operating plants. The method consists of a generic fluid mixing model. The nodal scheme in the model includes a node to represent the RCS volume and a flow path to represent CVS fluid transportation. The method with appropriate values of the initial RCS water volume and CVS flow rate is applicable to the AP600 analysis. The staff's review of the analysis is as follows.

15.2.4.6.1 Dilution During Refueling (Mode 6)

Uncontrolled boron dilution is not a credible event during the refueling mode because administrative controls isolate the RCS from the potential source of unborated water by locking closed specified valves in the CVS system during this mode of operation. Makeup water during refueling is supplied from the boric acid tank which contains borated water.

15.2.4.6.2 Dilution During Modes 4 and 5 of Operations

In Modes 4 and 5, the analysis assumes that the dilution flow rate is 12.6 L/sec (200 gpm) of unborated water, which bounds the flow rate of 11 L/sec (175 gpm) limited by a flow restrictor located in the discharge line of the CVS. The analysis also assumes a shutdown margin of 1.6 percent delta K/K, and Initial RCS water volumes of 73.7 $m^3$ (2601 $ft^3$) for Mode 4 and 63.6 $m^3$ (2245 $ft^3$) for Mode 5. For Mode 4, the volume is the minimum water volume of the RCS when the normal residual heat removal system (RNS) is used to remove the decay heat. For Mode 5, the volume is the minimum RCS water volume corresponding to the water level at mid-loop operations. The source range nuclear instrumentation is assumed to actuate an alarm

in the control room and close the DWS isolation valves when the neutron flux increased by 60 percent over any 50-minute period. The analysis shows that these actuations by the source range instrumentation will prevent the core from returning to criticality.

15.2.4.6.3 Dilution During Hot Standby (Mode 3)

Mode 3 differs from the preceding cases because the initial RCS water volume for Mode 3 is 162.4 $m^3$ (5737 $ft^3$). This is the minimum RCS water volume with the RCS filled in Mode 3. The analysis shows that the source range instrumentation will provide the same protection for this case as for the preceding cases.

15.2.4.6.4 Dilution During Startup (Mode 2)

During this mode of operation, rod control is in manual. The applicant performed an analysis of inadvertent deboration at initial conditions representative of the startup mode of operation with an assumed unborated water flow rate of 12.6 L/sec (200 gpm). The results of the analysis show that a reactor trip from a signal on the intermediate range neutron flux will initiate closure of the DWS isolation valves, terminate the boron dilution and maintain the plant in a subcritical condition.

15.2.4.6.5 Dilution During Power Operation (Mode 1)

For this portion of the analysis, the applicant analyzed both the manual mode and the automatic mode cases. For the manual mode case, the analytical result shows that a reactor trip on the overtemperature delta T will initiate closure of the DWS isolation valves and terminate the boron dilution without a post-trip return-to-criticality occurring. Since a reactor trip isolates DWS valves and terminates the event, the subsequent LOOP assumption following a turbine trip (which occurs immediately after a reactor trip) as required by GDC 17 will not affect the results of the deboration event for the case in manual mode.

For the automatic mode case, an increase in the power and temperature caused by a boron dilution event is compensated by slow insertion of the control rods to avoid the reactor trip. Since a reactor and turbine trip do not occur as predicted in the analysis for the case in automatic mode, the subsequent LOOP event following a turbine trip (as required by GDC 17) is not a credible event, and thus, is not modeled in the analysis. For the AP600 design, redundant pre-trip alarms available to the operator for Mode 1 operation include a low-level rod insertion limit alarm and an axial flux difference alarm. The analysis shows that the minimum possible time interval from a pre-trip alarm attributable to boron dilution to loss of shutdown margin is greater than 61 minutes. The staff finds that the applicant has demonstrated compliance with the guidance of SRP Section 15.4.6 in that the redundant pre-trip alarms alert the operator to initiation of the event in sufficient time to ensure detection of the boron dilution event at least 15 minutes before possible loss of shutdown margin (for a core with the control rods inserted).

The staff asked the applicant to validate the fluid mixing model used for the boron dilution analysis. In Westinghouse letter DCP/NRC-1248, dated February 6, 1998, the response to RAI 440.754F stated that the boron mixing model used in the analysis is consistent with the model used for existing plants. To validate the model, the applicant evaluated the flow regime through

the reactor vessel with the minimum flow of 63 L/sec (1000 gpm) as specified in TS 3.4.9. The evaluation shows that the flow through the reactor downcomer and lower plenum is turbulent, and thus, supports the assumption that the fluid in the reactor is well mixed. However, the staff notes that fluid in the entire RCS volume is assumed to mix uniformly with the incoming diluted fluid. This assumption may not be conservative for cases with low RCS flow rates because the transport time for the diluted fluid in the downcomer to reach the core is neglected in the deboration analysis. To address the concern on uncertainties associated with the flow mixing model at low RCS flow, the applicant modified the LCO in TS 3.4.9 from "RCS flow in the reactor vessel shall be $\geq$ 1000 gpm" to "At least one reactor coolant pump shall be operating" during Modes 3, 4 and 5. The modified TS will preclude potential boron dilution events when the RCPs are not running by isolating the demineralized water isolation valves (DMIV). With this TS change, the minimum RCS flow rate during Modes 3, 4 and 5 with the DMIVs open and one RCP operating is greater than 3280 L/sec (52,000 gpm), which is sufficient to support the assumption of the complete mixing in the model used for the boron dilution analysis.

The staff concludes that the analyses for inadvertent deboration events for all modes of operation are acceptable. For Modes 2 through 6, the analytical results show that no return-to-criticality occurs, thus ensuring the integrity of the fuel and RCS pressure boundary. For Mode 1, a sufficient time is available to satisfy the guidance in SRP Section 15.4.6 and enable the operator to detect and terminate the event before loss of shutdown margin for a post-trip core.

15.2.4.7 Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position (SSAR Section 15.4.7)

During fuel loadings, the applicant will follow strict administrative controls, in the form of previously approved and established procedures and startup testing, to prevent operation with a misplaced fuel assembly or a misloaded burnable poison assembly. Nevertheless, the applicant has performed an analysis of the consequences of a loading error. The staff reviewed this event in accordance with SRP Section 15.4.7 and the requirements of GDC 13.

The applicant used the NRC-approved methods documented in WCAP-10965-P-A, "ANC: Westinghouse Advanced Nodal Computer Code," to perform the analysis for this event. In SSAR Figures 15.4.7-1 through 15.4.7-4, the applicant provided comparisons of power distributions calculated for the nominal fuel loading pattern and those calculated for four loadings with misplaced fuel assemblies or burnable poison assemblies. The selected non-normal loadings represent the spectrum of potential inadvertent fuel misplacement. Calculations include, in particular, the power in assemblies that contain provisions for monitoring with incore detectors.

As part of the startup testing (SSAR Section 14.2.10.4.2), the incore detector system will be used to detect misloaded fuel before operating at power. The analyses described above show that resulting power distribution effects will be either detected by the startup test involving the incore detector system or cause an acceptable small perturbation within the measurement uncertainty of 5 percent. The testing requirements and the results of the analysis demonstrate that the applicant has met the requirements of GDC 13 with respect to minimizing the possibility that a misloaded fuel assembly (an AOO) goes undetected (and minimizes the consequences of reactor operation in the event of inadvertent fuel misload).

The staff has reviewed the consequences of the spectrum of postulated fuel loading errors and found that the analyses provided by the applicant shows, for each case considered, that either the error will be detectable by the available instrumentation (and hence remediable) or the error will be undetectable, but the offsite consequences of any fuel rod failures is a small fraction of 10 CFR 50.34(a)(1)(ii)(D)(*1*) limits, thus satisfying the acceptance criteria of SRP Section 15.4.7. Therefore, the staff concludes that the analysis is acceptable. The staff's evaluation of the radiological consequences is discussed in Section 15.3 of this report.

15.2.4.8 Spectrum of Rod Cluster Control Assembly Ejection Accidents (SSAR Section 15.4.8)

The mechanical failure of a control rod mechanism pressure housing may result in the ejection of an RCCA. For assemblies initially inserted, the consequences are a rapid reactivity insertion together with an adverse core power distribution, possibly leading to localized fuel rod damage. Although mechanical provisions have been made to render this accident extremely unlikely, the applicant has provided its analysis of the consequences of such an event. The applicant has considered plant systems and equipment discussed in SSAR Section 15.0.8 that are available to mitigate the effects of the event, and determined that no single active failure in these system or equipment adversely affects the consequences of the events. The staff has reviewed this analysis in accordance with SRP Section 15.4.8.

Methods used in the analysis are documented in WCAP-7588, Revision 1A, "An Evaluation of the Rod Ejection Accident in Westinghouse Pressurized Water Reactors Using Spatial Kinetics Methods," which the staff has previously reviewed and accepted. This report demonstrates that the model used in the accident analysis is conservative with regard to a three-dimensional kinetics calculation.

In this analysis, the applicant considered four cases including beginning-of-cycle at full-power and zero-power, and end-of-cycle at full-power and zero-power. For all cases, the calculated radial average fuel enthalpy is less than 182 calories per gram, which is less than the acceptance criterion of 280 calories per gram specified by RG 1.77, "Assumptions Used for Evaluating a Control Rod Ejection Accident for PWRs." In addition, the calculated pressure surge resulting from the rod ejection does not exceed the reactor coolant system emergency limits (Service Level C) and, thus, satisfies the guidance of RG 1.77.

To consider the effects of a LOOP, the applicant assumed that the power loss resulting in coastdown of the RCPs occurs 3 seconds after the turbine trip. The applicant has shown that the effect of a LOOP on the calculated minimum DNBR is negligible because a rapid decrease in the heat flux compensates for the decrease in the RCS flow caused by a LOOP, and the minimum DNBR occurs before initiation of a LOOP.

In Westinghouse letter DCP/NRC-0962, dated July 18, 1997, the response to comment 40 stated that less than 15 percent of the fuel rods experienced DNB as a result of the rod ejection event. For the purpose of calculating dose releases, the applicant assumed that all fuel rods (15 percent of the fuel) experiencing DNB failed. The assumption of fuel failure for the dose calculation is consistent with the guidance in SRP Section 4.4 and therefore, is acceptable.

Recent experimental data show failures of high burnup fuels at lower enthalpies than the fuel failure enthalpy limits specified in RG 1.77. However, generic analyses performed by

Westinghouse that assumed low enthalpy fuel failures showed that the radiological consequences of rod ejection accidents meet the acceptance criteria specified in SRP Section 15.4.8 (Appendix A). The generic analyses are documented in a Westinghouse submittal, NTD-NRC-95-4438, "Westinghouse Assessment of Topical Report Validity for Reactivity Insertion Accidents with High Burnup Fuel." The staff indicated that the applicant did not address the applicability of these analyses to AP600. In Westinghouse letter DCP/NRC-1229, dated January 26, 1998, the response to RAI 440.744F stated that the AP600 fuel rod contains $UO_2$ fuel and its cladding is ZIRLO with dimensions the same as those in current operating plants, and confirmed that the analyses in NTD-NRC-95-4438 are applicable to AP600 design. The analyses are predicated on conservative treatment of the experimental fuel data applied to existing and planned cores operating within approved burnup limits for Westinghouse reactors. In addition, there is broad agreement among the staff, the industry, and international community that burnup degradation in the margin to low-enthalpy fuel failure is likely to be regained by application of more detailed 3-dimensional analysis methods of the fuel response to rod ejection accidents. Therefore, the staff concludes that, although the RG 1.77 fuel failure enthalpy limits may not be conservative, the analyses in NTD-NRC-95-4438 provide reasonable assurance that radiological consequences of rod ejection accidents will not violate the acceptance criterion in SRP Section 15.4.8 for the AP600 core operating within the current NRC approved burnup limits (60 GWD/MTU average in the peak rod). The staff will not approve further extension of burnup limits until additional experimental information on fuel behavior is available to demonstrate that the fuel cladding will satisfy the regulatory acceptance criteria used in the rod ejection analyses for licensing applications.

### 15.2.5 Increase in Reactor Coolant System Inventory (SSAR Section 15.5)

In SSAR Section 15.5, the applicant considered two cases which would result in an in an increase in the RCS inventory. These cases are (1) an inadvertent operation of the CMTs, and (2) malfunction of the CVS. Discussion of the applicant's analyses and the staff's evaluation are below.

#### 15.2.5.1 Inadvertent Operation of the Core Makeup Tank During Power Operation (SSAR Section 15.5.1)

The applicant assessed the effects of spurious CMT operations at power that are caused by operator actions, a false electrical actuation signal, or a valve malfunction. The SSAR presents the results of the most limiting case, an inadvertent CMT operation resulting from a spurious "S" signal. The applicant analyzed the case using the LOFTRAN code. A sensitivity study, documented in the response to RAI 440.725, as provided by Westinghouse letter DCP/NRC-1115, dated October 31, 1997, was performed to determine the set of initial plant conditions that resulted in a minimum margin with respect to the pressurizer filling. The following initial conditions were established as a result of the sensitivity study to maximize the water level in the pressurizer:

- The reactor power is at 102 percent of nominal; the pressure is at 344.7 kPa (50 psi) below nominal and RCS temperature is at 3.6 °C (6.5 °F) above nominal.

- The pressurizer spray system and automatic rod control are operable.

- A least-negative moderator temperature coefficient, a low (absolute) Doppler power coefficient, and a maximum boron worth are assumed.

The CMT enthalpies are maximized to minimize the cooling provided by the CMTs. CMT injection and balance lines pressure drop is minimized to maximize the CMT flow injected into the primary system. Also, a minimum PRHR heat transfer is assumed for the decay heat removal.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and has identified the worst single failure as one of the two PRHR parallel isolation valves failing closed. In addressing the issue of a LOOP, the applicant assumed that a power loss resulting in a coastdown of the RCPs occurs 3 seconds after the turbine trip.

The analysis assumes that the event is initiated by an inadvertent opening of the CMT discharge valves which results in the two CMTs injecting borated water. The reactor is tripped upon receipt of the "S" signal on the "High-3" pressurizer level. Following reactor trip, the reactor power dropped and average RCS temperature decreased with subsequent coolant shrinkage. The CMT injection made up the RCS shrinkage and at 1 minute after actuation of the "High-3" pressurizer level signal, the "High-3" pressurizer level setpoint is once again reached. The PRHR, with appropriate delay time, was then assumed to initiate. The primary and secondary pressures increased initially because of the assumed unavailability of the non-safety-related control systems, but eventually decreased as the PRHR removed the core decay heat. At about 1.9 hours, the pressurizer water volume stopped increasing as the PRHR heat flux approached the core heat flux. After about 2.8 hours into the transient, the PRHR heat flux matched the core decay heat. The CMTs stopped recirculating at 5 hours into the transient.

In an NRC quality control inspection at Westinghouse from November 17 through 21, 1997, the staff found that in some scenarios, operator actions are necessary (opening of the reactor vessel head vents) to prevent the pressurizer from overfilling with water. However, the applicant had not provided a technical specification or an ITAAC for the reactor vessel head vents (RVHV) to ensure that they will reliably function as assumed in the design basis analysis. In Westinghouse letter DCP/NRC-1248, dated February 6, 1998, the applicant's response to RAI 440.753F proposed limiting conditions for operation in TS 3.4.17 to require that the RVHVs be operable for Modes 1 through 3. In addition, the TS LCO is applicable in Mode 4 when the RCS is not being cooled by the normal decay heat removal system (RNS). The surveillance requirements are specified to be consistent with the inservice testing program. The staff has reviewed the proposed TS and found that the LCOs, required actions, and surveillance requirements are consistent with a typical TS for the RVHVs. The staff therefore concludes that the TS is acceptable. To verify the flow capability, the applicant included the RVHVs in RCS ITAAC 2.1.2 and also required verification of the capacity of the RVHVs to be greater than 3.73 kg/sec (8.2 lbm/sec) at the RCS pressure of 8.63 MPa (1250 psia). The acceptance criteria in the ITAAC for the flow conditions ensure the minimum RVHV flow assumed in the design basis analysis will be available for mitigation of this event. The staff therefore, concludes that the added ITAAC for the RVHVs is acceptable.

The applicant uses the LOFTRAN code for the analysis, and the results show that no RCS water is relieved through the pressurizer safety valves as a result of the transient. In addition, the calculated minimum DNBR remains above the safety limit values and the RCS and SG pressures remain below 110 percent of their respective design pressures. The staff finds that the analysis meets the acceptance criteria of SRP Section 15.5.1 and therefore, concludes that the analysis is acceptable.

15.2.5.2 Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory (SSAR Section 15.5.2)

A CVS malfunction may result in an event which increases RCS inventory. The CVS malfunction may be caused by operator action, an electrical actuation signal, or valve failure. The applicant has analyzed CVS malfunction cases using the LOFTRAN code. A sensitivity study has been performed to determine a set of initial plant conditions that results in a minimum margin with respect to the pressurizer filling. The following initial conditions were established as a result of the sensitivity study to maximize the water level in the pressurizer:

- The reactor power is at 102 percent of nominal, the pressure is at 344.7 kPa (50 psi) above nominal and RCS temperature is at 3.6 °C (6.5 °F) above nominal.

- The pressurizer spray system is operable.

- A least-negative moderator temperature coefficient, a low (absolute) Doppler power coefficient, and a maximum boron worth are assumed.

- The initial boron concentration was chosen on the basis of an iterative analysis process, such that the limiting case bounds the cases that modeled explicit operator actions after the reactor trip.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and has identified the worst single failure as one of the two PRHR parallel isolation valves failing closed. In addressing the issue of a LOOP, the applicant assumes that a power loss resulting in a coastdown of the RCPs occurs 3 seconds after the turbine trip.

The analysis assumes that the event is initiated by a CVS malfunction that results in injection from two CVS pumps. As the CVS injection flow increases RCS inventory, pressurizer water volume begins increasing while the primary system is cooling down. The RCS temperature decreases to reach the low cold-leg temperature setpoint and actuates an "S" signal, resulting in a reactor trip. Following the trip, the turbine is tripped and after 3-second delay, a consequential LOOP is assumed and the RCPs are tripped. Soon after the reactor trip, the pressurizer heaters are blocked and main feedwater lines, steamlines and the CVS are isolated. After a delay of 22 seconds following the "S" signal, the CMT discharge valves are opened and the PRHR HX is actuated. The operation of the PRHR HX and CMTs cools down the plant, but the pressurizer level still continues to increase because of the expansion of the CMT water. At about 6 hours into the transient, the pressurizer water volume stops increasing as the PRHR heat flux approaches the core heat flux. After about 6.1 hours, the PRHR heat flux matches the core decay heat and the CMTs stop recirculating.

The applicant uses the LOFTRAN code for the analysis with conservative inputs, and the results show that no RCS water is relieved from the pressurizer safety valves. In addition, the calculated minimum DNBR remains above the safety limit values, and the RCS and SG pressures remain below 110 percent of their respective design pressures. The staff finds that the analysis meets the acceptance criteria of SRP Section 15.5.2 and is acceptable.

15.2.6 Decrease in Reactor Coolant Inventory (SSAR Section 15.6)

In SSAR Section 15.6, the applicant provided analyses of events that may decrease the reactor coolant system inventory.

15.2.6.1 Inadvertent Opening of a Pressurizer Safety or Inadvertent Operation of the ADS (SSAR Section 15.6.1)

An accidental depressurization of the RCS may occur as a result of an inadvertent opening of a pressurizer safety valve or automatic depressurization system (ADS) valves. During the transient, the RCS pressure rapidly decreases and, in turn, causes a decrease in power because of the moderator density feedback. The pressurizer level may eventually drop far enough to cause a reactor trip on a low pressurizer level signal.

The ADS consists of four stages of depressurization valves which are interlocked such that stage 1 is initiated first with subsequent stages actuated only after previous stages have been actuated. The AP600 design prohibits opening of the fourth-stage valves while the RCS is at nominal operating pressure. For inadvertent operation of the ADS valves, the applicant considers an opening of both first-stage ADS flow paths to be the limiting case because operation of these valves results in a greater depressurization rate than ADS stages 2 and 3 valves because of the shorter valve opening time.

The applicant also analyzed an inadvertent opening of the pressurizer safety valve. The flow area of the pressurizer valve is smaller than the combined two first-stage ADS valves; however, the safety valves open more rapidly than the ADS valves.

Normal reactor control systems are assumed not to function. The rod control system is assumed to be in automatic mode in order to maintain the core at full-power until the reactor trip protection function is reached.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and determined that no single active failure in these systems or equipment adversely affected the consequences of the event. In addressing a LOOP, the applicant assumed that a power loss resulting in a coastdown of the RCPs occurs 3 seconds after the turbine trip. The analysis showed that there is no effect of a LOOP on the calculated minimum DNBR since a rapid decrease in the heat flux compensates for the decrease in the RCS flow caused by the LOOP (which would follow a turbine trip) and that the minimum DNBR occurs before initiation of a LOOP.

The codes used by the applicant to perform the analysis for these events are LOFTRAN for the transient response calculation, FACTRAN for the heat flux calculation, and THINC for the DNBR calculation. These RCS valve opening events are analyzed using the revised thermal

margin procedure. Initial core power, reactor power and pressure, and RCS temperature are assumed to be at their nominal values consistent with steady-state full-power operation. Uncertainties in initial conditions are included in the DNBR limit as described in WCAP-11397-P-A. The reactor trip is assumed to actuate on a pressurizer low pressure trip signal.

The applicant analyzed the events using acceptable methods. The analysis shows the DNBR remains above the safety limiting value and the RCS pressure remains less than 110 percent of the design pressure throughout the transients. The staff finds that the analysis meets the acceptance criteria of SRP Section 15.6.1 and is acceptable.

15.2.6.2 Failure of Small Lines Carrying Primary Coolant Outside Containment (SSAR Section 15.6.2)

The reactor coolant may be directly released from a break or leak outside containment in a CVS discharge line or sample line. The applicant has identified that the worst case event is the double-ended break of the sample line between the isolation valve outside the containment and the sample panel. This sample line break results in the largest release of reactor coolant outside containment. The maximum break flow is limited to 8.2 L/sec (130 gpm) by the sample line orifices.

Both the isolation valves inside and outside containment are open only during sampling and the loss of sample flow will provide indication of the break to plant operators. A break in a sample line releases radioactivity and will actuate area and air radiation monitors. Since multiple indications are available for the operator actions, the applicant assumed that 30 minutes after initiation of a break, the operator would isolate the sample line and terminate further release of primary fluid discharged to atmosphere. The assumed operator action delay time of 30 minutes is consistent with the current operating plant design-basis analysis of a break of a small line outside containment and therefore, is acceptable.

The staff requested the applicant to provide the technical justification that the valves in the applicable CVS or sample lines are qualified to isolate a pipe break upon demand. In Westinghouse letter DCP/NRC-1040, dated September 18, 1997, the applicant provided a response to comment 41 which stated that the isolation valves of concern will be qualified to close on demand. For example, two isolation valves in the letdown line, two CVS purification line isolation valves and six containment isolation valves in the sample lines are designed to close in the event of piping breaks. Valve closure is ensured by specifying valve operators sized to close under the differential pressures expected during applicable design-basis events. These valves are tested in accordance with the requirements specified in SSAR Table 3.9-16, "Valve Inservice Test (IST) Requirements." Since the applicant specifies valve operators sized to close under the differential pressures expected during applicable design-basis events and will use the IST program to ensure the operability of the isolation valves, the staff concludes that the applicant has provided reasonable assurance that the isolation valves will close on demand.

The assumptions used for analysis of this event are conservative and acceptable and the scenario described in SSAR Section 15.6.2 ensures that the applicant has considered the most severe failure of piping carrying the primary coolant outside containment. In addition, the radiological releases are within the 10 CFR 50.34(a)(1)(ii)(D)(*1*) limits. Thus, the staff

concludes that the analysis is acceptable. The staff's evaluation of the radiological release calculations is discussed in Section 15.3 of this report.

15.2.6.3 Steam Generator Tube Rupture (SSAR Section 15.6.3)

The SGTR accident is defined by a penetration of the barrier between the RCS and the main steam system. This accident may be caused by the failure of a SG U-tube.

The applicant performed the SGTR analysis using the LOFTTR2 code for a case with complete severance of a single steam generator tube. At initiation of an SGTR, the reactor is assumed at nominal full-power. The initial secondary mass is assumed at nominal SG mass with an allowance for uncertainties. A LOOP is assumed following the reactor trip, and the CVS pumps are assumed to be loaded onto the diesel generators. Maximum CVS flows and energy addition from the pressurizer heaters are assumed following reactor trip to maximize primary to secondary leakage. The CVS is assumed to isolate on the "High-2" SG narrow range level setpoint. Since the failure of the steam dump system would result in a steam release from the SG PORVs to the atmosphere following the reactor trip, the steam dump system is assumed to be inoperable to maximize the radiological releases.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and identified that the most limiting single failure is a failed-open PORV on the affected SG. The applicant assumed that the single failure occurs coincidently with the low pressurizer pressure "S" signal, maximizing the integrated RCS-to-secondary break flow. The SG PORV is isolated when the associated block valve is automatically closed on a low steamline pressure protection system signal.

Consistent with the assumption of a LOOP, main feedwater pump coastdown occurs after the reactor trip and no startup feedwater is assumed in order to minimize SG secondary inventory and, thus, maximize secondary activity concentration and steam release.

Following the SGTR event, pressurizer low pressure and low-level alarms are actuated, and the CVS and pressurizer heaters are started to maintain pressurizer level and pressure. Alarms signaling pressurizer low pressure and low level, high condenser air removal discharge radiation, high steam generator blowdown sample radiation, and high steamline radiation would assist the plant operator to determine that an SGTR has occurred. However, no operator actions are assumed in the limiting case analysis, and the plant protection system is assumed to provide the protection for the plant. Continued loss of RCS inventory leads to a reactor trip signal generated by a low pressurizer pressure trip signal. The reactor trip automatically trips the turbine and terminates steam flow to the turbine. The secondary pressure rapidly increases after reactor trip and results in steam release to the atmosphere through the SG safety valves or PORVs or both.

After the reactor trip, a safeguard "S" signal is generated by low pressurizer pressure. The "S" signal results in CMT actuation and PRHR system actuation. Opening of the SG PORVs and operation of the PRHR and CMTs decreases the primary and secondary pressures. When the secondary pressure decreases to the low steamline pressure setpoint, the steamline isolation valves and SG PORV block valves are closed. Following closure of the block valves, the primary and secondary pressures and faulted SG secondary water volume increase as break

flow accumulates. This increase continues until the SG secondary level reached the "High-2" narrow range level and isolates the CVS pump. With continued RCS cooldown and depressurization provided by the PRHR system, primary pressure will fall to match the secondary pressure. At about 3 hours after the transient, the break flow terminates and the system reaches a stable condition. The analysis shows that the PRHR is capable of removing the core decay heat and preventing the unaffected PORV from opening. During the transient, the CMTs remain full and ADS actuation does not occur.

During an SGTR, the RCS depressurizes as a result of the primary-to-secondary leakage through the ruptured SG tube. The depressurization reduces the calculated DNBR. The analysis shows that the depressurization before reactor trip for the SGTR is slower than for the RCS depressurization events discussed in Section 15.2.6.1 of this report. Following a reactor trip, the DNBR rapidly increases. Thus, the staff's conclusion for the event discussed in Section 15.2.6.1 of this report also applies to the SGTR event in that the calculated DNBR remains above the safety limit.

For this analysis, the applicant uses the LOFTTR2 computer code together with conservative and acceptable assumptions. On that basis, the analysis shows that the maximum RCS will not exceed 110 percent of design pressure, and the minimum DNBR will remain greater than the safety DNBR limits. In addition, the analysis shows that long-term cooling can be achieved by the PRHR and CMTs, and the radiological releases will remain within the limits of 10 CFR 50.34(a)(1)(ii)(D)(*1*). As a result, the staff finds that the SGTR analysis meets the acceptance criteria of SRP Section 15.6.3 and is acceptable. The staff's evaluation of the radiological release is discussed in Section 15.3 of this report.

15.2.6.4 Spectrum of Boiling Water Reactor Steam System Piping Failure outside Containment (SSAR Section 15.6.4)

This section of the SSAR is not applicable to the AP600 design.

15.2.6.5 Loss of Coolant Accidents (SSAR Section 15.6.5)

In SSAR Section 15.6.5, Westinghouse presents the LOCA analysis results. The applicant's analyses examine small break LOCAs, large break LOCAs, and post-LOCA long term cooling. Small break LOCAs for the AP600 are defined by the applicant as minor pipe breaks that may occur during the lifetime of the plant and have an equivalent diameter of $\leq$ 25.4 cm (10 in). Large break LOCAs for the AP600 are defined by the applicant a major pipe break with a size greater than small breaks and would not be expected to occur during the lifetime of the plant.

The applicant also analyzes the long term performance the AP600 safety-related systems to provide cooling of the reactor core indefinitely due to a LOCA which ultimately progresses into containment sump recirculation. The staff evaluation of post-LOCA long term cooling of the AP600 is presented in Section 15.2.7 of this report.

The applicant performed the SBLOCA analyses using the NOTRUMP code as documented in WCAP-14206, "Applicability of the NOTRUMP Computer code to AP600 SSAR Small-Break LOCA Analyses," and WCAP-14807, "NOTRUMP Final Verification and Validation Report." NOTRUMP is assessed as a 10 CFR 50.46, Appendix K evaluation model. It is a one-dimensional, variable nodalization code based on a nonequilibrium model for two-phase

conditions. Significant code features include flow regime-dependent drift flux calculations with counter-current flooding limitations, mixture level tracking logic in multiple-stacking fluid nodes, and regime-dependent heat transfer correlations. The staff's evaluation and acceptance of the NOTRUMP code is discussed in Section 21.6.2 of this report.

The applicant performed the LBLOCA analyses using the WCOBRA/TRAC code as documented in WCAP-12954, "Code Qualification Document for Best Estimate LOCA Analysis." This is the Westinghouse's "best estimate" (BE) thermal-hydraulic computer code used to calculate fluid conditions in the reactor system during blowdown and reflood of a postulated LBLOCA. To support the acceptance of WCOBRA/TRAC for the AP600 application, the applicant submitted WCAP-14171, "WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident," for NRC review and approval. This code is comprised of the BE features needed to satisfy the requirements of 10 CFR 50.46(a)(1)(i) for a realistic code. The staff review of the WCOBRA/TRAC code has found that the analytical models used in the code realistically describe the behavior of the reactor systems during a LBLOCA. The applicant compared the code predictions with the applicable experimental data and identified uncertainties in the analysis. In the LBLOCA analysis for AP600 design, the applicant accounts for the effects of uncertainties on the calculated ECCS cooling performance as required by 10 CFR 50.46(a)(1)(i). The staff's detailed evaluation and acceptance of the WCOBRA/TRAC code is discussed in Section 21.6.3 of this report. In addition, WCOBRA/TRAC is used to analyze the post-LOCA long term cooling of the AP600 using 10 CFR Part 50, Appendix K, decay heat assumptions and evaluating discreet, discontinuous, semi-steady state intervals which the applicant refers to as "windows." The staff's detailed evaluation and acceptance of the WCOBRA/TRAC code for post-LOCA long term cooling is discussed in Section 21.6.4 of this report.

The applicant's LOCA analyses meet the following acceptance criteria for the calculated ECCS performance:

(1) The calculated peak cladding temperature (PCT) is less than 1204 °C (2200 °F).

(2) The calculated total oxidation of the cladding is within 0.17 times the total cladding thickness before oxidation.

(3) The calculated total amount of hydrogen generated is less than 0.01 times the hypothetical amount that can be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, are to react.

(4) Any calculated changes in core geometry will be such that the core remains amenable to cooling.

(5) After any calculated successful initial operation of the ECCS, the calculated core temperature will be maintained at an acceptably low value and decay heat will be removed for the extended time required by the long-lived radioactivity remaining in the core.

These criteria are established to provide significant margin for ECCS performance following a LOCA. The staff finds that these acceptance criteria are consistent with the requirements of 10 CFR 50.46 (b)(1) - b)(5) for ECCS performance and, therefore, are acceptable.

15.2.6.5.1 Small-Breaks

The applicant performed the SBLOCA analyses with the NOTRUMP code for eight cases:

(1) 25.4-cm (10-inch) cold-leg break

(2) double-ended CMT balance line break (17.8-cm [7-inch] in equivalent diameter)

(3) double-ended rupture of direct vessel injection line (10.2-cm [4-inch] in equivalent diameter)

(4) 5.08-cm (2-inch) cold-leg break in the PRHR loop

(5) 5.08-cm (2-inch) cold-leg break in the CMT loop

(6) 6.14-cm (2.4-inch) inadvertent opening of ADS flow paths

(7) 1.27-cm (0.5-inch) cold-leg break

(8) 5.08-cm (2-inch) hot-leg break

The applicant has considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8 . The applicant's analysis and confirmatory calculations provided in response to RAI 440.662 by Westinghouse letter DCP/NRC-0991, dated August 15, 1997, demonstrate that the most limiting single failure is the failure of one of four ADS-4 valves to open.

In the SBLOCA analysis, initial pressurizer pressure, RCS inlet and outlet temperatures, RCS flow rate, and SG pressure are assumed to be their nominal values consistent with steady-state full-power operation. Major assumptions made in the SBLOCA analyses are as follows:

- As required by Appendix K to 10 CFR Part 50, the initial core power is assumed to be 102 percent of the nominal core power, and the ANS-1971 decay heat plus 20 percent is used.

- Accumulators are initiated at a pressure of 4.83 MPa (700 psia).

- The PRHR is opened with the maximum delay of 21.2 seconds after initiation of an "S" signal to delay the cooling capability of the heat exchanger to the RCS.

- The "S" signal is actuated when the pressurizer pressure decreased below 11.72 MPa (1700 psia). The CMT isolation valves are opened with the maximum delay of 21.2 seconds after the "S" signal to minimize its contribution to RCS inventory in the initial stage of larger SBLOCAs. The main feedwater isolation valves are ramped closed

between 5 and 10 seconds after the "S" signal. The RCPs are tripped 16.2 seconds after the "S" signal.

- The ADS actuation signals are taken from the lower of the two CMT levels to be consistent with the CMT actuation delay feature.

- The SG isolates (by closure of the turbine stop valves) 1 second after the reactor trip signal to maximize the SG secondary energy. The SG safety valves actuate when the SG pressure reaches 7.58 MPa (1100 psia).

The applicant presented the results of the SBLOCA analyses in SSAR Tables 15.6.5-12 through 15.6.5-19 and Figures 15.6.5B-1 through 15.6.5B-104. Following an SBLOCA, the reactor is tripped on the low pressurizer pressure trip signal. After a reactor trip, an "S" signal is generated by a low pressurizer pressure actuation signal. The "S" signal results in RCP trip, CMT actuation, PRHR actuation, main feedwater isolation, and containment isolation. CMT actuation allows the cold water stored in the CMTs to flow into the RCS and the PRHR system actuation initiates heat removal from the RCS to the IRWST. When the lower of the two CMT liquid levels reaches 67.5 percent, the first-stage ADS valves are actuated, followed at specific time intervals by the second- and third-stage ADS valves. These stage ADS valves discharge RCS coolant into the IRWST. Soon after the level in either CMTs decreases to 20 percent, the fourth-stage ADS valves are activated. These valves discharge RCS coolant into the containment. Opening of the fourth-stage ADS valves continues to depressurize the RCS. When the RCS depressurizes to 4.83 MPa (700 psia), the accumulators begin to inject borated water to the reactor vessel. When the pressure difference between the RCS and containment decreases below the gravitational head of IRWST water, the IRWST begins to inject water through the direct vessel injection (DVI) lines to the reactor vessel.

The results show the 10-inch break case to be the limiting SBLOCA case with a calculated PCT of 453 °C (848 °F). Based on the 10 CFR Part 50, Appendix K evaluation model (EM) code used to perform the SBLOCA analyses, and analytical results which meet the acceptance criteria of 10 CFR 50.46 (PCT of less than 1204 °C (2200 °F), metal-water reaction of less than 17 percent of the total cladding thickness, cladding oxidation of less than 1 percent of the metal in the cladding cylinders surrounding the fuel, and maintenance of core coolability and long-term-cooling), the staff concludes that the SBLOCA analysis is acceptable.

15.2.6.5.2 Large-Breaks

The applicant used the WCOBRA/TRAC code to perform the LBLOCA analysis. SSAR Table 15.6.5-4 lists the initial plant physical configuration, power-related parameters, initial fluid conditions, and RCS boundary conditions used for the break spectrum calculation. These initial conditions are determined from the applicant's sensitivity study of the worst-case set of combinations that result in a highest limiting calculated PCT. To determine the limiting break case, the applicant analyzed eight LBLOCA cases, including split and guillotine breaks ranging in size from 0.147 $m^2$ (1.58 $ft^2$) to a DECLG break area (0.49 $m^2$ (5.28 $ft^2$)). The results of the analysis show that the DECLG break results in a maximum PCT and is the limiting case.

The staff requested that the applicant extend the LOCA spectrum analysis to smaller breaks of 0.05 $m^2$ (0.55 $ft^2$), the largest SBLOCA break analyzed, using acceptable methods. In

response, the applicant analyzed two cases with break areas of 0.10 $m^2$ (1.06 $ft^2$) and 0.07 $m^2$ (0.78 $ft^2$) using the WCOBRA/TRAC methods. Westinghouse letter DCP/NRC-1108, dated October 27, 1997, provided the applicant's response to RAI 440.660 and included an analysis which confirmed that both cases are not the limiting LBLOCA case. The staff also requested that the applicant show that, for breaks at various locations, the DECLG is the limiting break, as stated in the SSAR Section 15.6.5. Westinghouse letter DCP/NRC-1060, dated September 30, 1997, provided the applicant's response to comment 51 and stated that the sensitivity study for the existing Westinghouse four-loop plants showed that the breaks at the RCP-suction piping of the cold-leg and the breaks at the hot-leg are less limiting than the breaks at the discharge-piping of the cold-leg. Since the RCPs are integrated into the SG outlet nozzles, the AP600 design does not include RCP-suction piping of the cold-leg. To verify that the hot-leg break location is non-limiting, the applicant performed an analysis for the double-ended guillotine break at the hot-leg (DEHLG). The results of the analysis showed that the core flow does not reverse direction during the hot-leg break and the blowdown cooling of the core is effective to maintain the PCT to be less than the steady-state value and, thus, verified that the DEHLG break is bounded by the DECLG break.

The applicant considered plant systems and equipment that are available to mitigate the effects of the event, as discussed in SSAR Section 15.0.8, and identified that the limiting single failure is a failure of one CMT discharge valve to open. In modeling the CMTs and accumulators, the applicant minimized the capability to add borated water by assuming the failure of one CMT discharge valve to reflect the limiting single failure. The applicant's sensitivity study showed that the case with a LOOP results in a lower PCT compared to the case with the offsite power available. Thus, the offsite power is assumed to be available to calculate the PCT.

The applicant used the BE WCOBRA/TRAC code to analyze postulated large-break LOCAs. To account for the uncertainties of the BE analysis, the applicant used the methods described in WCAP-14171 to calculate the 95th percentile PCT. The PCT uncertainties for the BE LOCA methodology are affected by initial condition-related parameters, as well as model-related parameters. In LBLOCA analyses, the initial condition-related parameters (such as plant physical configuration, power-related parameters, and initial fluid conditions) listed in SSAR Table 15.6.5-10 are bounding and conservative values for the AP600, rather than being part of the PCT uncertainty evaluation. The calculated PCT uncertainties are derived from the effects of the model-related parameters (such as broken loop resistance, break discharge coefficient, and condensation rate). This approach will result in a higher PCTs and is therefore, conservative.

The applicant presents the results of the LBLOCA analyses in SSAR Tables 15.6.5-6 through 15.6.5-10 and Figures 15.6.5A-1 through 15.6.5A-73. Following an LBLOCA, the reactor trip actuates on the low pressurizer pressure trip signal. The insertion of the control rods is not credited in the LBLOCA analysis. Within a few seconds after the initiation of a LBLOCA, an "S" signal actuates on the containment "High-2" pressure. As a result, after appropriate delays, the PRHR and CMT isolation valves open and containment isolation occurs. The rapid depressurization of the RCS during an LBLOCA leads to the initiation of accumulator injection early in the transient. The accumulator flow reduces CMT delivery to the degree that the CMT level does not reach the ADS stage-1 valve actuation setpoint until after the accumulator tank empties following completion of the blowdown phase. The applicant's calculations continue until the fuel rods are quenched.

The results of the analysis shows that, for all analyzed cases, an LBLOCA yields results with less margin to the acceptance criteria limits than an SBLOCA, and the 95th percentile PCT including uncertainty for the limiting case DECLG break is less than 927 °C (1700 °F), the lower bound threshold for the oxidation reaction.

The applicant uses WCOBRA/TRAC models to perform the LBLOCA analyses with calculated PCT uncertainties that are derived from the effects of model-related parameters while the initial condition-related parameters used in analyses are bounding and conservative values for the AP600. The analytical results meet the acceptance criteria of 10 CFR 50.46 (PCT of less than 1204 °C (2200 °F), metal-water reaction of less than 17 percent of the total cladding thickness, cladding oxidation of less than 1 percent of the metal in the cladding cylinders surrounding the fuel, and maintenance of core coolability and long-term-cooling) and therefore, the staff concludes that the analysis is acceptable.

15.2.7 Post-LOCA Long-Term Cooling

AP600 SSAR Section 15.6.5.4C discusses the results of the safety analyses for the long term cooling (LTC) phase following a LOCA transient. The stabilization of IRWST injection flow is considered the beginning of the LTC phase. IRWST injection follows the automatic depressurization system blowdown (ADS stages 1-4). In part the blowdown is achieved by water and/or steam leakage through the break. IRWST injection provides the initial post-LOCA sustained LTC of the core as cooling water enters the RCS via the DVI lines from the IRWST and exits the RCS via the break and the ADS valves. When the IRWST drains to the "low-3" level, the sump isolation valves open initiating vessel sump injection. Water will be boiling in the vessel at this time and the sump water temperature will be rising to near the saturation temperature. Steam transports core heat to the containment shell and steam condensation returns the water to the IRWST or the sump. Heat rejection from the containment shell to the environment provides the ultimate heat sink. The cycle so established continues until the plant is recovered.

The purpose of the LTC analysis is to establish that the passive cooling mode (absence of active components or beneficial operator intervention) provides adequate core cooling until the plant is recovered. In this context, plant recovery means that the reactor is in a safe and stable configuration under operator control. In addition it must be established that sufficient water flow in and out of the vessel is present to prevent boron concentration (or precipitation) during the LTC phase. The accumulators, the CMTs and the IRWST all contain borated water. All of their contents are eventually spilled into the sump which is the final source of cooling water for the LTC phase. During the quasi-steady state LTC phase, cooling water enters the vessel and part of it exits as steam and part as liquid. The boron concentration in the vessel will increase to an equilibrium value depending on the steam/water ratio. If all of the cooling water is evaporated in the vessel, the boron concentration would continuously increase. The equilibrium concentration is inversely proportional to the fraction of liquid exiting the vessel. For the temperature of the water in the vessel, the equilibrium concentration could increase over the original sump concentration without resulting in boron precipitation.

Both LBLOCA and SBLOCA initiating events are considered. The computer code used to analyze the AP600 thermal-hydraulic behavior during LTC is WCOBRA/TRAC, which has been qualified by the applicant for the LTC phase in WCAP-14776, "WCOBRA/TRAC OSU

Long-Term Cooling Final Validation Report." The qualification is based on a series of experiments at a quarter-scale test facility at Oregon State University. The staff's evaluation of the application of WCOBRA/TRAC to AP600 LTC analysis is provided in Section 21.6.4 of this report. Initial and boundary conditions for the LTC analyses are derived either from WCOBRA/TRAC, which is used for the LBLOCA analysis, or NOTRUMP, which is used for the analysis of the SBLOCA initiating phase. Boundary conditions may be changing during LTC, but so slowly as to be considered constant. The thermal hydraulics of the LTC transient are not strictly steady-state because of the variation of the heat source strength as a function of time and the transition from IRWST injection to sump injection.

15.2.7.1 The Window Method

WCOBRA/TRAC is a complex code requiring large amounts of computation time to track a transient. The LTC phase (regardless of the break that initiates the transient) is a slowly evolving, extremely long transient not experienced in any existing type of reactor. For these reasons, the applicant has used a "window" method for analysis of the transients. The windows consists of the analysis of between 1000 to 5000 second time segments of the transient with the window start and stop times chosen to encompass the most important portions of the transient from a safety perspective.

The applicant claims that this method for the LTC analysis conforms to 10 CFR Part 50, Appendix K. However, the LTC transients do not involve all of the characteristics assumed in Appendix K. The only clearly applicable Appendix K feature is the use of ANS 71 + 20 percent for the assumed strength of the core decay heat source. The applicant also complies with the general requirement of 10 CFR Part 50, Appendix A, to consider single failure for the LTC transients. The noding used in modeling the vessel in WCOBRA/TRAC for LTC transient analysis is much coarser than that applied in a LBLOCA. This is a slower transient and coarser noding allows for a faster computation. The initial temperatures of the reactor metal components are those predicted by the WCOBRA/TRAC or NOTRUMP codes used to analyze the beginning of these LOCA initiated transients. However, any inaccuracies in the metal component temperature does not affect the convergence of the solution which depends mainly on the decay heat strength and cooling water flow. The containment pressure input is from a WGOTHIC code calculation which is performed in a conservative manner (i.e., the predicted pressure is lower than that expected during the transient). In addition to the heat source and the containment pressure conservatisms, the applicant applied maximum design flow resistance in the ADS stage 4 flow paths, the DVI lines, and the sump injection flowpaths in order to obtain bounding results and to demonstrate margin in the design.

15.2.7.2 Analyzed Transients

The applicant analyzed a total of 12 transients to demonstrate the long term cooling capability of the AP600 design. The analyzed transients include three initiated by a DECLG break, five initiated by SBLOCAs, and four initiated by double-ended direct vessel injection (DEDVI) LOCAs. The transient case designations used in the report correspond to the case designations used by the applicant in the AP600 SSAR Section 15.6.5.4C.2.1. The boundary conditions and analyses results are discussed in the following evaluation.

**Long Term Cooling Cases Initiated by DECLG Breaks**

The Case A transients below have been broken into three subcases (A1, A2, and A3) by the staff to clarify the discussion. Each subcase transient is initiated by a DECLG break in one of the cold legs on the non-PRHR loop. Case A1 is not a window analysis, instead, it is an extension of the DECLG LBLOCA calculation beyond the time of core quench (which is normally considered the end of a LOCA analysis) to 1500 seconds after break initiation. The calculation is carried out using the best estimate WCOBRA/TRAC code evaluation model and includes emptying of the accumulator and injection (draining) of CMT up to the point where IRWST is initiated on a low-low CMT level signal. Cases A2 and A3 are window analyses and both consider a window as starting at 20,000 seconds from the DECLG break and a window width of 1600 seconds. The difference between Cases A2 and A3 is the effect of containment condensate returned to the sump (Case A2) compared to condensate returned to the IRWST (Case A3). Case A2 provides a conservative treatment of long term cooling because of the lower injection head which results from the containment condensate water being returned to the sump rather than the IRWST. Case A3 provides a conservative treatment of the long term cooling injection with respect to water temperature since all the containment condensate in directed back into the IRWST. The condensate will be at a higher temperature than the sump water and, because of the IRWST head, will dominate injection flow into the downcomer cooling water injection temperature. The calculations for Cases A2 and A3 are performed using the LTC qualified version of the WCOBRA/TRAC.

Case A1: DECLG Break up to IRWST Injection - Core Makeup Tank Draining

IRWST injection into the reactor vessel begins with the opening of the squib valves in the IRWST to DVI lines and the simultaneous opening of the ADS stage-4 squib valves for final reactor system venting. The squib valve opening signal is actuated when the level in the CMT reaches the low-low level setpoint. The discharge flow rate from the CMTs just before actuation of IRWST injection is lower than the discharge rate from the IRWST due to the higher liquid level in the IRWST. In addition, core decay heat levels are still relatively high at this point. Therefore, the analysis of injection flow from the CMTs just prior to IRWST injection represents a potential limiting case relative to challenging the long term cooling capability of the AP600 design. The analysis performed by the applicant for this case is a continuation of the LBLOCA analysis up to 1500 seconds from the break initiation time (which corresponds to the latter part of the CMT draindown).

After the initiation of the DECLG LBLOCA the accumulators provide flow to the reactor vessel downcomer through the DVI lines. Depressurization is accomplished mainly through the break. The water flows down through the downcomer and up through the core. The downcomer refills with subcooled water during the LOCA reflood phase to a collapsed level of 6.4 m (21 ft) to 6.7 m (22 ft) up to the DVI injection point level. At the time the accumulators empty, the water level in the vessel is about 1.8 m (6 ft). Pressure spikes produced from boiling in the core temporarily reverse the flow, but the flow is predominantly upward. During the CMT draindown, water flows through the core and out the break and water level in the upper plenum is established. The single failure assumed in this transient is a failure to open of one of the CMT isolation valves but this should have negligible impact on the CMT draindown injection flow. The analysis shows that the core PCT does not exceed 127.8 °C (262 °F) after CMT draindown has begun. In addition, the water flow from the CMTs, through the DVI lines, through the core,

and out through the break will provide adequate flow to ensure boric acid concentration in the vessel remains low and precludes the possibility of boron precipitation. Responding to a staff request, Westinghouse letter DCP/NRC-1020, dated September 8, 1997, provided a calculation which showed that the limiting vessel boron concentration for this analysis will be 4600 ppm. Considering the solubility of boron at 100 °C (212 °F) is 50,000 ppm, the staff agrees that there is adequate flow through the core to prevent boron precipitation. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient.

Case A2: DECLG Break with IRWST Injection When Sump Level Is Within the Break Perimeter

Case A2 is an extension of the A1 case in which stable IRWST injection is in progress. The sump water level has flooded up to within the break perimeter (approximately centerline of cold leg) and the condensate gutter delivery system is assumed not to be functional so that all condensate returns to the sump. The window for this case starts at 20,000 seconds after initiation of the DECLG break and is analyzed for a transient duration of 1600 seconds. One ADS stage-4 valve is assumed to have failed. The initial vessel liquid inventory and temperatures for this window are from the results determined from Case A1 above.

The heat source used in this calculation is ANS 71 + 20 percent. In addition, the condensate drains into the sump which raises the sump liquid level to the height of the break. Water flows into the downcomer and up through the core. Part of the steam and water mixture flows up and out of the vessel side break. Boiling in the core produces steam, which carries liquid into the upper plenum and out the ADS stage 4 flow paths to flush the core. The core remains covered throughout the transient. The PCT remains relatively constant at 125.6 °C (258 °F). Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case A3: DECLG Break with Condensate Return to the IRWST.

This case is essentially the same as Case A2 with condensate returned to the IRWST rather than the containment sump (i.e., the gutter delivery system is functional). The difference between this case and Case A2 is a slightly higher liquid level in the IRWST and sump liquid level below the break so that the break connects to vapor only. However, the temperature of liquid being injected is much higher than in Case A2 due to the high temperature of the condensate returned to the IRWST relative to the sump water temperature. The collapsed liquid level in the vessel ranges from 2.9 m (9.5 ft) to 3.5 m (11.5 ft) with respect to the bottom of the heated part of the core. The PCT remains around 125 °C (257 °F) which is close to the coolant saturation temperature. The collapsed liquid level in the downcomer ranges between 6.1 m to 7 m (20 ft to 23 ft). Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

**Conclusions Regarding Long Term Cooling Cases Initiated by DECLG Breaks**

The post-LOCA LTC window analyses described above indicate that the most important time period is at the end of the CMT draining when the injection flow is at its lowest and the decay

heat is still at a high level. However, the core is adequately cooled in all cases and there is adequate liquid flow through the core to preclude high boron concentration and precipitation.

**Long Term Cooling Cases Initiated by SBLOCAs**

The following five transients are initiated by a small (2-inch diameter) cold leg split break. The first and second cases account for an ADS stage-4 single failure and consider the last portion of the IRWST injection and initial sump injection. The next two cases consider DVI valve failure at the end of the IRWST injection and initial sump injection respectively. The last case considers DVI failure combined with wall-to-wall flooding.

Case B: SBLOCA with ADS Stage-4 Single Failure: End of IRWST Injection Window

This transient is initiated by a 2-inch diameter split break in a non-PRHR loop at the bottom of a horizontal section of the cold leg piping. This window, which begins at 33,500 seconds after break initiation, investigates the switch from IRWST to sump injection. One ADS stage-4 is assumed to have failed. The initial conditions for the window are determined from the NOTRUMP calculated results for the same initiating event. The vessel collapsed level is at 2.7 m (9 ft) with respect to the bottom of the heated section of the core, with 0.1 m (0.2 ft) of collapsed liquid at the upper plenum. Metal component temperatures are defined by NOTRUMP, fuel rod temperatures are set at saturation temperature and the pressure is assumed at 172 kPa (25 psia) consistent with WGOTHIC analysis.

The IRWST provides sufficient head to inject water into the downcomer through the DVI lines. The water will flow down into the lower plenum and up through the boiling core into the upper plenum and out through the functioning ADS stage-4 valves and initially through the break. There is very little water flow through the break. At about 900 seconds into the transient, water is entrained in the hot legs, thereby increasing the pressure drop across the ADS stage-4 valves and increasing the upper plenum pressure. This results in a long reverse injection (that is from the upper plenum) of approximately 50 seconds. However, increasing void fraction and the boiling driving pressure reestablish DVI injection. During this brief flow reversal there is no PCT increase. The core collapsed level is about 3.4 m (11 ft) with respect to the bottom of the heated core at the beginning of the transient and drops to about 2.7 m (9 ft) at 1000 seconds into this window. Small boiling spikes are seen throughout the calculational window. The water flow through the core and out through the ADS stage-4 valves ensures adequate core cooling and core flushing to prevent boron concentration or boron precipitation. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case C: SBLOCA with ADS Stage 4 Single Failure; Sump Injection Window

This window is a continuation of Case B with the window start and duration designed to cover the beginning of sump injection. Initial conditions for the start of this window are created by using the conditions at the end of the previous window (Case B). Both IRWST and sump injection are in effect at the start of the window and take place for about 500 seconds. After that, the calculation is carried forth for another 2000 seconds before a quasi-steady state condition is established. The total window time width is 4000 seconds. The sump level is

simulated as having a constant liquid level of 33 m (108.2 ft) and the sump temperature is set at 115.6 °C (240 °F) which is the saturation temperature at the 172 KPa (25 psia) containment pressure computed by WGOTHIC. The sump provides sufficient head to inject water to the downcomer through the DVI line. The water from the downcomer flows up through the core and steam and water mixture flows out from the ADS stage-4 valves. Boiling in the core produces pressure and flow spikes but the flow is predominantly upward through the core. At about 3100 seconds into the window, there is a brief period of flow reversal, but sump injection is reestablished soon thereafter. Flow through the break is negligible, and there is neither a significant amount of coolant nor flow in the cold legs. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case D: SBLOCA with DVI Single Failure; Last Portion of IRWST Injection Window

This window is the same as Case B above except that the single failure is in a DVI line parallel flow path valve (instead of an ADS stage-4 valve) which reduces (although negligibly) the injection flow capability. The same period (i.e., end of IRWST injection) is examined in this window. The IRWST level is set constant at the low-3 level for the 2000 seconds duration of this window. The IRWST head and the available DVI capability are sufficient to inject adequate water into the downcomer. Steam produced in the core entrains liquid and flows out through the ADS stage-4 vents. Boiling in the core produces pressure and flow spikes which momentarily may reverse the flow. Nevertheless, core flow is predominantly upward. The collapsed core level is between 2.75 m (9 ft) and 3.35 m (11 ft) of water. Liquid is present throughout the core which remains adequately cooled. The PCT remains slightly above the saturation temperature. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case E. SBLOCA with DVI Single Failure; Sump Injection Window

This window is a continuation of Case D with the window start and duration designed to cover the beginning of sump injection. It is also noted that this window is the same as Case C above except that the single failure is in a DVI line parallel flow path valve (instead of an ADS stage-4 valve) which reduces (although negligibly) the injection flow capability. Initial conditions for the start of this window are created by using the conditions at the end of the previous window (Case D). Both IRWST and sump injection are in effect at the start of the window and take place for about 500 seconds. After that, the calculation is carried forth for another 2800 seconds before a quasi-steady state condition is established. The total window time width is 4000 seconds. The sump level is simulated as having a constant liquid level of 33 m (108.2 ft) and the sump temperature is set at 115.6 °C (240 °F) which is the saturation temperature at the 172 kPa (25 psia) containment pressure computed by WGOTHIC. The sump provides sufficient head to inject water into the downcomer to maintain the level at about 6.1 m (20 ft), which is about 1.5 m (5 ft) below the low point of the cold leg nozzle. The downcomer water flows up through the core where the steam produced by boiling entrains water which flows out through the ADS stage-4 vents. The core collapsed water level is maintained above 2.45 m (8 ft) except for brief periods (at 2900 seconds and again at 3900 seconds) when the collapsed level drops to about 1.85 m (6 ft). At the end of the window calculation, the core level is above 2.45 m (8 ft). The PCT is maintained slightly above the liquid saturation temperature. Flow through the break is negligible, and there is neither a significant amount of coolant nor flow in

the cold legs. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case F: SBLOCA with DVI Failure and Wall-to-Wall Flooding; Sump Injection Window

This window models a condition in which all containment compartment volumes below the sump liquid level are flooded. The resulting sump level is 31.65 m (103.77 ft) which represent the lowest possible driving head during LTC sump recirculation cooling. The condition is assumed to be initiated by a DEDVI line break which will flood one normally unflooded compartment and that leakage between all other unflooded spaces is at 37.85 L/m (10 gpm) which the applicant states is conservative based on leakage through compartment drainage check valves, penetrations, and other miscellaneous leak paths. The applicant's calculations show that the time to total floodup of all compartments would be 28.5 days after event initiation.

The initial conditions for this window are assumed to be equivalent to the conditions at the end of the Case E window above. The containment pressure is calculated at 193 kPa (28 psia). In addition, one ADS stage-4 failure is assumed. The IRWST is also assumed to be empty. The sump level is maintained at 31.65 m (103.7 ft) throughout the transient which is run for a duration of 5000 seconds. The core level ranges between 3 m (10 ft) and 3.4 m (11 ft) and the downcomer level ranges between 7 m (23 ft) and 7.3 m (24 ft). The PCT is around 123 °C (254 °F) which is slightly above the saturation temperature. The hot legs are almost filled with liquid, which occasionally increases the pressure and reverses the flow, but, on average remains upward through the core. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

**Conclusions Regarding Long Term Cooling Cases Initiated by SBLOCAs**

The first four SBLOCA initiated cases presented above covered the most critical periods of the LTC transient, including the end of IRWST injection and the switch over to sump injection. At the end of the IRWST injection, there is a combination of low flow and high decay heat. At the beginning of sump injection, there is also the potential for low injection head, sump water temperature at or close to saturation, and relatively high decay heat. The above cases represent the most conservative time windows in the LTC part of the transient. In addition, the applicant considered a fifth SBLOCA initiated case where the containment lower level compartments, which are normally dry, experience wall-to-wall flooding. This case indicates that the minimum possible head is adequate to provide core cooling flow for the long term. Therefore, the staff concludes that the LTC phase following small break LOCAs are adequately analyzed and the reactor will remain cooled. In addition, the staff also concludes that there is sufficient liquid flow present through the core to prevent boron precipitation.

**Long Term Cooling Cases Initiated by DVI Line Breaks**

The final four LTC window cases analyzed by the applicant assume a DEDVI line break with an ADS stage-4 valve single failure. Cases G and H examine the last portion of the IRWST injection and initial sump injection LTC phases following a DEDVI line break. Cases I and J (the last two cases) consider a variation in the DEDVI transients in which the RNS system operates

initially (injecting water from the IRWST) which accelerates the depletion of the IRWST inventory by pumping spill flow through the DEDVI line break. This causes the IRWST to reach its low level sump recirculation actuation setpoint much more quickly with much higher core decay heat levels.

Case G: DEDVI Break LOCA with ADS Stage 4 Single Failure: IRWST Injection Window

A DEDVI line rupture is assumed as the initiating LOCA for this LTC window analysis. The starting time for the window is 17,150 seconds after the break. The IRWST is assumed to have been drained to the "low-3" level (which would represent the minimum IRWST injection head before sump recirculation is initiated). One ADS stage-4 valve is assumed to have failed, creating reduced venting capability. The initial conditions for this window transient are determined from the NOTRUMP calculated results for the same initiating event.

The vessel collapsed liquid level is 2.7 m (9 ft) and the upper plenum collapsed level is 0.1 m (0.3 ft). The injection liquid temperature is set at 59.4 °C (139 °F) and is maintained during the transient. (The accuracy of the estimated injection liquid temperature has a negligible effect on the peak cladding temperature.) The DEDVI break drains into the valve room which, during this time window, is filled with water. Injection through this break is modeled. Metal component temperature is estimated from NOTRUMP. The initial fuel rod temperature is specified as the saturation temperature. Containment pressure is set at 165.5 kPa (24 psia) as calculated by WGOTHIC.

The IRWST liquid level is maintained constant at the "low-3" level for the 1000 seconds duration of this window. This IRWST liquid level still provides sufficient head to inject water into the downcomer. Water also flows into the downcomer from the passive core cooling system valve room through the broken DVI line. At about 250 seconds into the window a quasi-steady-state condition is established. Water from the downcomer flows up through the core. Boiling establishes a two-phase flow out of the ADS stage-4 vents. However, as water deposition increases in the hot legs, venting is reduced and associated pressure increases result in temporary flow reduction or even flow reversal. Nevertheless, the flow is predominantly upward through the core. The downcomer liquid level stabilizes at about 7 m (23 ft) and the core collapsed level is at about 3.4 m (11 ft). The PCT remains slightly above the saturation temperature. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case H: DEDVI Break LOCA with ADS Stage-4 Failure; Sump Injection Window.

This window is a continuation of Case G with the window start and duration designed to cover the time frame from the end of IRWST injection to the beginning of sump injection. Initial conditions for the start of this window are created by using the conditions at the end of the previous window (Case G).

The calculational duration for this window is 3000 seconds out of which the first 1000 seconds are required to establish quasi-steady-state conditions. The sump level is established and maintained at 32.7 m (107.2 ft) and the sump water temperature is set at 89.4 °C (193 °F), as computed by WGOTHIC. The valve room water temperature is 60 °C (140 °F) due to subcooling caused by the IRWST liquid that was spilled into the room through the DEDVI line

break. The sump provides sufficient head to inject into the downcomer through the DVI nozzles. Additional water flows to the downcomer from the passive core cooling system valve room through the broken DVI line. The downcomer liquid level varies between 5.8 m (19 ft) and 7 m (23 ft). The core collapsed liquid level varies between 2.4 m (8 ft) and 3.5 m (11.5 ft). The PCT ranges between 123.3 °C (254 °F)and 125.6 °C (258 °F). Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case I: DEDVI Break LOCA with ADS Stage 4 Single Failure: IRWST Injection Window - Normal Residual Heat Removal System Operating.

This window examines the same basic time period as Case G above with the difference being the assumption that the IRWST has been drained to the "low-3" level by operation of the RNS pumps which accelerate the IRWST spill out the DEDVI line break. Specifically, both RNS pumps are assumed to be operational, having been started by the operator 2000 seconds after initiation of a DEDVI line break. The RHR pumps take suction from the IRWST and spill into the DVI valve room. This empties the IRWST to the "low-3" level at 7570 seconds. At this time, the RNS pumps are assumed to fail. Operation of the pumps drains the IRWST much more quickly to the minimum level, thus, maximizing the core decay heat rate during this window. (It should be noted that in Case G, the equivalent time to reach the IRWST "low-3" level was calculated to be 17,150 seconds.)

The window calculation is carried out to 3000 seconds and a quasi-steady-state is established at about 1000 seconds into the calculation. The IRWST injection into the downcomer maintains the water level at about 5.8 m (19 ft). The water from the downcomer flows up through the core. A collapsed liquid level of 2.3 m (7.5 ft) to 2.7 m (9 ft) is maintained in the core. Core boiling produces pressure and flow spikes but the flow through the core is, on the average, upward. The PCT is maintained slightly above saturation. Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

Case J: DEDVI Break LOCA with ADS Stage 4 Single Failure; Sump Injection Window - Normal Residual Heat Removal System Operating.

This window is continuation of Case I with the window start and duration designed to cover the beginning of sump injection. Initial conditions for the start of this window are created by using the conditions at the end of the previous window (Case I). As in Case I, this transient has been worsened by early entry into the sump injection phase which results in a higher decay heat level than the comparable Case H. The early sump injection is due, again, to the RNS pumpdown of the IRWST.

This window calculation has a duration of 2800 seconds. The first 1000 seconds are used to establish a quasi-steady-state condition. The sump level is set at 32.7 m (107.2 ft) and the sump temperature is set at 77.8 °C (172 °F) as calculated by WGOTHIC. The water temperature is 59.4 °C (139 °F) in the valve room and 77.8 °C (172 °F) in the sump. The sump head provides injection flow through the intact DVI nozzles. In addition, water from the passive core cooling system is introduced into the downcomer through the broken DVI line. Water from the downcomer flows up through the core and steam produced in the core creates

two-phase flow through the ADS stage-4 vents. Because water accumulates in the hot legs, there is a temporary pressure increase in the upper plenum, which results in a temporary flow reversal as observed at about 1800 seconds. Nonetheless, the average flow is upward through the core. The downcomer collapsed liquid level varies from 5.1 m (16.7 ft) to 5.3 m (17.5 ft). The core collapsed liquid level is in the range of 2.3 m (7.5 ft) to 2.4 m (8 ft). Therefore, based on the results of the applicant's analysis, the staff concludes that the core remains adequately cooled during this transient and there is adequate liquid flow through the core to prevent boron precipitation.

**Conclusions Regarding Long Term Cooling Cases Initiated by DVI Line Breaks**

The four LTC window cases presented above cover the most critical segments of the LTC transient following a DEDVI line break. The results of the analysis indicate that the core will remain cooled with adequate liquid flow to prevent boron precipitation.

15.2.7.3 Summary

The staff has reviewed Section 15.6.5.4C of the AP600 SSAR, "Post-LOCA Long-Term Cooling," with respect to both core coolability and potential for boron precipitation. The physical phenomena which appear during AP600 LTC transients are not normally encountered in the 10 CFR 50.46 LOCA analyses for the current generation of operating PWRs, and are relatively benign compared to typical 10 CFR 50.46 phenomena. The only significant characteristic retained in this analysis from 10 CFR 50.46 and Appendix K is the decay heat source strength. The review indicated that the applicant chose conservative conditions for the analysis. The results demonstrate that, in all instances, there is sufficient liquid and steam coolant flow to ensure core cooling and provide core flushing to avoid boron concentration concerns. Therefore, the staff finds the AP600 SSAR post-LOCA long term cooling evaluations acceptable.

15.2.8 Deboration during SBLOCAs

15.2.8.1 Background

Recent analysis and experimental evidence have shown that an inherent mechanism for boron dilution could exist for certain SBLOCA events in PWRs. The concern develops during reflux cooling heat removal through the steam generators in the RCP loop piping. The deborated water in the RCP loops could be transported to the core through the natural circulation processes or startup of the RCPs. This injection of deborated coolant into the core could result in a significant reactivity addition and could possibly cause fuel damage. The staff asked the applicant, to address the applicability of this boron dilution event to the AP600 reactor design and to resolve the issue.

In response to this request, the applicant submitted a boron dilution transient analyses for the AP600 reactor system design. The objectives of the analyses were to identify the potential for stagnation of diluted coolant scenarios within the AP600 system, and to conservatively estimate the size of the coolant slug that could be injected into the core without resulting in fuel damage. In addition, the applicant will use the results of these analyses to develop recovery strategies in case dilution of the coolant is suspected in one or more of the loops.

The analysis conducted by the applicant included a full AP600 primary side model, as well as a passive safety system. The scenarios are modeled by a coupled three-dimensional thermal-hydraulic, neutronic simulation of the core, including a high-order "solute tracker" to better track the transport of the unborated slug throughout the RCS loops.

The applicant analyzed the following scenarios pertaining to the AP600 design that could cause the accumulation of unborated water in the RCS loops:

(1) the "Finnish Center" scenario, which postulates a small break of 1 to 3 inches in the cold leg and the accumulation of highly diluted coolant in the loop seals

(2) the introduction of an unborated slug as a result of a reverse break flow following a SGTR

(3) additional deboration analyses related to operational transients

Information in support of these analyses were provided by the applicant in Westinghouse letters NSD-NRC-96-4773, dated July 18, 1996; NSD-NRC-97-5126, dated May 14, 1997; NSD-NRC-97-5353, dated October 1, 1997; and NSD-NRC-98-5525, dated January 16, 1998. In addition, the following references were reviewed: Pennsylvania State University Study titled "High Order Numerical Modeling of Solute Transport in System Codes," R. Maccan and J. Mahaffy, September 1995; and Pennsylvania State University Study titled "Analysis of Boron Dilution Transients in the AP600," R. Maccan, K. Ivanov, and G. Robinson, June 1996.

15.2.8.2 Natural Circulation Flow and the "Finnish Center" Scenario

The Finnish Center scenario is not significant to the AP600 reactor design because the SGs are not relied on to cool the RCS during a LOCA event. Consequently, the SGs should not generate any significant amount of boron-free condensate via reflux condensation over an extended period of time during a LOCA event. In the AP600 design, the steam generator functions as a "heat source" as the RCS depressurizes, rather than a "heat sink" as it does in a conventional PWR designs. Therefore, the differential temperature across the primary and secondary side of the generators is such that steam from the reactor will not condense on the tubes. However, in the AP600 design, the PRHR heat exchanger rapidly becomes the dominant RCS heat sink following the generation of an "S" signal during postulated SBLOCA events. Consequently, the PRHR heat exchanger may become a potential source for generating a volume of unborated coolant during an SBLOCA.

Condensate generated in the PRHR is delivered to the Loop 1 SG outlet plenum during an SBLOCA event. For conservatism, the condensate from the PRHR is assumed to contain zero boron. In addition, no mixing with the other liquid is credited in the cold legs. However, since the AP600 has no loop seals, only a small amount of condensate (approximately 0.6 $m^3$ (21 $ft^3$)) can accumulate in the RCP casing before the excess will drain from the SG outlets into the Loop 1 cold legs, and eventually down the downcomer. Thus, an unborated slug cannot stagnate in the RCS loop cold legs of a AP600 design. The continuous stream of condensate (approximately 41 kg/sec [90 lbm/sec]), from the PRHR/SG outlets, must pass through highly borated water in the downcomer (3400 ppm from the passive safety injection CMTs and/or accumulators), before reaching the lower plenum. This continuous stream of condensate

enters the downcomer with horizontal momentum, where it impinges on the core barrel, at which time it begins to move down the downcomer. Results from the applicant's analysis show that the velocity of the condensate stream diminishes as the plume proceeds down the downcomer, and it decreases to an insignificant amount as it enters the lower plenum.

During an AP600 LOCA event, an "S" signal actuates passive safety injection from the CMTs and/or accumulators, injecting 108,862 kg (240,000 lbm) of water at a boron concentration of 3400 ppm (the minimum TS value), into the already heavily borated (1800 ppm, HFP) downcomer. Analysis conducted by the applicant shows that the relatively low flow rate of condensate down the downcomer and into the core, following the post-RCP trip "natural circulation" phase of a SBLOCA event, enables mixing to occur in the downcomer and in the lower plenum. In addition, since there are no loop seals in the AP600 design, no unborated "slugs" of condensate can form in the PRHR loops and thus no unmixed slugs can enter the downcomer, or the core, during design-basis LOCA scenarios. The staff concurs with this analysis.

15.2.8.3 Transients or Accidents Addressed by the Analysis

The RCS flow associated with the operation of the PRHR and the CMT systems is caused by the thermal driving head established by convective heat transfer (natural circulation). The applicant performed an analysis to investigate the flow behavior throughout the RCS while the PRHR and the CMT systems are removing core decay heat, and to quantify the resulting boron distribution that could form as convective flow rates approach stagnation. The case study used is the "loss of normal feedwater" (LONF) transient. This transient is chosen because under the conditions corresponding to beginning of life, equilibrium cycle, and no xenon, this transient would represent the most limiting plant conditions with respect to core recriticality prediction.

The analysis focused on identifying regions of the primary system that could contain stagnant pockets of critical boron concentration, and that, under certain conditions could somehow be filled with unborated water. The analysis used the TRAC-PF1/MOD2 code to perform the design-basis LONF transient that is presented in SSAR Chapter 15. The applicant benchmarked the TRAC-PF1/MOD2 thermal-hydraulic component with SSAR data generated by the AP600 LOFTRAN code and showed good agreement. The neutronic component of TRAC-PF1/MOD2 is compared with Westinghouse 3-D reference core data. The neutronic component of TRAC-PF1/MOD2 uses the Nodal Enhanced Model (NEM). Comparison of the TRAC-PF1/MOD2 results to the referenced core data, specifically, the calculated power distributions and rod worth values, also showed good agreement.

The results of the LONF transient analysis indicated that all of the regions of the RCS became sufficiently borated following an RCP trip and the actuation of the CMT. The results also showed that boron concentrations through the RCS are greater than the critical boron concentration required for cold (93.3 °C [200 °F]) temperatures with N-1 rods inserted (the most reactive RCCA is assumed to be stuck out of the core), and no xenon conditions. From the results of the study, the applicant concluded that subsequent RCS loop recovery, following CMT actuation and RCS cooldown to equilibrium temperatures, will not pose a recriticality potential. The staff has reviewed the analysis and, for the reasons stated above, agree with the results.

### 15.2.8.4 Maximum Slug Size Accumulated and Pump Restart Analysis Following an SGTR Event

The applicant conducted analyses to quantify the volume of deborated water that could be allowed to collect in the RCP casings and the SG channel heads, without resulting in a decrease of localized core inlet boron concentrations to below the critical boron concentration following the restart of the RCPs. The study also included the effects of nominal and reduced decay heat situations. The study focused on two possible scenarios:

(1) the direct mixing case, where the two RCP pumps in the loop where the unborated slug is located (Loop 2) are restarted

(2) the reverse mixing case, where the two RCP pumps in the loop without the unborated slug (Loop 1) are restarted.

The study employed the TRAC-PF1/MOD2 code for tracking the unborated slug through the RCS and the core. The tracking method is benchmarked against experimental mixing data from a 1/5 scale model of a three-loop Westinghouse PWR. Analysis of the results show that the solute tracking model conservatively under-predicted the mixing that would occur. The model did not take credit for mixing due to impingement of the water jet onto the downcomer walls of the reactor vessel, or the high turbulence flow caused by the RCP impellers. Thus, larger volumes of unborated coolant could be shown to be acceptable if the mixing that would occur from these ignored effects were explicitly modeled.

Results of Case 1 (direct mixing), in which the RCPs are started in sequence in the loop containing the unborated water, namely Loop 2, yielded unborated volumes greater than 3.3 $m^3$ (115 $ft^3$) where the nominal decay heat had been assumed, and an unborated volume greater than 1.9 $m^3$ (66 $ft^3$) for the situation where the decay heat had been assumed to be 1 percent of the ANS 1979 curve. That is, these volumes could be accumulated in the loops and then pushed into the core with the core remaining subcritical at a specified cold leg temperature. However, one RCP casing can hold only approximately 0.6 $m^3$ (21 $ft^3$) before the accumulated unborated coolant begins to spill into the cold leg piping connection, mixing with existing borated coolant in the RCS before reaching the reactor vessel. Thus, the maximum volume of unborated water that could collect in a steam generator channel head region cannot be greater than 1.2 $m^3$ (42 $ft^3$) (i.e., two RCPs per steam generator outlet channel head). Analysis of the results indicate that approximately one and one-half times this credible value can be accommodated (i.e., this volume can theoretically accumulate and not result in the core inlet boron concentration dropping below the critical concentration following RCP restart in the adjacent loops), under low decay heat conditions, and more than two and one-half times as much under nominal decay heat conditions.

The analysis conducted for Case 2 is similar to that conducted for Case 1. The restart sequence is similar to that used for the direct mixing case, with the pumps in Loop 2 remaining idle. The results demonstrated that the mixing caused by the reverse flow through the faulted SG, and associated RCS loop can accommodate large volumes of unborated water in the faulted SG U-tubes and channel head, so that the localized core inlet boron concentrations remains above the critical boron concentration for both the standard decay heat and the low decay heat situations.

This transient is much less severe than the direct mixing case. That is because of the flow patterns that develop in the primary system legs after the restart of the pumps in Loop 1. The flow in Loop 2 is reversed and enters the vessel through the Loop 2 hot leg. Then it mixes with a much larger flow coming from the core, and leaves the vessel through the Loop 1 hot leg nozzle. The flow from the core is highly borated when compared to the coolant injected from Loop 2, by approximately 10 to 1, and the dilution of the coolant leaving the vessel toward Loop 1 is therefore relatively small. This highly borated water enters the vessel again through the Loop 1 cold legs, and after flowing down the downcomer, the coolant enters the core. Consequently, the reverse mixing provides a mechanism for restarting the pumps under conditions when it is suspected that a highly diluted slug may exist in one of the loops. The reverse flow is implemented through the RCP restart guidelines. As a result, the restart of the pumps in the loop, which does not contain the deborated coolant, will avoid a rapid injection of well-defined deborated slugs into the core. This provides a much larger margin for safety, in case highly diluted pockets of coolant are suspected somewhere else in the primary system. The staff concurs with the results of this analysis.

15.2.8.5 Protective Measures

The applicant changed its Emergency Response Guidelines (ERGs), specifically AES-1.1 and 1.2, to add cautionary notes to instruct the operators to confirm the establishment of natural circulation before restarting RCPs. Also, in case natural circulation through the SG has not been established, procedural changes were implemented to include precautions to throttle the PRHR heat exchanger valves to avoid excessive cooldown following RCP restart.

For the AP600 design, the RCPs are integral with the SG channel head, and there is no low point that would allow for the collection of a large unborated slug of deborated (pure) water. However, establishing natural circulation with both SGs prior to RCP restart provides added assurance that the RCS is well-mixed, and minimizes any potential for an inadvertent criticality following RCP restart.

In ERG AE-3, the applicant specifically addressed the RCP restart in conjunction with the SGTR accident. Even though analyses showed that recriticality does not occur following the restart of an adjacent RCP, the applicant included a caution in the ERG AE-3, regarding the potential for inadvertent criticality following any natural circulation or PRHR cooldown, if the first RCP started is in the ruptured loop. As stated above, this potential is reduced when the first RCPs restarted are those in the intact loop.

15.2.8.6 Analyses of Additional Deboration Scenarios

The applicant also addressed the possibility of the loss of AC power during a dilution to criticality (the so-called "French Scenario"). In the French Scenario, it is assumed that if a loss of power occurs, the standby diesel generators startup and allow the charging/makeup pumps to continue the dilution without the RCPs in operation, thus providing the means to accumulate unborated water in the RCS loops.

The AP600 CVS is designed to address a potential rapid boron dilution scenario in the event of a loss of power to the two CVS remotely-operated demineralized water system isolation valves. When power is interrupted, the CVS makeup pumps stop and two safety-related motor-operated gate valves, in series, from the demineralized water system automatically close

to isolate the unborated water source. In addition, the three-way CVS makeup pump suction valve is automatically aligned to the boric acid tank. The CVS makeup pumps are sequenced onto the diesel generator, but will not restart unless actuated by low pressurizer level signal or the makeup control system. In the event that the pumps are actuated, the system is aligned to take suction from the borated water source, and the unborated water source is isolated. Restoration of power to the isolation valves does not cause the valves to reopen. Consequently, loss of power does not result in a dilution event.

The applicant also addressed concerns about RCP restart following maintenance activities (such as SG flushing), that have the potential to form low-concentration, or deborated water pockets in the RCS. The applicant recommends that these concerns should be procedurally addressed, as for any PWR design. The staff agrees with this conclusion.

The applicant stated in the submittal that interlocks will be integrated in the logic systems to prevent inadvertent activation of the RCP power supply. These interlocks, together with the AP600 ERGs/EOPs, will preclude the inadvertent restart of the RCPs following the actuation of the passive core cooling systems.

15.2.8.7 Conclusions

The staff reviewed the applicant's submittals in support of AP600 boron dilution transients analyses concerns following a SBLOCA (as well as other possible deboration transients), and the restart of RCPs following a deboration event.

With regard to RCP restart, the applicant demonstrated that the accumulation of unborated water upstream of the idle RCP casings will not result in recriticality following RCP restart. The analyses also showed that substantial safety margin to recriticality existed for the scenarios considered. Specifically, those scenarios included direct mixing in which the two pumps adjacent to the loop where the unborated slug is located (Loop 2) are restarted, and reverse mixing where the two pumps of the loop without the unborated slug (Loop 1) are restarted. In particular, as the discussion provided above indicates, reverse mixing is more conservative because it demonstrates a larger margin to recriticality. This is expected because very complete mixing will occur in the RCS loops under the reverse flow configuration, and this phenomenon will be used procedurally in those instances where it will be apparent to the operator that a deborated water volume may exist. Therefore, the applicant has shown that for the AP600 design, RCP restart following a boron dilution event will not create recriticality accidents. Furthermore, the applicant has taken additional steps to minimize the possibility of boron dilution potential events, thereby maintaining a defense-in-depth approach to this issue. The staff concurs with the results.

With regard to natural circulation, the applicant has demonstrated that following a loss of heat sink event, and following CMT actuation and the RCS cooldown to equilibrium temperatures, the RCS loop recovery will not pose a recriticality potential.

15.2.9 Anticipated Transients Without Scram (SSAR Section 15.8)

An ATWS event is defined as an anticipated operational occurrence (such as loss of normal feedwater, loss of condenser vacuum, or LOOP) combined with an assumed failure of the

reactor trip system (RTS) to shut down the reactor. On June 26, 1984, the staff amended the *Code of Federal Regulations* to include 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants" (known as the "ATWS rule"). This rule, as amended on July 6, 1984, November 6, 1986, April 3, 1989, and July 29, 1996, requires nuclear power plant facilities to reduce the likelihood of failure to shut down the reactor following anticipated transients, and to mitigate the consequences of ATWS events.

In general, the equipment to be installed in accordance with the ATWS rule is required to be diverse from the existing RTS, and must be capable of being tested at power. This equipment is intended to provide needed diversity to reduce the potential for common-mode failures that result in an ATWS and lead to unacceptable plant conditions.

For the PWRs manufactured by Westinghouse, the basic requirements of the ATWS rule are specified in paragraph (c)(1) of 10 CFR 50.62, which includes the following statement:

> Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

The AP600 design includes a control-grade diverse actuation system (DAS) to provide an alternate turbine trip signal, and an alternate actuation signal of the PRHR system for decay heat removal, which are separate and diverse from the safety-grade reactor trip system and PRHR normal actuation signals. The DAS also provides a diverse scram function. The staff's review of the applicant's DAS design is discussed in Section 7.7 of this report. The AP600 design relies on the PRHR in lieu of an auxiliary or emergency feedwater system as its safety-related method of removing decay heat. The applicant has submitted a request for exemption from the part of the ATWS regulation, 10 CFR 50.62(c)(1), that requires auxiliary or emergency feedwater as an alternate system for decay heat removal during an ATWS event. The staff concludes that the applicant has met the intent of the ATWS rule by relying on the PRHR system to remove the decay heat, and meets the underlying purpose of the rule. Therefore, the Commission has determined that the special circumstances described in 10 CFR 50.12(a)(2)(ii) exist in that the requirement for an auxiliary or emergency feedwater system is not necessary to achieve the underlying purpose of 10 CFR 50.62(c)(1), because Westinghouse has adopted acceptable alternatives that accomplish the intent of this regulation, and the exemption is authorized by law, will not present an undue risk to public health and safety, and is consistent with the common defense and security.

In the course of the review, the staff asked the applicant to submit an analysis demonstrating that the AP600 ATWS response is within the bounds considered by the staff during its deliberations leading to the ATWS rule. In Westinghouse letter NTD-NRC-94-4075, dated March 4, 1994, the applicant provided a response to RAI 440.26 which provided the results of an ATWS analysis for the staff to review. In its analysis, the applicant had used a complete loss of normal feedwater (LONF) event for the ATWS

analysis because the LONF event was previously established as the limiting case (i.e., produced the maximum RCS pressure) for conventional Westinghouse PWRs. The AP600 passive design is different from conventional PWRs in that the AP600 relies mainly on the PRHR system instead of the auxiliary feedwater system use by the existing PWRs to remove the decay heat during an ATWS event. Because the AP600 also has other significant design differences from conventional PWRs, the staff requested the applicant to show that the methodology used for the existing ATWS analyses are applicable to AP600. The staff also wanted additional justification that the LONF analysis was the worst ATWS case.

Based on further discussions with the applicant, it was agreed that the following acceptance criterion would be used for the AP600 ATWS analysis:

> The ATWS must show that the unfavorable exposure time (UET), given the cycle design (including the moderator temperature coefficient [MTC]), will be less than 5 percent, or equivalently, that the ATWS pressure limit will be met for at least 95 percent of the cycle. The UET is the time during the cycle when reactivity feedback is not sufficient to maintain pressure under 22.06 MPa (3200 psi) for a given reactor state.

The staff had previously approved this acceptance criterion in a letter from the NRC to the Commonwealth Edison Company, dated July 27, 1995. In Westinghouse letter DCP/NRC 1240, dated January 30, 1998, the applicant's responses to RAIs 440.659 and 440.740F identified the most risk-significant ATWS scenarios, and performed plant analyses of these scenarios to demonstrate that the LONF scenario is bounding and meets the reactor coolant pressure boundary pressure limit of 22.06 MPa (3200 psi). To identify the most risk-significant ATWS scenarios, the applicant performed a probabilistic risk assessment (PRA) evaluation to identify the frequency of the anticipated transients in SSAR Chapter 15 for AP600. In the PRA evaluation, the applicant assumed that the failure of rod insertion is attributable to one of three common mode failures:

(1) failure of the reactor trip portion of the plant monitoring system (PMS)
(2) failure of the reactor trip breakers (RTB) to open
(3) mechanical failure which prevents rod insertion

The probabilities for these failure modes were developed and combined with the anticipated transients frequencies to define the most risk-significant ATWS scenarios. The applicant then performed ATWS analyses on the most risk-significant ATWS cases to identify which scenario results in the least margin to the reactor coolant pressure boundary limit. The following are the most risk-significant ATWS scenarios analyzed for the AP600:

(1) ATWS attributable to a failure of the PMS

    (a) turbine trip

    (b) loss of condenser vacuum

    (c) loss of normal feedwater

(d) complete loss of forced RCS flow

(e) feedwater malfunction that results in decrease in feedwater temperature

(f) inadvertent operation of the passive core cooling system during power operation

(g) inadvertent operation of the PRHR

(2) ATWS attributable to a failure of RTB

(a) turbine trip
(b) loss of normal feedwater

(3) ATWS attributable to mechanical failure that prevents rod insertion

(a) turbine trip
(b) loss of normal feedwater
(c) complete loss of forced RCS flow

Based on the results of the applicant's PRA evaluation, the analyzed events make up more than 97 percent of the AP600 ATWS initiating event frequency. The applicant performed the ATWS analyses with the LOFTRAN code. A MTC of -7.0 pcm/°F is used. The MTC is more negative than -7.0 pcm/°F for more than 95 percent of the AP600 18- and 24-month fuel cycles. The other kinetics parameters (such as the Doppler coefficient and minimum boron worth) used in the analyses are conservative values that bound 100 percent of the AP600 18- and 24-month first-core and equilibrium-core cycles. Consistent with the ATWS analyses for the existing plants, the plant is assumed at nominal operating conditions. To maximize the peak calculated RCS pressures, the applicant assumed 10 percent pressure accumulation for the spring-loaded pressurizer safety valves when relieving water. Nominal values for the delay times to open the CMT and PRHR discharge valves were used. For other systems factored into the ATWS analyses, conservative safety analyses setpoints and delays were used. The AP600 DAS is credited to function in the analyses for ATWS cases. Specifically, the DAS is credited to actuate a turbine trip and the PRHR when applicable automatic signals are generated. For cases where a mechanical common mode failure (which prevents rods from inserting) is not assumed, the DAS is credited to insert the control rods on an appropriate automatic signal. The analyses show that the limiting ATWS case is the LONF with a mechanical failure which prevents the rods from inserting. For the limiting case, the maximum calculated pressure is 21.83 MPa (3167 psia) which is below the acceptance criteria of 22.06 MPa (3200 psi). Since conservative values for the input parameters are used, the MTC and values for kinetic parameters used in the analyses capture more than 95 percent of the AP600 fuel cycles, and the calculated peak pressure for the limiting case is within the pressure limit acceptance criteria, the staff concludes that the ATWS analyses are acceptable.

## 15.3 Radiological Consequences of Accidents

In Chapter 15 of the SSAR, Westinghouse performed radiological consequence assessments of the following seven reactor design-basis accidents (DBAs) using the

bounding set of atmospheric relative concentration (dispersion) values (or χ/Q values) provided in Table 15A-5 of Appendix 15A to the SSAR. These χ/Q values determine the required minimum distances to the exclusion area boundary (EAB) and the low-population zone (LPZ) for a given site in order to provide reasonable assurance that the radiological consequences of a DBA will be within the dose limits specified in 10 CFR 50.34(a)(1)(ii)(D)(*1*). The analyzed DBAs are

(1) main steamline failure outside containment (SSAR Section 15.1.5)

(2) reactor coolant pump shaft seizure (locked rotor) (SSAR Section 15.3.3)

(3) control element assembly ejection (SSAR Section 15.4.8)

(4) failure of small lines carrying primary coolant outside containment (SSAR Section 15.6.2)

(5) steam generator tube rupture (SSAR Section 15.6.3)

(6) loss-of-coolant accident (SSAR Section 15.6.5)

(7) fuel handling accident (SSAR Section 15.7.4)

In Chapter 15 of the SSAR, Westinghouse concludes that the AP600 design will provide reasonable assurance that the radiological consequences resulting from any of the above DBAs will be within the dose criteria specified in 10 CFR 50.34(a)(1)(ii)(D)(*1*) [25 rem Total Effective Dose Equivalent (TEDE)] and the control room operator dose criterion specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600 design, 5 rem TEDE). Westinghouse reached this conclusion

(1) using the reactor accident source terms provided in NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants,"

(2) relying on natural deposition of fission-product aerosol within the containment,

(3) controlling the pH of the water in the containment to prevent iodine evolution, and

(4) using a bounding set of hypothetical χ/Q values.

The χ/Q values are the relative atmospheric concentrations of radiological releases at the receptor point in terms of the rate of radioactivity release. In lieu of site-specific meteorological data, Westinghouse provided a bounding set of χ/Q values for the AP600 design using the meteorological data that is representative of an 80 to 90th percentile of U.S. operating nuclear power plant sites. The bounding set of χ/Q values are listed in Tables 2-1 and 15A-5 of the SSAR.

The staff performed its evaluation of the radiological consequences of DBAs against the dose criteria specified in 10 CFR 50.34(a)(1)(ii)(D) because it was the Commission's intent that this new siting criteria be used for future nuclear power plants. However, when the staff

codified the new reactor site criteria for nuclear power plants (61 FR 65157; December 11, 1996), it made an error in the assignment of applicants that could use the new dose criteria [25 rem TEDE]. The assignment of applicants in 10 CFR 50.34(a)(1) should not have included applicants for a design certification or combined license who applied prior to January 10, 1997 (refer to 61 FR 65158). The Commission adopted 25 rem TEDE as the new dose criterion for future plant evaluation purposes, because this value is essentially the same level of risk as the current criteria (61 FR 65160). Therefore, the Commission has determined that the special circumstances described in 10 CFR 50.12(a)(2)(ii) exist in that application of the 25 rem whole body criterion is not necessary to achieve the underlying purpose of the rule because 25 rem TEDE is essentially the same level of risk. On this basis, the Commission concludes that the AP600 design review can be performed pursuant to the new dose criteria [25 rem TEDE] and an exemption from the requirements of 10 CFR 50.34(a)(1) is authorized by law, will not present an undue risk to public health and safety, and is consistent with the common defense and security.

The staff also used a criterion of 5 rem TEDE for evaluating the radiological consequences from DBAs in the control room of the AP600 design, pursuant to GDC 19 of Appendix A to 10 CFR Part 50. The staff used the 5 rem TEDE criterion to be consistent with the new reactor site criteria for nuclear power plants (61 FR 65157; December 11, 1996), although GDC 19 specifies ... "5 rem whole body, or its equivalent to any part of the body" ... The Commission adopted 25 rem TEDE as the new dose criterion for plant evaluation purposes, because this value is essentially the same level of risk as the current criteria (61 FR 65160). Therefore, the Commission has determined that the special circumstances described in 10 CFR 50.12(a)(2)(ii) exist in that application of the 5 rem whole body criterion is not necessary to achieve the underlying purpose of the rule because 5 rem TEDE is essentially the same level of risk. On this basis, the Commission concludes that an exemption from GDC 19 is authorized by law, will not present an undue risk to public health and safety, and is consistent with the common defense and security.

The staff reviewed the radiological consequence analyses performed by Westinghouse using the bounding $\chi/Q$ values in SSAR Table 15A-5, and finds that the radiological consequence calculated by Westinghouse meet the above relevant dose acceptance criteria. To verify the Westinghouse analyses, the staff performed independent radiological calculations for the above DBAs using the bounding $\chi/Q$ values provided by Westinghouse and computer code described in Supplement 1 to NUREG/CR-6210, "Computer Codes for Evaluation of Control Room Habitability (HABIT)." The staff's findings are described in the following sections.

**Accident Source Terms**

In SECY-94-302, "Source Term-Related Technical and Licensing Issues Relating to Evolutionary and Passive Light-Water-Reactor Designs," dated December 19, 1994, the staff proposed to use only the "coolant," "gap," and "early in-vessel" releases from NUREG-1465 for the radiological consequence assessments of DBAs for the passive ALWR designs. These source terms encompass a broad range of accident scenarios, including significant levels of core damage with the core remaining in the vessel. These would be the most severe scenarios from which the plant could be expected to return to a safe-shutdown condition. The revised source terms in NUREG-1465 are to be applied

conservatively in evaluating DBAs in conjunction with conservative assumptions in calculating doses, such as adverse meteorology. Application to severe accidents may use more realistic assumptions.

The staff considered the inclusion of the "ex-vessel" and the "late in-vessel" source terms to be unduly conservative for DBA purposes. Such releases would only result from core damage accidents with vessel failure and core-concrete interactions. For passive ALWRs, the estimated frequencies of such scenarios are low enough that they need not be considered credible for the purpose of meeting 10 CFR 50.34. The Commission approved the staff-recommended technical positions to use only the coolant, gap, and early in-vessel releases from NUREG-1465 for the radiological consequence assessments of DBAs for the passive ALWR designs.

In an earlier submittal, Westinghouse proposed the following two departures from direct use of the NUREG-1465 source term:

(1) Low-Volatile Fission Product Release Fractions

In an earlier submittal, Westinghouse used low-volatile fission product release fractions different from that provided in NUREG-1465. The Westinghouse values were primarily based on the EPRI document entitled "Passive ALWR Source Term," issued in February 1991; compared to NUREG-1465, this source term is a reduction by a factor of 5 for the barium and strontium group and for the cerium group, and a reduction by a factor of 2 for the lanthanide group.

DSER Open Item 15.3-1 stated that Westinghouse should revise its low-volatile fission product release fractions in future SSAR revisions to reflect the staff position in NUREG-1465. Subsequently, in Revision 20 to the SSAR, Westinghouse revised its low-volatile release fractions to be consistent with those values in NUREG-1465. The staff finds these values acceptable and, therefore, DSER Open Item 15.3-1 is closed.

(2) Fission Product Release Initiation Time from Fuel Gap

In an earlier submittal, Westinghouse used a gap fission product release timing different from that provided in NUREG-1465. In that submittal, Westinghouse proposed that there would be no fission product release from the reactor core until 53 minutes into a postulated design-basis LOCA, and that the gap and in-vessel releases of fission products would continue for 4 hours. Subsequently, in Revision 13 to the SSAR, Westinghouse stated that the release of fission products from the fuel to the containment in the gap release phase would be in two stages:

(a) The release of gap activity from 5 percent of the fuel rods would begin instantaneously at the initiation of a DBA.

(b) The release of gap activity from the remaining 95 percent of the fuel rods would begin at the 50-minute mark from the initiation of a DBA.

In the DSER, the staff stated that its review of Westinghouse's technical positions regarding fission product release timing and the bounding reactor accident sequences selected for the source term applications was not complete. This was identified as DSER Open Item 15.3-2. Subsequently, the staff has completed its review and found that the gap fission product release timing proposed in the earlier submittal for the AP600 design by Westinghouse are not acceptable for the AP600 design certification. As a result of this finding, in Revision 20 to the SSAR, Westinghouse revised the gap fission product release timing to be consistent with that in NUREG-1465. The staff finds these values acceptable and, therefore, DSER Open Item 15.3-2 is closed.

**Post-Accident Containment Water Chemistry Management**

In NUREG-1465, the staff concluded that iodine entering the containment from the reactor core during an accident would be composed of at least 95 percent cesium iodide (CsI), with no more than 5 percent of iodine (I) and hydrogen iodide (HI). However, organic iodide can be produced by the reaction of elemental iodine with organic materials present in the containment.

In its radiological consequence assessments of LWRs, the staff found that iodine in organic form is a significant contributor for the offsite control room operator doses because no removal mechanisms are available for the organic form of iodine other than decay and passive deposition within the containment. Since the AP600 design provides no active iodine removal mechanisms other than passive aerosol deposition, the staff believes that the amount of organic iodine formation is less significant when compared to that for LWRs with active removal mechanisms.

In the DSER, the staff stated that when the pH of the water in the containment is maintained above 7, no more than 4 percent of the airborne elemental iodine will be converted into organic species. This amount of organic iodide would thus correspond to about 0.2 percent of the core iodine inventory (i.e., 4 percent conversion of the 5 percent elemental iodine is 0.2 percent). Westinghouse proposed to use 0.15 percent organic iodine formation based on the EPRI passive plant source term. This was identified as DSER Open Item 15.3-3.

Subsequently, when the final version of NUREG-1465 was issued, the staff revised its technical position concerning the amount of organic iodine so that no more than 3 percent (instead of 4 percent) of the airborne elemental iodine will be converted into organic species. This amount of organic iodide would thus correspond to about 0.15 percent of the core iodine inventory (i.e., 3 percent conversion of the 5 percent elemental iodine is 0.15 percent); therefore, the staff agrees with the Westinghouse position.

In the DSER, the staff stated that the SSAR should be revised to reflect the use of the staff's value of 0.2 percent iodine in organic form for the AP600 design. This was identified as DSER Open Item 15.3-3. As a result of its final evaluation of this matter as discussed in NUREG-1465, the staff withdrew this request. Therefore, DSER Open Item 15.3-3 is closed.

Once in the containment, highly soluble cesium iodide will readily dissolve in water pools, forming iodide ($I^-$) in solution and deposit onto the interior surfaces. The staff also stated in NUREG-1465 that the radiation-induced conversion of iodide in water into elemental

iodine ($I_2$) is strongly dependent on the pH. The staff indicated that without pH control, large fractions of iodine dissolved in water pools in ionic form will be converted to elemental iodine, and will be released into the containment atmosphere if the pH is less than 7.

On the other hand, if the pH is maintained above 7, very little (less than 1 percent) of the dissolved iodine will be converted to elemental iodine. The chemical addition to and mixing of the AP600 containment water following a DBA to control and maintain the pH of the water in the containment above 7 was identified as DSER Open Item 15.3-4. In response to RAI Q470.31 concerning DSER Open Item 15.3-4, Westinghouse evaluated iodine evolution and pH control for the following three water transport cases within the containment following a DBA:

(1) LBLOCA with complete mixing of the containment water
(2) SBLOCA with poor mixing of the IRWST solution and the containment water
(3) LBLOCA with poor mixing of the IRWST solution and the containment water

In the analyses of these accident sequences, Westinghouse considered the following factors:

(1) the water mass and its boric acid concentrations in the reactor coolant system and the passive core cooling system injection lines

(2) the addition of trisodium phosphate (TSP)

(3) hydrochloric acid generated from electrical cable degradation

(4) cesium hydroxide formed from the fission products released from the core

(5) nitric acid produced by irradiation of water and air

Westinghouse used the methods and models described in NUREG/CR-5950, "Iodine Evolution and pH Control," to determine the formation of hydrochloric and nitric acids.

The first case assumes a LBLOCA and all of the water in the containment is well mixed including the residual water in the IRWST. Both Westinghouse and the staff (using an independent calculation) concluded that, with the amount of TSP provided in the AP600 containment, the pH of the post-accident water in the containment will remain above 7 for the entire duration of a DBA. To verify this conclusion, the staff experimentally measured the pH of a solution comprised with the same proportions of containment water, TSP, boron, and cesium hydroxide expected to be present in the AP600 containment following an LBLOCA. The pH of this solution was measured as 6.9. After this pH measurement, the solution was titrated with nitric acid to simulate the radiolytic production of hydrochloric and nitric acid formation from water, air, and electrical cables. With this titration, the pH value decreased to 6.8. The staff finds that the difference of 0.2 in pH value (calculated value against the staff's measured value) is insignificant for radiolytic conversion of iodide in solution to elemental iodine based on the iodide-to-iodine conversion model in NUREG/CR-5950.

The second case assumes an SB LOCA depositing all of the source term in the IRWST, maximizing the initial iodine activity in the IRWST. It is further assumed that water in the IRWST is drained; less than 20 percent of the water remains in the IRWST; and containment water, which is treated with TSP, is assumed not to mix with the residual water in the IRWST. The condensed steam from the containment shell is delivered to the IRWST with hydrochloric and nitric acids generated in the high-radiation environment.

Westinghouse calculated that the water in the IRWST will initially be at a pH of 6.2, a pH of 5.4 at 12 hours into a DBA, and a pH in the range of 4.6 to 4.8 after 24 hours. Therefore, there will be conversion of cesium iodide into elemental iodine in water and reevolution of iodine into the containment atmosphere. Using methodology and models provided in NUREG/CR-5950, Westinghouse calculated that the conversion of iodide to iodine in solution would result in additional radiological consequences of less than 0.1 rem TEDE at the LPZ and less than 0.5 rem TEDE to the operators in the main control room.

The staff believes that, for the first 24 hours into a DBA, the cesium iodide source term behavior and its transport within the containment will be entirely dominated by aerosol transport and removal mechanisms independent of iodine evolution and pH control. Consequently, any postulated radiological consequences at any point on the boundary of the exclusion area for a 24-hour period is not affected by iodine evolution and pH control. The staff independently verified the iodine reevolution from the containment water into the containment atmosphere calculated by Westinghouse using models in the TRENDS code, and confirmed that the additional radiological consequences are less than 0.1 rem TEDE at the LPZ and less than 0.5 rem TEDE to the operators in the main control room. Even with the calculated doses of additional 0.1 rem TEDE at the LPZ and 0.5 rem TEDE to the operators in the main control room due to the iodine evolution, the doses calculated for the containment leak are within the dose criteria specified in 10 CFR 50.34 and GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600 design, 5 rem TEDE), respectively (see Table 15.3-1 of this report).

The third case assumes an LBLOCA that releases the entire source term into the containment atmosphere. As in Case 2 above, it is assumed that the water in the IRWST is drained, less than 20 percent of the water remains in the IRWST, and containment water treated with TSP is assumed not to mix with the residual water in the IRWST. The steam condensing on the containment shell and surfaces is assumed to be collected by the gutters and delivered to the IRWST.

Using the methodology and models provided in NUREG/CR-5950, Westinghouse calculated additional radiological consequences for this case of less than 0.2 rem TEDE at the LPZ and less than 1.0 rem TEDE to the operators in the control room. As in Case 2 above, the staff independently verified the iodine reevolution from the containment water into the containment atmosphere calculated by Westinghouse using models in the TRENDS code, and confirmed that the additional radiological consequences are less than 0.1 rem TEDE at the LPZ and less than 1.0 rem TEDE to the operators in the main control room. Even with the calculated doses of an additional 0.1 rem TEDE at the LPZ and 1.0 rem TEDE to the operators in the main control room due to the iodine evolution, the doses calculated for the containment leak are within the dose criteria specified in 10 CFR 50.34 and GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600 design, 5 rem TEDE), respectively (see Table 15.3-1).

In the DSER, the staff stated that the issue of chemical addition to and mixing of the containment water following a DBA to control and maintain pH of the water in the containment above 7 was not resolved. This was identified as DSER Open Item 15.3-4. Subsequently, on the basis of the above evaluation, Westinghouse's response to RAI Q470.31, and the staff's independent verifications, the staff finds that Westinghouse has adequately addressed this open item and, therefore, DSER Open Item 15.3-4 is closed.

**Aerosol Removal Mechanisms**

An active containment atmosphere cleanup system has not been provided for the AP600 design. Reliance is placed on natural aerosol removal processes in the containment such as holdup (for decay), sedimentation (for settling), diffusion (for plateout), and leakage (for depletion). In Revision 17 to the SSAR, Westinghouse provided a containment spray system for accident management following a severe accident as part of the AP600 fire protection system design. (See Section 19.2.3.3.9 of this report.) The containment spray system design is not safety-related, and is not intended to be used during or following a DBA. Therefore, no credit is given for mitigation of radiological consequence assessments following a DBA.

In Table 15B-1 of Appendix 15B to the SSAR, Westinghouse provides aerosol removal coefficients starting at the onset of gap release through the first 24 hours into a DBA. The values range between 0.43 to 0.72 per hour. In its independent evaluation of aerosol removal coefficients, the staff considered two natural processes for removing aerosols from the containment atmosphere over the entire period of an accident (30 days):

(1) sedimentation mechanism of gravitational settling, including aerosol agglomeration
(2) diffusion mechanisms of diffusiophoresis and thermophoresis

Considering these two natural processes for removing aerosols from the containment atmosphere, the staff performed quantitative analyses of uncertainties in prediction of the aerosol removal rates. The uncertainty analyses were performed using Monte Carlo methods.

In its evaluation of aerosol removal rates, the staff used

(1) the containment geometry (volume, upward facing surface area, etc.) and thermal-hydraulic parameters provided by Westinghouse

(2) fission product release timing, fractions, and release rates as described in NUREG-1465

The principal uncertainties in aerosol properties and aerosol behavior considered in the staff's analyses included

(1) aerosol size distribution
(2) aerosol void fraction (aerosol particle shape factors)
(3) non-radioactive aerosols
(4) chemical forms of radionuclides

The staff estimated aerosol removal rates at several confidence levels (i.e., 10, 50, 90, and 95 percent confidence levels).

In its estimation of aerosol removal rates in the containment, the staff used the thermal-hydraulic (T-H) conditions associated with the 3BE-1 severe accident sequence (direct vessel injection line failure with failure to inject water from the refueling water storage tank). During its review of the AP600 design, the ACRS raised a concern about using the thermal-hydraulic conditions associated with a specific sequence while determining aerosol removal rates due to diffusiophoresis and thermophoresis. The staff concludes that using the T-H conditions associated with the 3BE-1 severe accident sequence is representative of the spectrum of accidents evaluated for the AP600 because

(1) It is representative of the "3BE" accident class, which is the dominant contributor to the core damage frequency for the AP600.

(2) It is the most analyzed accident sequence by Westinghouse and the staff.

(3) The T-H conditions for 3BE accidents are typical of most of the analyzed sequences because the majority of severe accident sequences analyzed for the AP600 design are fully depressurized and reflooded, given the highly reliable automatic depressurization system.

(4) The corresponding T-H profiles for these depressurized and reflooded cases are sufficiently similar.

(5) The use of a fully depressurized, low pressure accident sequence in conjunction with the source term described in NUREG-1465 is appropriate because the release fractions for the source terms presented in NUREG-1465 are intended to be representative or typical of those associated with a low pressure core-melt accident

Therefore, the staff concludes that the 3BE-1 accident sequence is appropriate for determining the amount of credit to give to the natural aerosol removal processes in the AP600 containment. Because of the unique nature of the AP600 design that enhances natural aerosol removal phenomena (such as the enhanced condensation of steam by external cooling of the containment vessel instead of an internal containment spray), the staff has approved the use of this T-H profile specifically for the AP600. Credit for aerosol removal due to diffusiophoresis and thermophoresis is not intended to be generic for other plant designs, and will need to be approved on a case-by-case basis.

The AP600 design relies on natural circulation currents enhanced by the passive containment cooling system (PCS) to inhibit stratification of the containment atmosphere. The physical mechanisms of natural circulation mixing that occur in the AP600 are discussed in Appendix 15A of the SSAR. Steam generated by decay heat can vent into the containment atmosphere in the form of a jet plume through the postulated break or the fourth stage of the ADS. The interaction of the plume with the ambient atmosphere can be described in terms of entrainment flow induced by the plume. Entrainment flow results in the mixing of ambient atmosphere with the steam flow in the plume. The plume will rise to the containment dome where the steam will be condensed on the inner surface of the containment shell and the resulting cooler, denser air will fall to the operating deck.

Westinghouse provided an estimate of the degree of mixing by calculating volumetric flow rates of gas entrained by a rising buoyant plume associated with steam generated by decay heat. The calculations were made on the basis of steam production rates corresponding to decay heat at 1 hour and 24 hours into the accident. Entrainment flow rates were calculated using equations presented in an article by Peterson in Volume 37, Supplement 1, of the International Journal of Heat and Mass Transfer, entitled, "Scaling and Analysis of Mixing in Large Stratified Volumes." In the Westinghouse estimate, no credit was taken for cold plumes falling from the containment dome which cause further circulation above the operating deck. Westinghouse estimated the circulation time constant at 1 hour to be 490 seconds and at 24 hours to be 670 seconds. Confirmatory calculations by the staff using the same equations as Westinghouse, but containment atmospheric conditions calculated by the staff, indicate that the estimates are reasonable. (See Section 6.2.4 of this report.) Therefore, the staff concludes that the AP600 containment atmosphere is well-mixed for the purpose of determining the aerosol removal rates.

The staff finds that the conservative lower bound aerosol removal rate ranged between 0.35 to 0.82 per hour for the first 24 hours into a DBA (see Table 15.3-7). The best-estimate (50 percent confidence level) aerosol removal rates ranged from 0.38 to 0.86. The staff concludes that the 95 percent confidence level values for the aerosol removal rates are the appropriate values for DBA dose calculations; these values provide an acceptable level of conservatism.

In the DSER, the staff stated that it would perform an independent evaluation of the bounding accident sequence and the aerosol behavior and removal rates corresponding to the selected bounding accident sequence in the containment following a DBA. This was identified as DSER Open Item 15.3-5. The staff has completed its evaluation, and finds that the difference in resulting calculated radiological consequences using Westinghouse and the staff's aerosol removal rates are insignificant. Accordingly, the Westinghouse aerosol removal rates are acceptable, and DSER Open Item 15.3-5 is closed.

15.3.1 Radiological Consequences of a Main Steamline Break Outside Containment

Both the staff and Westinghouse have evaluated the radiological consequences of a postulated steamline break accident occurring outside of the containment and upstream of the main steam isolation valves. Westinghouse analyzed this hypothetical accident using

(1) 500 gallons per day of primary-to-secondary leakage through any one steam generator, as specified in the AP600 TS

(2) discharge of the entire mass of secondary water from one affected steam generator (182,000 lbs) to the environment with no iodine partition

Westinghouse submitted a radiological analysis for the main steamline break accident in Section 15.1.5.4 of the SSAR.

The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable, and that the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria.

To verify the Westinghouse assessment, the staff performed an independent radiological consequence calculation for three scenarios for the main steamline break accident. For Case 1, the most reactive control rod was assumed to be stuck in the fully withdrawn position. Westinghouse indicates, and the staff agrees, that no departure from nucleate boiling is expected to occur; therefore, no fuel-cladding failure was assumed in the calculation. With no additional fuel failures occurring, Case 1 becomes identical to Case 2 (discussed below), and no radiological consequences are presented for Case 1.

For Case 2, the staff assumed that a temporary increase in the primary coolant iodine concentration (iodine spike) occurred as a result of the power/pressure transient caused by the main steamline break accident. Before the accident, the AP600 reactor was assumed to be operating at the AP600 TS equilibrium limit of 0.4 μCi/gm dose equivalent iodine-131 (DEI-131) in the primary coolant. The iodine spike generated during the accident is assumed to increase the release rate of iodine from the fuel by a factor of 500. This increase in the release rate results in an increasing concentration in the primary coolant during the course of the accident. For Case 3, the staff assumed that previous reactor operation had resulted in a primary coolant iodine concentration equal to the maximum instantaneous AP600 TS limit of 24 μCi/gm DEI-131.

The major parameters and assumptions used by the staff for the main steamline break accident are provided in Table 15.3-2, and the resulting radiological consequence analyses for the EAB, LPZ, and control room are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design, as bounded by the atmospheric relative concentrations proposed by Westinghouse, will provide reasonable assurance that the radiological consequences of a postulated main steamline break accident will not exceed a small fraction (i.e., 10 percent or 2.5 rem TEDE) of the dose criteria set forth in 10 CFR 50.34 and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

### 15.3.2 Reactor Primary Coolant Pump Seizure (Locked Rotor)

The reactor primary coolant pump seizure accident is caused by an instantaneous seizure of an RCP rotor rapidly reducing the primary coolant flow through the affected reactor coolant loop leading to a reactor trip on a low-flow signal. Westinghouse analyzed this hypothetical accident assuming that 18 percent of the fuel elements will experience cladding failure, releasing the entire fission product inventory in the fuel-cladding gap of these elements to the reactor coolant. Activity released to the primary coolant is carried to the secondary coolant by the maximum allowable 260 lbs/hour (1000 gallons/day) of primary-to-secondary leakage through two SGs as specified in the AP600 TS. Activity is released to the environment via the steamline safety valves or the power-operated relief valves. Westinghouse submitted a radiological analysis for the reactor primary coolant pump seizure accident in Section 15.3.3 of the SSAR.

The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable, and that the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria.

To verify the Westinghouse assessment, the staff performed independent radiological consequence calculations for the reactor primary coolant pump seizure accident using NUREG-1465 source terms. The major parameters and assumptions used by the staff are provided in Table 15.3-3 of this report, and the resulting radiological consequence analyses are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design, as bounded by the atmospheric relative concentrations proposed by Westinghouse, will provide reasonable assurance that the radiological consequences of a postulated reactor primary coolant pump seizure accident will not exceed a small fraction (i.e., 10 percent or 2.5 rem TEDE) of the dose criteria set forth in 10 CFR 50.34 and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

15.3.3 Radiological Consequences of Control Element Assembly Ejection

The mechanical failure of a control rod mechanism pressure housing is postulated to result in the ejection of a rod cluster control assembly (RCCA) and drive shaft. Because of the resultant opening in the pressure vessel, primary coolant is lost to the containment with concurrent rapid depressurization of the reactor pressure vessel. The consequence of this mechanical failure is a rapid positive reactivity insertion together with an adverse core power distribution, possibly leading to localized fuel rod damage.

Westinghouse has assumed that 15 percent of the fuel elements will experience cladding failure, releasing the entire fission product inventory in the fuel-cladding gap of these elements. In addition, Westinghouse assumed that 0.375 percent of the fuel rods may experience fuel melting. Westinghouse performed its calculations to obtain these parameters using the guidelines provide in RG 1.77, "Assumptions Used for Evaluating a Control Rod Ejection Accident for PWRs;" therefore, the staff finds these assumptions to be acceptable. Westinghouse submitted a radiological consequence analysis for control element assembly ejection accident in Section 15.4.8 of the SSAR.

The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable and that the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria.

Westinghouse assumed that the release of fission products to the environment may occur via either of two pathways. The first pathway involves a release of primary coolant to the containment, which is then assumed to leak to the environment at the design leak rate of the containment. In the second pathway, fission products would reach the secondary coolant via the steam generators with a maximum total allowable primary-to-secondary leak rate of 1000 gallons/day as specified in the AP600 TS. For both pathways, Westinghouse assumed that the AP600 reactor was operating at its TS instantaneous primary coolant limit of 24 μCi/gm for DEI-131.

To verify the Westinghouse assessment, the staff performed independent radiological consequence calculations for the same two pathways as described above for the control rod ejection accident using NUREG-1465 source terms. The major parameters and

assumptions used by the staff are provided in Table 15.3-4 of this report, and the resulting radiological consequence analyses are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design, as bounded by the atmospheric relative concentrations proposed by Westinghouse, will provide reasonable assurance that the radiological consequences of a postulated control element assembly ejection accident will be well within the dose criteria set forth in 10 CFR 50.34 and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

In the DSER, the staff stated that it would complete an independent radiological consequence assessment of the control element assembly ejection accident when source term related issues were resolved to verify that the following criteria are fulfilled:

(1) The Westinghouse analysis of the radiological consequences following a postulated control element assembly ejection accident provided in Section 15.4.8 of the SSAR is adequate.

(2) The proposed operation of the AP600 reactor within the limits of the TS assumed above will provide reasonable assurance that the calculated radiological consequences are well within (less than 25 percent) of the dose reference values of 10 CFR Part 100 (as applied to the AP600, this will now be 10 CFR 50.34).

This was identified as DSER Open Item 15.3.2-1. As discussed above, the staff finds that the calculated radiological consequences due to a postulated control rod ejection accident. meet relevant dose acceptance criteria. Therefore, DSER Open Item 15.3.2-1 is closed.

### 15.3.4 Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment

GDC 55 contains a provision to ensure isolation of all pipes that are part of the reactor coolant pressure boundary and penetrate the containment building. GDC 55 also provides that small-diameter pipes that must be continuously connected to the primary coolant system in order to perform necessary functions may be acceptable based on some other defined bases. For these lines, methods of mitigating the consequences of a rupture are necessary because the lines cannot be automatically isolated. For the AP600 design, there are two small lines in this category:

(1) the reactor coolant system sample line

(2) the discharge line from the CVS to the liquid radwaste system

No instrument lines carry primary coolant outside containment in the AP600 design.

When excess primary coolant inventory is generated as a result of boron dilution operations, the CVS purification flow is diverted out of containment to the liquid radwaste system. Before passing outside containment, the flow stream passes through the CVS heat exchangers and mixed bed demineralizer. The flow leaving the containment will be at

temperature of less than 60 °C (140 °F) and has been processed by the demineralizer. The flow from a postulated break in this line is limited to the CVS purification normal flow rate of 100 gpm. Considering the low temperature of the break flow and the reduced iodine activity, Westinghouse proposed in SSAR Section 15.6.2, and the staff accepted, that the postulated sample line is the more limiting event for the radiological consequence assessment.

The sample line includes a flow restrictor at the point of sample to limit the break flow to less than 130 gpm. Westinghouse proposed in SSAR Section 15.6.2, and the staff accepted, that the break flow isolation time will be less than 30 minutes. The fluid escaping the break is assumed by Westinghouse to be at the equilibrium (accident initiated spike) primary coolant iodine concentration limits in the AP600 TS. The staff finds this to be acceptable. Westinghouse submitted a radiological analysis for a small line failure in Section 15.6.2 of the SSAR.

The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable, and the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria. To verify the Westinghouse assessment, the staff performed independent radiological consequence calculations for two scenarios for a postulated small line break accident. For Case 1, the staff assumed that a temporary increase in the primary coolant iodine concentration (iodine spike) occurred as a result of the power/pressure transient caused by the small line break accident. Before the postulated accident, the AP600 reactor was assumed to be operating at the AP600 TS equilibrium concentration limit of 0.4 μCi/gm DEI-131 in the primary coolant.

The iodine spike generated during the accident is assumed to increase the release rate of iodine from the fuel by a factor of 500. This increase in the release rate results in an increasing iodine concentration in the primary coolant during the course of the accident. For Case 2, the staff assumed that previous reactor operation had resulted in a primary coolant concentration equal to the maximum instantaneous iodine concentration limit of 24 μCi/gm DEI-131 specified in the AP600 TS.

The major parameters and assumptions used by the staff are provided in Table 15.3-5, and the resulting radiological consequence analyses are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design as bounded by the atmospheric relative concentrations proposed by Westinghouse will provide reasonable assurance that the radiological consequences of a postulated small line break accident will not exceed a small fraction (i.e., 10 percent or 2.5 rem TEDE) of the dose criteria set forth in 10 CFR 50.34 and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

### 15.3.5 Steam Generator Tube Rupture Accident

Westinghouse has evaluated the radiological consequences of a postulated SGTR accident and provided a radiological consequence analysis for the accident in SSAR Section 15.6.3. The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable, and the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria.

To verify the Westinghouse assessments, the staff performed independent radiological consequence calculations for two scenarios for the SGTR accident. For Case 1, the staff assumed that a temporary increase in the primary coolant iodine concentration (iodine spike) occurred as a result of the power/pressure transient caused by the SGTR. Before the postulated accident, the AP600 reactor was assumed to be operating at the AP600 TS equilibrium iodine concentration limit of 0.4 μCi/gm DEI-131 in the primary coolant. The iodine spike generated during the accident is assumed to increase the release rate of iodine from the fuel by a factor of 500. This increase in the release rate results in an increasing iodine concentration in the primary coolant during the course of the accident.

For Case 2, the staff assumed that previous reactor operation had resulted in a primary coolant concentration equal to the maximum instantaneous concentration limit of 24 μCi/gm DEI-131 specified in the AP600 TS. The major parameters and assumptions used by the staff are provided in Table 15.3-2 of this report, and the resulting radiological consequence analyses for the exclusion area boundary and low population zone and for the control room are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design as bounded by the atmospheric relative concentrations proposed by Westinghouse will provide reasonable assurance that the radiological consequences of a postulated SGTR accident will not exceed a small fraction (i.e., 10 percent or 2.5 rem TEDE) of the dose criteria set forth in 10 CFR 50.34 and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

In the DSER, the staff stated that its independent radiological consequence calculations for the SGTR event were not complete. This was identified as DSER Open Item 15.3.5-1. As discussed above, the staff has completed its independent calculations; therefore, DSER Open Item 15.3.5-1 is closed.

### 15.3.6 Radiological Consequences of Loss-of-Coolant Accidents (LOCAs)

In SSAR Section 15.6.5, Westinghouse analyzed a hypothetical design-basis LOCA. Westinghouse concludes that certain bounding sets of atmospheric relative concentration values specified in SSAR Section 2.3, in conjunction of the use of natural deposition of fission product aerosol within the containment and controlling the pH of the water in the containment to prevent iodine evolution, are sufficient to provide reasonable assurance that the calculated radiological consequences of a postulated design-basis LOCA will be within the relevant dose criteria established in 10 CFR 50.34 and in GDC 19 (as applied to the AP600 design, 5 rem TEDE).

Because no specific site is associated with the AP600 plant, Westinghouse defined the site boundaries only in terms of various hypothetical atmospheric relative concentrations ($\chi/Q$) values at fixed EAB and LPZ distances. The staff will perform an independent assessment of short-term (less than 30 days) atmospheric dispersion factors for potential accident consequence analyses on a site-specific basis for a COL applicant who references the AP600 design. If site-specific atmospheric dispersion factors are greater than the enveloping values (e.g., poorer dispersion characteristics) used in this evaluation, a COL applicant may have to consider compensatory measures, such as increasing the size of the site or providing engineered safety feature systems in the AP600 design, to meet the relevant dose limits set forth in 10 CFR 50.34 and GDC 19 (as applied to the AP600 design, 5 rem TEDE).

All of the fission product releases due to the LOCA are the result of containment leakage. The AP600 design does not have engineered safety features (ESF) systems outside of the containment; therefore, no leakage from the ESF systems is considered for the radiological consequence analyses. The containment was assumed to leak at its design leak rate of 0.1 weight percent per day for the entire duration of the accident (30 days). The AP600 design provides neither an ESF filtration (e.g., charcoal adsorbers) nor a safety-related containment spray system.

To verify the Westinghouse assessment, the staff performed independent radiological consequence calculations for a postulated design-basis LOCA coincident with the loss of spent fuel pool cooling capability. In this calculation, the staff used the NUREG-1465 source term and aerosol removal rates developed by the staff. The major parameters and assumptions used by the staff are provided in Tables 15.3-6 and 15.3-7 of this report, and the resulting radiological consequence analyses are provided in Table 15.3-1. The major assumptions used by the staff to determine the radiological consequences to the control room operators following a LOCA are provided in Table 15.3-8, and those used to determine the radiological consequences to personnel in the main control room and technical support center following a LOCA with the nuclear island non-radioactive ventilation (VBS) system operation are provided in Table 15.3-9.

As shown in Table 15.3-1, the staff finds that the radiological consequences of a design-basis LOCA coincident with the loss of spent fuel pool cooling capability at the EAB and LPZ, and control room operator dose with the bounding atmospheric relative concentrations proposed by Westinghouse, meet the dose criteria set forth in 10 CFR 50.34 (25 rem TEDE) and GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600 design, 5 rem TEDE), respectively. Therefore, the staff finds that the AP600 design is acceptable.

In the DSER, the staff stated that a COL applicant referencing the AP600 design should identify all compensatory measures to be relied on in order to meet the relevant requirements of 10 CFR 50.34 and GDC 19. This was identified as DSER Open Item 15.3.4-1 and COL Action Item 15.3.4-1. Revision 13 to the SSAR included this information in Sections 2.3.6.4 and 2.3.6.5; therefore, DSER Open Item 15.3.4-1 is closed.

In the DSER, the staff stated that it would review the bounding accident break size (an LBLOCA followed by gravity injection failure) proposed by Westinghouse during a meeting on source terms in conjunction with Westinghouse technical positions on fission product

release timing. This was identified as DSER Open Item 15.3.4-2. Subsequently, in Revision 20 to the SSAR, Westinghouse followed the NUREG-1465 source term with no exceptions as stated in SSAR Section 15.3. Therefore, DSER Open Item 15.3.4-2 is closed with the closure of DSER Open Items 15.3-1, 15.3-2, and 15.3-3. (See Section 15.3 of this report.)

In the DSER, the staff stated that it had not completed its review related to the use of non-safety-related systems in response to a DBA for potential leakages, and the staff was awaiting Westinghouse's submittal of proposed ERGs for the AP600 design in order to complete its safety review. This was identified as DSER Open Item 15.3.4-3. Subsequently, Westinghouse submitted the ERGs. The staff's review is discussed in Chapter 19 of this report. The staff concludes that there will be no significant leakage resulting from the use of non-safety-related systems following a DBA to contribute to the radiological consequences analyzed. The staff finds this acceptable and, therefore, DSER Open Item 15.3.4-3 is closed.

In the DSER, the staff stated that it would complete its independent radiological consequence assessment of a hypothetical LOCA when it resolved source term related issues with Westinghouse. This was identified as DSER Open Item 15.3.4-4. Subsequently, as discussed throughout Section 15.3 of this report, the staff completed its independent radiological consequence assessment of a postulated LOCA; therefore, DSER Open Item 15.3.4-4 is closed.

### 15.3.7 Radiological Consequences of Fuel Handling Accident

In SSAR Section 15.7.4, Westinghouse presented its analyses of the radiological consequences of a postulated fuel handling accident (FHA). For the AP600 design, an FHA can be postulated to occur either inside containment or in the fuel handling area inside the auxiliary building. If the FHA occurs in the containment, the release of fission products can be terminated by closure of the containment purge lines based on the detection of high airborne radioactivity. For the postulated FHA occurring in the containment and in the auxiliary building (spent fuel pit), Westinghouse assumed, and the staff agrees, that fission products are directly released to the environment within a 2-hour period without credit for any iodine removal processes.

Westinghouse performed the radiological consequences analyses of an FHA assuming a single fuel assembly dropped such that the activity in every rod in the dropped assembly is released. The loss of spent fuel pool cooling capability is also assumed. The kinetic energy of the falling fuel assembly is assumed to break open the maximum possible number of fuel rods (264) using perfect mechanical efficiency. Instantaneous release of noble gases and radioiodine vapor from the gaps of the broken rods (3.6 percent of noble gases, iodine, and cesium inventories in the reactor core) is assumed to occur, with the released gases bubbling up through the fuel pool water (with an effective decontamination factor of 133 for elemental iodines and of 1 for noble gases and organic iodine). Westinghouse assumed that iodine in the particulate form is not volatile, and therefore, not released.

In NUREG-1465, the gap release fractions for iodine, cesium, and noble gases are specified as 3 percent of core inventory if long-term fuel cooling is maintained. Westinghouse increased the gap release fractions, and the staff agrees, to 3.6 percent to address

concerns identified in NUREG-1465 regarding applicability of the 3 percent gap release fractions to fuel with burnup in excess of 40 gigawatt days per metric tons of uranium (GWD/T). According to NUREG-5009, "Assessment of the Use of Extended Burnup Fuel in Light Water Power Reactors," dated February 1989, a maximum burnup of 60 GWD/T increases the iodine doses for a FHA by a factor of 1.2.

The spent fuel pool cooling system is designed to perform the following functions:

(1) remove heat from the spent fuel pit
(2) remove radioactive corrosion and fission products
(3) maintain water clarity during all modes of plant operation

The system consists of redundant trains. Each train includes a pump, a heat exchanger, a filter, and a demineralizer. However, the spent fuel pool cooling system is a non-safety-related system. Therefore, Westinghouse assumed, and the staff agrees, that there is a loss of spent fuel pool cooling capability coincident with the fuel handling accident.

The staff has reviewed the Westinghouse analysis and finds that the calculational methods used for the radiological consequence assessment are acceptable, and the radiological consequences calculated by Westinghouse meet the relevant dose acceptance criteria.

To verify the Westinghouse assessments, the staff performed independent radiological consequence calculations for the fuel handling accident coincident with a loss of the spent fuel pool cooling capability. The major parameters and assumptions used by the staff are provided in Table 15.3-10 of this report, and the resulting radiological consequence analyses are provided in Table 15.3-1. The radiological consequences calculated by the staff are consistent with those calculated by Westinghouse.

The staff concludes that the AP600 design as bounded by the atmospheric relative concentrations proposed by Westinghouse will provide reasonable assurance that the radiological consequences of a postulated fuel handling accident with the loss of spent fuel pool cooling capability will be well within the dose criteria set forth in 10 CFR 50.34 (i.e., 25 percent or 6.2 rem TEDE) and the control room dose acceptance criteria specified in GDC 19 of Appendix A to 10 CFR Part 50 (as applied to the AP600, 5 rem TEDE).

In the DSER, the staff stated that Westinghouse assumed that less than 3 percent of fission-product core inventory will be in the fuel gap while 5 percent of that is assumed in draft NUREG-1465. This was identified as DSER Open Item 15.3.6-1. The final revision of NUREG-1465 revised the 5 percent value to 3 percent if long-term fuel cooling is maintained. In Revision 13 to the SSAR, Westinghouse assumed 3.6 percent of fission product core inventory in the fuel gap, as discussed above. The staff finds this value acceptable, and therefore, DSER Open Item 15.3.6-1 is closed.

In the DSER, the staff stated that Westinghouse assumed an iodine decontamination factor (DF) of 250 in the fuel pit through 7 m (23 ft) of water depth while a value of 100 is recommended in RG 1.25 for an FHA. This was identified as DSER Open Item 15.3.6-2 . In Revision 13 to the SSAR, Westinghouse revised the elemental iodine DF to 133. The DF of 100 in RG 1.25 is for the iodine chemical composition of TID-14844 source term, and the

equivalent elemental iodine DF for the NUREG-1465 chemical composition is 133. Therefore, the staff finds that the elemental iodine DF of 133 used by Westinghouse is acceptable, and DSER Open Item 15.3.6-2 is closed.

In the DSER, the staff stated that it was reviewing the spent fuel pool boiloff rate, boiloff time, and iodine partition factor for the spent fuel pool water. This was identified as DSER Open Item 15.3.6-3. The staff has completed its review of these items (see Section 6.4) and finds that they are acceptable. Therefore, DSER Open Item 15.3.6-3 is closed.

In the DSER, the staff stated that its independent radiological consequence assessment of the fuel handling accident was not completed. This was identified as DSER Open Item 15.3.6-4. As discussed in this section, the staff has completed its assessment and, therefore, DSER Open Item 15.3.6-4 is closed.

In the DSER, the staff stated that Westinghouse had not provided the radiological consequence assessment for dropping a heavy object onto the fuel assemblies in the reactor vessel during refueling operations. This was identified as DSER Open Item 15.3.6-5. In Revision 13 to SSAR Section 15.7.6, Westinghouse stated that the spent fuel cask handling crane is prevented from traveling over the fuel pool; therefore, this evaluation is not required and DSER Open Item 15.3.6-5 is closed.

15.3.8 Offsite Radiological Consequences of Liquid Tank Failure

The staff has reviewed the liquid tank failure accident in accordance with SRP Section 15.7.3, "Postulated Radioactive Releases due to Liquid Containing Tank Failures." The acceptance criteria specified in this SRP section are based on meeting the following regulations:

(1) General Design Criterion GDC 60 as it relates to the radioactive waste management system being designed to control release of radioactive materials to the environment

(2) 10 CFR Part 20 as it relates to radioactivity in effluents to unrestricted areas.

The failure of the most limiting (i.e., in terms of offsite radiological consequences) liquid radwaste system (WLS) equipment outside the containment does not result in radionuclide concentrations in water at the nearest potable water supply in an unrestricted area exceeding the liquid effluent concentration limits for the corresponding radionuclides specified in Appendix B to 10 CFR Part 20 (Table 2, Column 2) or specific design features to mitigate the effects of failure are incorporated in the design of the WLS, if it does not meet the above requirements of 10 CFR Part 20.

In Revision 13 to SSAR Section 15.7.3, Westinghouse took a position deviating from SRP Section 15.7.3. The deviation was on the safety analysis assumption in SRP Section 15.7.3 that credit cannot be taken for liquid retention by an unlined building foundation. Westinghouse stated that in the event of a tank failure, the liquid would be directed to the auxiliary building sump. The basement of the auxiliary building is 1.8 m (6 ft) thick and the exterior walls are sealed to prevent leakage. Westinghouse assumed that there was no release of the spilled liquid waste to the environment, and no radiological consequence analysis was needed.

The staff reviewed Westinghouse's justification for the deviation and found it unacceptable, because Westinghouse did not consider the possibility of concrete cracking in the auxiliary building foundations and did not provide any basis for its position. In addition, Westinghouse did not address the potential for auxiliary building seal deterioration. There was no leak testing, technical specification control, or surveillance requirement on the leak-tightness of the auxiliary building. Therefore, the staff determined that taking credit for the building seal in the accident analysis was not acceptable.

In response to the staff's finding, Westinghouse revised SSAR Section 15.7.3 in Revision 19 to include a commitment for a COL action item to perform a site-specific offsite radiological consequence analysis, including the corresponding source term resulting from a postulated liquid tank failure. The staff finds this commitment to be acceptable because the assessment of offsite radiological consequences of liquid tank failures depends upon site-specific parameters, such as the mode of transport of radioactive fluid resulting from the failure to the region of potable water supply, the location of potable water supply, the characteristics of the soil through which the transport occurs, and the available dilution by water-bodies before the radioactive liquid reaches the potable water supply. The staff will evaluate the site-specific analysis in accordance with SRP Section 15.3.7 for each COL applicant referencing the AP600 standard design.

Table 15.3-1
Radiological Consequences of Design-Basis Accidents
(rem TEDE)

| Postulated Accident | EAB | LPZ | Control Room |
|---|---|---|---|
| Loss of coolant | 21.8 | 6.1 | 4.6 |
| Main steamline failure outside containment: | | | |
| With concomitant iodine spike | <1.0 | <1.0 | <1.0 |
| With preaccident iodine spike | <1.0 | <1.0 | <1.0 |
| Reactor coolant pump shaft seizure | <1.0 | <1.0 | <1.0 |
| Rod ejection accident | 1.4 | <1.0 | <1.0 |
| Fuel handling accident | 1.0 | <1.0 | 3.6 |
| Small line break accident | | | |
| With concomitant iodine spike | <1.0 | <1.0 | 2.2 |
| With preaccident iodine spike | 1.8 | <1.0 | 4.6 |
| Steam generator tube rupture | | | |
| With concomitant iodine spike | <1.0 | <1.0 | <1.0 |
| With preaccident iodine spike | 1.5 | <1.0 | <1.0 |

Table 15.3-2
Assumptions Used in Computing Main Steamline Break Accident and Outside Containment and Steam Generator Tube Rupture Accident Dose

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Reactor primary coolant iodine concentrations | |
| Accident initiated iodine spike, μCi/gm DEI-131 | 0.4 |
| Preaccident iodine spike, μCi/gm DEI-131 | 24 |
| Steam generator in faulted loop | |
| Initial water mass, lb | 1.82E+5 |
| Primary to secondary leak rate, gpd | 500 |
| Iodine partition | 1 |
| Steam generator in intact loop | |
| Primary to secondary leak rate, gpd | 500 |
| Iodine partition | 0.01 |
| Steam released, lb | |
| 0 to 2 hr | 3.64E+5 |
| 2 to 8 hr | 7.15E+5 |
| Ratio of iodine release rate from fuel during iodine spike to that during steady-state operation | 500 |
| Reactor primary coolant mass, kgm | 1.63E+5 |
| Duration of accident, hr | 8 |
| Atmospheric dispersion values | |
| 0 to 2 hours, sec/$m^3$ EAB | 1.00E-3 |
| 0 to 8 hours, sec/$m^3$ LPZ | 1.35E-4 |

Table 15.3-3
Assumptions Used to Evaluate the
Reactor Coolant Pump Shaft Seizure Accident

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Fraction of fuel rods failed | 0.18 |
| Fraction of core activity in failed fuel rod gap | 0.036 |
| Reactor primary coolant iodine concentrations | |
| Accident initiated iodine spike, µCi/gm DEI-131 | 0.4 |
| Preaccident iodine spike, µCi/gm DEI-131 | 24 |
| Secondary Coolant Mass, lb | 2.15E+5 |
| Primary to secondary leak rate, lb/hr | 260 |
| Iodine partition | 0.01 |
| Steam released, lb | |
| 0 to 2 hr | 5.75E+5 |
| 2 to 8 hr | 1.04E+6 |
| Ratio of iodine release rate from fuel during iodine spike to that during steady-state operation | 500 |
| Reactor primary coolant mass, lbs | 3.39E+5 |
| Duration of accident, hrs | 8 |
| Atmospheric dispersion values | |
| 0 to 2 hours, sec/$m^3$ EAB | 1.00E-3 |
| 0 to 8 hours, sec/$m^3$ LPZ | 1.35E-4 |

Table 15.3-4
Assumptions Used in Computing Rod Ejection Accident Doses

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Peaking factor | 1.65 |
| Fraction of fuel rods failed | 0.15 |
| Fraction of fuel rods melted | 0.00375 |
| Fraction of fission-product inventory released to coolant from perforated fuel rods | |
| Iodines, percent | 5 |
| Noble gases, percent | 5 |
| Cesium, percent | 5 |
| Initial reactor coolant iodine activity, μCi/gm (DEI-131) | 24 |
| Reactor coolant mass, lbs | 3.38E+5 |
| Duration of accident, days | 30 |
| Iodine chemical form fractions | |
| Organic | 0.0015 |
| Elemental | 0.0485 |
| Particulate | 0.95 |
| Primary to secondary leak, lbs/hr | 260 |
| Atmospheric dispersion values | |
| 0 to 2 hours, sec/$m^3$ EAB | 1.00E-3 |
| 0 to 8 hours, sec/$m^3$ LPZ | 1.35E-4 |
| 8 to 24 hours, sec/$m^3$ LPZ | 1.00E-4 |
| 24 to 96 hours, sec/$m^3$ LPZ | 5.40E-5 |
| 96 to 720 hours, sec/$m^3$ LPZ | 2.20E-5 |

Table 15.3-5
Assumptions Used in Computing Small Line Failure Accident Doses

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Peaking factor | 1.65 |
| Reactor primary coolant iodine concentrations | |
| Accident initiated iodine spike, μCi/gm DEI-131 | 0.4 |
| Preaccident iodine spike, μCi/gm DEI-131 | 24 |
| Reactor coolant mass, lbs | 3.38E+5 |
| Duration of accident, minutes | 30 |
| Sample line break flow, gpm | 130 |
| Atmospheric dispersion values | |
| 0 to 2 hours, sec/$m^3$ EAB | 1.00E-3 |
| 0 to 8 hours, sec/$m^3$ LPZ | 1.35E-4 |

Table 15.3-6
Assumptions Used to Evaluate the Loss-of-Coolant Accident

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Fraction of core inventory released, fractions (NUREG-1465) | |
| Noble gases | 1.0 |
| Iodine | 0.4 |
| Cesium | 0.3 |
| Tellurium | 0.05 |
| Strontium | 0.02 |
| Barium | 0.02 |
| Ruthenium | 0.0025 |
| Cerium | 0.0005 |
| Lanthanum | 0.0002 |
| Start time for fission-product release (NUREG-1465) | |
| Coolant Activity, minutes | 0 |
| Gap Activity, minutes | 10 |
| Early In-Vessel, minutes | 40 |
| Iodines chemical form fractions (NUREG-1465) | |
| Organic | 0.0015 |
| Elemental | 0.0485 |
| Particulate | 0.95 |
| Primary containment leakage, weight percent/day | 0.1 |
| Accident duration, days | 30 |
| Primary containment free volume, cubic feet | 1.62E+6 |
| Atmospheric dispersion values | |
| 0-02 hour EAB, sec/$m^3$ | 1.00E-3 |
| 0-08 hour LPZ, sec/$m^3$ | 1.35E-4 |
| 8-24 hour LPZ, sec/$m^3$ | 1.00E-4 |
| 1-04 day LPZ, sec/$m^3$ | 5.40E-5 |
| 4-30 day LPZ, sec/$m^3$ | 2.20E-5 |

Table 15.3-7
Aerosol Removal Rates Used to Evaluate
Loss-of-Coolant Accident

| Time (hours) | Removal Rates ($hour^{-1}$) |
|---|---|
| 0.0 to 0.5 | 0.823 |
| 0.5 to 1.8 | 0.743 |
| 1.8 to 3.8 | 0.529 |
| 3.8 to 13.8 | 0.367 |
| 13.8 to 24 | 0.350 |

Table 15.3-8
Assumptions and Estimates
of the Radiological Consequences
to Control Room Operators Following a LOCA

| Parameter | Value |
|---|---|
| Control room free volume | 3.57E+4 $ft^3$ |
| Time of bottled air depleted | 72 hr |
| Prior to depletion of bottled air | |
| Flow from compressed air bottles | 60 cfm |
| Unfiltered in-leakage | 5.0 cfm |
| After depletion of bottled air | |
| Air intake flow | 1700 cfm |
| Filter efficiencies | N/A |
| Recirculation flow | N/A |
| Breathing rate of operators in control room for the course of the accident | 3.47E-4 $m^3$/sec |
| Atmospheric dispersion values | |
| 0 to 0.1925 hr | 2.0E-3 sec/$m^3$ |
| 0.1925 to 2 hr | 1.0E-3 sec/$m^3$ |
| 2 to 8 hr | 6.0E-4 sec/$m^3$ |
| 8 to 72 hr | 3.0E-4 sec/$m^3$ |
| 72 to 96 hr | 5.0E-4 sec/$m^3$ |
| 96 to 720 hr | 4.0E-4 sec/$m^3$ |
| Control room operator occupational factors | |
| 0 to 24 hr | 1 |
| 24 to 96 hr | 0.6 |
| 96 to 720 hr | 0.4 |

Table 15.3-9
Assumptions and Estimates of the Radiological Consequences to Personnel in Main Control Room and Technical Support Center Following a LOCA (for operation with VBS)

| Parameter | Value |
|---|---|
| Control room and technical support center free volume | 1.05E+5 $ft^3$ |
| Air intake flow | 860 cfm |
| Intake flow filter efficiency[1] | 90 percent |
| Unfiltered in-leakage | 140 cfm |
| Recirculation flow | 2740 cfm |
| Recirculation filter efficiency[1] | 90 percent |
| Breathing rate of operators in control room for the course of the accident | 3.47E-4 $m^3$/sec |
| Atmospheric dispersion values | |
| 0 to 2 hr | 2.0E-3 sec/$m^3$ |
| 2 to 8 hr | 1.0E-3 sec/$m^3$ |
| 8 to 24 hr | 5.0E-4 sec/$m^3$ |
| 24 to 96 hr | 5.0E-4 sec/$m^3$ |
| 96 to 720 hr | 4.0E-4 sec/$m^3$ |
| Control room operator occupancy factors | |
| 0 to 24 hr | 1 |
| 24 to 96 hr | 0.6 |
| 96 to 720 hr | 0.4 |
| Control room and technical support center operator dose (for 30-day accident duration) | 2.2 rem TEDE |

[1]For elemental and organic iodines. The filter efficiency for particulate iodine is 99 percent.

Table 15.3-10
Assumptions Used in Computing Fuel Handling Accident Doses

| Parameter | Value |
|---|---|
| Power level, Mwt | 1972 |
| Peaking factor | 1.65 |
| Number of fuel rods damaged | 264 |
| Reactor shutdown time before fuel movement, hours | 100 |
| Core fractions released from damaged rods | |
| Iodine | 0.036 |
| Noble gases | 0.036 |
| Cesium | 0.036 |
| Iodine chemical form fractions | |
| Organic | 0.0015 |
| Elemental | 0.0485 |
| Particulate | 0.95 |
| Pool decontamination factor | |
| Elemental and particulate iodines | 133 |
| Organic iodine | 1 |
| Noble gases | 1 |
| Duration of accident, hours | 2 |
| Initial iodine inventory in the spent pool (Ci) | |
| Iodine-131 | 1.60E+4 |
| Iodine-132 | 1.31E+4 |
| Iodine-133 | 1.60E+3 |
| Initial pool water mass, lbs | 1.44E+6 |
| Iodine partition factor in pool water | 100 |
| Atmospheric dispersion values | |
| 0 to 2 hours, sec/$m^3$ EAB | 1.00E-3 |
| 0 to 8 hours, sec/$m^3$ LPZ | 1.35E-4 |

# 16 TECHNICAL SPECIFICATIONS

## 16.1 Introduction

The AP600 Technical Specifications (TS) were modeled after the "Standard Technical Specifications, Westinghouse Plants," NUREG-1431 (STS). These STS were developed from the requirements resulting from the Technical Specifications Improvement Program in accordance with the Commission Final Policy Statement on Technical Specifications Improvements, SECY-93-067. In addition, Westinghouse states that the AP600 TS comply with 10 CFR 50.36(c)(2)(ii).

The staff's review of the AP600 TS concentrated on differences from the STS. These differences are the result of the new passive systems design, structural differences from existing systems, advanced microprocessor-based instrumentation and control, and the results of the review of shutdown operations.

The staff forwarded to Westinghouse comments from its review of the AP600 technical specifications for resolution and incorporation into the final technical specifications. The final AP600 technical specifications include resolution of issues raised by the staff and are certified to be accurate by Westinghouse.

## 16.2 Evaluation

The staff evaluated the AP600 technical specifications to confirm that the TS will preserve the validity of the plant design as described in the AP600 SSAR by assuring that the AP600 plant will be operated (1) within the required conditions bounded by the AP600 SSAR and (2) with operable equipment that is essential to prevent accidents and to mitigate the consequences of accidents postulated in the AP600 SSAR. The staff also assessed the AP600 TS to confirm that a limiting condition for operation (LCO) was established for any aspect of the design which met the criteria in 10 CFR 50.36(c)(2)(ii).

The AP600 design includes safety systems that are innovative and simplified. It employs passive safety-related systems that rely on natural forces such as gravity, convection, evaporation, and condensation. Although the staff requested that the AP600 TS be modeled after NUREG-1431 to the maximum extent possible, it was necessary to develop technical specifications beyond those in the STS to account for the AP600 first-of-a-kind, advanced, passive, design features. However, in most cases, the AP600 system design functions are similar to existing PWRs even though the components and systems are new. The staff requested that Westinghouse model the technical specifications based on the equivalent STS safety function. Where the staff believed modification of the STS appropriate due to the new design features, the completion times and surveillance frequencies were maintained as in the STS.

A comparison of the AP600 technical specifications with STS and an evaluation of the differences are as follows:

**AP600 TS "USE AND APPLICATION"**

The AP600 definitions, logical connectors, completion time rules, and frequency rules correspond to those specified in STS and are acceptable to the staff.

**AP600 TS "SAFETY LIMITS"**

The AP600 safety limit LCOs correspond to those specified in STS and are acceptable to the staff.

**AP600 TS "LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY AND SURVEILLANCE REQUIREMENT (SR) APPLICABILITY"**

The AP600 LCO and SR applicabilities correspond to those specified in STS and are acceptable to the staff. In addition, AP600 has added LCO 3.0.8 which provides directions for action when in Modes 5 or 6 and the applicable shutdown LCOs cannot be met. This is a consequence of the AP600 adding shutdown LCOs which are not included in STS. The AP600 TS LCO 3.0.8 has been constructed to be similar to LCO 3.0.3 for shutdown operations and the staff has assessed it to be conservative and improved over STS and is, therefore, acceptable.

**AP600 TS "REACTIVITY CONTROL SYSTEMS"**

The AP600 reactivity control systems LCOs correspond to those specified in STS and are acceptable to the staff. In addition, AP600 has added an LCO for isolation of the demineralizer water from the CVS to prevent an inadvertent boron dilution event. The need for this TS is in accordance with Criterion 3 of 10 CFR 50.36(c)(2)(ii). The new demineralizer water isolation TS LCO has been constructed to be similar to STS LCOs and the staff has assessed it to be conservative and improved over STS and is, therefore, acceptable.

**AP600 TS "POWER DISTRIBUTION LIMITS"**

The AP600 power distribution limits LCOs correspond to those specified in STS and are acceptable to the staff. In addition, AP600 has added an LCO that addresses the use of its on-line power distribution monitoring system (OPDMS). This system continuously monitors power distribution parameters within the core via fixed incore detectors and has been included in the AP600 TS LCOs in accordance with Criterion 2 of 10 CFR 50.36(c)(2)(ii). The new OPDMS TS LCO has been constructed to be similar to STS LCOs and the staff has assessed it to be conservative and improved over STS and is, therefore, acceptable.

**AP600 TS "INSTRUMENTATION"**

The AP600 uses a digital instrumentation and control system. Instrumentation and controls for non-safety-related systems do not require technical specifications. Therefore, the instrumentation and controls system technical specifications required extensive modifications from STS. Four LCOs remain the same as STS: reactor trip system instrumentation, engineered safety features actuation system instrumentation, post accident monitoring system

instrumentation, and remote shutdown system instrumentation. Each of these LCOs has been extensively modified to account for the design differences of the AP600 together with the digital I&C systems. The STS LCOs for loss of power diesel generator start instrumentation and fuel building air cleaning system actuation instrumentation are not required because these are non-safety-related systems under the AP600 design. The LCO for containment purge and exhaust isolation instrumentation, control room emergency filtration system actuation, and boron dilution protection systems are not listed as separate LCOs. These functions are included in LCOs for the engineered safety features actuation system.

The AP600 TS LCOs associated with the instrumentation systems implement modified versions of the STS LCOs. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for instrumentation functions and assessed to be conservative or improved over STS. The staff agrees that where STS LCOs have not been included in AP600, it is justified by the AP600 design differences. The staff finds the AP600 instrumentation TS LCOs acceptable.

**AP600 TS "REACTOR COOLANT SYSTEM"**

The AP600 reactor coolant system LCOs correspond to those specified in STS with the exception of reactor coolant system (RCS) power-operated relief valves (PORVs) and loop isolation valves. TS LCO for RCS PORVs and loop isolation valves have not been included since they are not used in the AP600 design. Additional AP600 TS LCOs have been added in this area to address the automatic depressurization system (ADS). The ADS consists of four different stages of depressurization valves, which, when actuated, depressurizes the reactor coolant system to allow gravity injection of water from the in-containment refueling water storage tank (IRWST) or from the containment sump for long-term recirculation cooling. Also, AP600 TS LCOs have been added to specify minimum RCS flow to maintain uniform RCS mixing as an initial condition for boron dilution transients; maintain operability of the reactor vessel head vents to prevent overfilling of the pressurizer in some RCS addition transients; and maintain operability of the CVS isolation valves to prevent overfilling of the steam generators in some steam generator tube rupture accidents. These additional TS LCOs have been included for AP600 TS LCOs in accordance with criterion 3 of 10 CFR 50.36(c)(2)(ii).

The AP600 TS LCO in the area of RCS operational leakage limitations has been modified based on reduction in allowable unidentified leakage to 0.5 gpm (from the STS value of 1 gpm) to support leak-before-break assumptions. The RCS leakage detection instrumentation LCO has been modified to reflect AP600 design differences.

The AP600 TS LCOs associated with the reactor coolant system implement modified versions of the STS LCOs. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for the reactor coolant system functions and assessed to be conservative or improved over STS. The staff agrees that where STS LCOs have not been included in AP600, it is justified by the AP600 design differences. The staff finds the AP600 reactor coolant system TS LCOs acceptable.

**AP600 TS " PASSIVE CORE COOLING SYSTEM"**
(Equivalent to STS Emergency Core Cooling System)

The AP600 uses passive core cooling systems (PXS) rather than the pump-driven, active emergency core cooling systems (ECCS) in existing plants. The safety-related PXS is designed to perform emergency core cooling and decay heat removal, reactor coolant emergency makeup and boration, and safety injection. The PXS is located inside the containment; it consists of the several subsystems and associated components including the passive residual heat removal heat exchanger system, core makeup tanks, in-containment refueling water storage tank, automatic depressurization system, and accumulators.

The passive residual heat removal system transfers decay heat to the IRWST via natural circulation from the RCS whenever forced circulation cooling of the RCS is not available via the steam generators.

Core makeup tanks supply high pressure safety injection cooling and boration to the reactor via natural circulation and gravity injection and are designed to inject at any RCS pressure since the tanks are connected and maintained within the RCS pressure boundary.

The accumulators perform the same function for the AP600 as for current Westinghouse PWRs and the TS LCOs are the same as STS.

The IRWST provides low-head safety injection cooling and boration via gravity injection after the RCS has been depressurized via the ADS system or from the RCS break. Operability of the IRWST includes the containment sump recirculation flow paths to support long-term cooling of the core.

The AP600 uses canned rotor pumps which eliminates shaft seals and the possibility of an associated shaft seal failure LOCA. Consequently, the STS seal injection flow TS LCO is not required for AP600.

The AP600 TS LCOs associated with the passive core cooling system implement modified versions of the STS LCOs for ECCS. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for the ECCS functions and assessed to be conservative or improved over STS. The staff agrees that where STS LCOs have not been included in AP600, it is justified by the AP600 design differences. The staff finds the AP600 passive core cooling system TS LCOs acceptable.

**AP600 TS "CONTAINMENT SYSTEMS"**

The passive containment cooling system (PCS) provides the containment safety-grade ultimate heat sink to prevent the containment shell from exceeding its design pressure of 45 psig (310 kPa). The PCS uses natural air circulation past the containment shell enhanced by distribution of cooling water onto the containment shell. The water is gravity fed from a 531,000 gallon (1930 $m^3$) annular tank designed into the roof on the containment shield building. This tank has sufficient water to provide at least three days of cooling. New TS LCOs were developed for the PCS that were modeled after STS containment cooling LCOs.

A new technical specification was developed for the passive autocatalytic recombiners for design basis hydrogen control and for the pH adjustment of the sump water for controlling release of radionuclides from water in the containment following a LOCA with fuel damage.

No containment spray LCO is specified for the AP600 since the AP600 containment spray is not credited for mitigating any design-basis accident (DBA) analysis.

The AP600 TS LCOs associated with the containment systems implement modified versions of the STS LCOs for containment systems. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for containment cooling and isolation functions and assessed to be conservative or improved over STS. The staff agrees that where STS LCOs have not been included in AP600, it is justified by the AP600 design differences. The staff finds the AP600 containment system TS LCOs acceptable.

**AP600 TS "PLANT SYSTEMS"**

The AP600 uses a startup feedwater system, a non-safety-related system, to perform the function that the safety-related auxiliary feedwater system performs for an operating PWR. The safety-related decay heat removal system for the AP600 is provided by the passive residual heat removal system. Consequently, STS LCOs for the auxiliary feedwater system and condensate storage tank are not required. The AP600 applies the leak-before-break technology to the main steamline and the primary coolant system, while existing PWRs apply this technology only to the primary coolant system. New technical specifications are provided for these differences.

In addition, a new technical specification was provided for the main control room habitability system which provides safety related control room ventilation and radiation protection. Also, a technical specification was also added to require availability of a spent fuel pool makeup water source under certain spent fuel pool decay heat loads.

The AP600 TS LCOs associated with plant systems implement modified versions of the STS LCOs for plant systems. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for plant systems and assessed to be conservative or improved over STS. The staff agrees that where STS LCOs have not been included in AP600, it is justified by the AP600 design differences. The staff finds the AP600 plant system TS LCOs acceptable.

**AP600 TS "ELECTRICAL POWER SYSTEMS"**

The AP600 does not rely on ac power to mitigate design-basis accidents or attain safe shutdown (except for instrumentation and control which is ultimately powered from the dc system). Therefore, the STS for ac sources-operating; ac sources-shutdown; and diesel fuel oil, lube oil, and starting air are not required.

The staff finds the remaining technical specifications acceptable in the electrical area noting the following modification. The completion time for one dc subsystem inoperable was extended from two hours to six hours on the basis of the continued capability of the AP600 design to

reach safe-shutdown and mitigate all DBAs with the capacity of the remaining dc subsystems. A two-hour completion time was added for two dc subsystems inoperable to permit limited time to assess and restore an inoperable dc subsystem on the basis of the AP600 design to still reach safe-shutdown with two subsystems inoperable and the ability to mitigate most DBAs . Other technical specifications on inverters, distribution subsystems, and battery cell parameters are either consistent with STS or have only minor acceptable variations.

The AP600 TS LCOs associated with the electrical power system implement modified versions of the STS LCOs for the dc electrical power systems. The staff finds that they have been constructed to be essentially equivalent to the STS LCOs for electrical power system functions and assessed to be comparable to STS. The staff agrees that where STS LCOs have not been included in AP600 in the area of ac power systems, it is justified by the AP600 design differences. The staff finds the AP600 electrical power system TS LCOs acceptable.

**AP600 TS "REFUELING OPERATIONS"**

The AP600 TS LCOs for refueling operations are comparable to STS LCOs with the exception of requiring LCOs on the active residual heat removal system (RNS). The AP600 safety-related method of removing decay heat while in a refueling mode is via feed-and-bleed from the IRWST if water remains available in the IRWST or from refueling cavity boiling if the refueling canal is full and upper internals are removed. Th active RNS does not meet the inclusion criterion of 10 CFR 50.36(c)(2)(ii).

**AP600 Shutdown Operations**

Westinghouse proposed new technical specifications to control the availability of portions of the PXS, PCS, containment closure, and related systems during shutdown operations (Modes 5 and 6). These new technical specifications were proposed by Westinghouse to maintain the capability of passively cooling the core and maintaining cooling water inventory inside the containment following loss of the normal residual heat removal system during shutdown operations. If the RCS boundary is closed, the passive residual heat removal system will eventually be able to remove core decay heat following heatup of the RCS. If the RCS is open, the loss of residual heat removal results in steam being released to the containment. Core cooling can be maintained via a feed-and-bleed-type injection from the IRWST and eventually long term containment sump recirculation if necessary. In either case (RCS open or closed), as long as the containment is closed, and sufficient cooling is provided through the containment shell to condense the steam, the condensate will eventually drain back to the reactor coolant system, providing long term decay heat removal. Technical specifications for the ADS, PRHR, PCS, and containment penetrations, provide assurance that portions of these systems and components will be maintained for shutdown conditions.

In addition, a number of I&C engineered safety features actuation system signals have been added to ensure ability to actuate the systems during Modes 5 and 6.

The AP600 TS LCOs associated with shutdown operations do not have equivalent STS LCO versions. The staff finds that the shutdown operation TS LCOs have been constructed to be essentially equivalent to the STS LCO format and assessed to be conservative or improved over STS. Consequently, the staff finds the AP600 shutdown operation TS LCOs acceptable.

**AP600 TS "DESIGN FEATURES"**

The AP600 design features correspond to those specified in STS and are acceptable to the staff.

**AP600 TS "ADMINISTRATIVE CONTROLS"**

The AP600 administrative controls correspond to those specified in STS and are acceptable to the staff.

**DSER Open Item Resolution**

DSER Open Item 16.1-1 stated that the staff was reviewing Section 4.0 of the TS for consistency with recent industry proposals. Westinghouse has made the AP600 TS consistent with STS and therefore, DSER Open Item 16.1-1 is closed. DSER Open Item 16.1-2 stated that the staff was evaluating Section 5.0 of the TS to determine if Westinghouse should provide information on administrative controls for design certification. The staff has determined that Section 5.0 of the AP600 TS is consistent with STS, and DSER Open Item 16.1-2 is therefore closed.

As noted in SECY-93-190, and as stated in NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," dated September 1993, the results from shutdown and low-power evaluations should be incorporated into the reviews for advance light-water reactors. For DSER Open Item 16.1-3, the staff had not yet determined whether the current LCO during shutdown conditions were adequate, or whether additional requirements were needed. Based on staff and Westinghouse assessment of shutdown operations and risks, as evaluated in Section 19.3 of this report, the staff is now satisfied that the AP600 shutdown technical specification are acceptable, and DSER Open Item 16.1-3 is closed.

During the DSER review, Westinghouse proposed a significant revision to LCO 3.0.3, which did not require the RCS temperature to be reduced below 200 °F (93.3 °C). The acceptability of this change was DSER Open Item 16.1-4. Westinghouse subsequently reinstated LCO 3.0.3 to be consistent with STS. Therefore, DSER Open Item 16.1-4 is closed.

The DSER stated that the AP600 TS are to be formatted in accordance with NUREG-1431. The formatting should include correction of the footers and headers. This was DSER Open Item 16.1-5. Westinghouse has reformatted its TS to be consistent with NUREG-1431, and DSER Open Item 16.1-5 is closed.

The DSER stated that the AP600 TS and their bases should be separated in accordance with NUREG-1431. This was identified as DSER Open Item 16.1-6. Westinghouse has separated the TS and their bases in accordance with NUREG-1431, and therefore, DSER Open Item 16.1-6 is closed.

For the DSER, the staff had not yet completed its review of Westinghouse's responses to questions related to the TS. This was identified as DSER Open Item 16.1-7. Westinghouse has incorporated the resolution of staff comments into the AP600 TS, modeled the AP600 TS to

conform with STS to the maximum extent possible, and verified that the TS complies with 10 CFR 50.36(c)(2)(ii). On the basis of the staff's review, as documented above, the staff finds that Westinghouse has acceptably responded to all TS questions, and DSER Open Item 16.1-7 is closed.

During the staff's review of AP600 TS for the DSER, Westinghouse had identified certain AP600 TS based on the Utility Requirements Document (URD). The staff consideration of the URD references in its review was identified as DSER Open Item 16.1-8. The current AP600 TS are based on 10 CFR 50.36 and NUREG-1431 and are not based on the URD. Therefore, DSER Open Item 16.1-8 is closed.

There are cases where detailed design information, equipment selection, allowable values, or other information is required to establish the information to be included in the TS. Locations for this information are indicated by brackets indicating that the COL applicant needs to provide the plant-specific values or alternative text. This is COL Action Item 16.2-1.

16.3 Conclusion

Based on its review of the AP600 technical specifications, as discussed above, the staff concludes that the AP600 technical specifications are consistent with the regulatory guidance contained in the Westinghouse STS (NUREG-1431) and contain design specific parameters and additional technical specification requirements considered appropriate by the staff. The staff concludes that the AP600 technical specifications comply with 10 CFR 50.34 and 10 CFR 50.36 and are acceptable.

Revision 22 of the AP600 SSAR provided an extensive update to the technical specification in SSAR Chapter 16. The technical specification had last been updated in Revision 16 of the SSAR and a number of commitments had been made by Westinghouse in the interim involving resolution of open items. In the process of completing its review of the updated technical specifications, the staff had a general concern about a number of inconsistencies. These concerns were documented in a letter to Westinghouse on April 9, 1998.

On April 16, 1998, the staff and Westinghouse met to discuss the concerns identified in the staff's April 9, 1998 letter. During this meeting, the staff and Westinghouse reached agreement on wording changes that would resolve most of the concerns identified in the April 9, 1998 letter as documented in a meeting summary dated April 28, 1998. Although the staff believed that all the items discussed in the meeting summary were technically resolved, the staff could not close these items in its technical specification evaluation until a revision to the AP600 technical specifications to incorporate these changes was provided. In addition, Westinghouse stated during the meeting the SSAR Chapter 5 would be revised to document the basis for PRHR identified leakage and SSAR Chapter 7 would be revised to document the ESFAS logic for containment recirculation valve actuation in shutdown modes. Documentation of the changes committed to by Westinghouse related to the above discussion was FSER Confirmatory Item 16.3-1.

Revision 23 of the AP600 SSAR provided an update to the technical specifications (SSAR Chapter 16), which properly incorporated all the necessary changes discussed above. Revision 24 of the AP600 SSAR documents the basis for the PRHR identified leakage in SSAR

Chapter 5 and the revision to the containment recirculation valve ESFAS logic in SSAR Chapter 7. Therefore, FSER confirmatory Item 16.3-1 is closed.

As the result of a design assurance review of the AP600 TS, Westinghouse determined that the isolation function of the SG PORVs, PORV block valves, and SG blowdown isolation valves is relied upon to mitigate some DBA scenarios but not included in the AP600 TS. Consequently, the staff and Westinghouse agree that AP600 TS LCOs for these valves are required per 10 CFR 50.36(c)(2)(ii), Criterion 3. In a telephone conference with Westinghouse on April 23, 1998, Westinghouse agreed to add an AP600 TS LCO to cover the operability of these valves. The submittal of this TS LCO was FSER Confirmatory Item 16.3-2. Revision 23 of the AP600 SSAR properly added TS LCO 3.7.10, "Steam Generator Isolation Valves," to cover the operability requirements of the SG PORVs, PORV block valves, and SG blowdown isolation valves. Therefore, FSER Confirmatory Item 16.3-2 is closed.

During the April 16, 1998, meeting with Westinghouse on AP600 technical specifications, the staff and Westinghouse had extensive discussions on the AP600 technical specifications for containment closure during movement of irradiated fuel in containment and the auxiliary building ventilation technical specification for movement of irradiated fuel in the spent fuel pool. The Westinghouse AP600 design does not use safety-related ventilation systems. In addition, Westinghouse analyses of the radiological consequences of fuel handling accident are well within the dose acceptance criteria of 10 CFR 50.34. Westinghouse contended that, based on the first three technical specification inclusion criterion of 10 CFR 50.36, no technical specification LCOs are required for containment closure or for auxiliary building ventilation while moving irradiated fuel. The staff took the position that, although the analyzed dose from a fuel handling accident may not exceed the dose acceptance criteria, the principle of defense-in-depth makes it prudent to establish some type of containment barrier to a postulated release from a fuel handling accident. The staff noted to Westinghouse that operating plants have requested relaxation of fuel handling technical specifications to permit opening equipment hatches and personnel air locks while moving fuel. The staff has granted licensing changes to permit maintaining personnel air locks open as long as specific compensatory measures are taken to assure the staff that the personnel air locks could be closed quickly.

Westinghouse states that for the AP600, all the direct containment penetrations (including the equipment hatches) open to the radiologically controlled auxiliary building rather than directly to atmosphere. Westinghouse states that if the major equipment hatches were open, the AP600 design has roll doors in the auxiliary building mezzanine areas which could, in conjunction with an operating containment air filtration system, function as an alternate barrier, equivalent, from a defense-in-depth perspective, to an equipment hatch on containment with four bolts in place.

Upon further consideration of the AP600 design and the low radiological consequences of a fuel handling accident, the staff agreed that the use of an alternate barrier and the establishment of an operating filtered ventilation system when moving irradiated fuel within the containment represents an equivalent defense-in-depth concept for containment. The staff suggested, however, that additional changes be made to the current technical specifications included in the AP600 TS. Final wording, agreeable to all the NRC technical staff, for a containment closure technical specification applicable to the AP600 design, was not reached during the April 16, 1998, meeting. In addition, the staff had requested that Westinghouse propose an equivalent defense-in-depth technical specification for the auxiliary building ventilation system for

movement of irradiated fuel in the spent fuel pool. Westinghouse did provide such a TS for the AP600 and the staff discussed how the current spent fuel pool fuel handling technical specification for the AP600 could be made acceptable to the staff. However, no definitive agreement between the staff and Westinghouse could be reached on this issue during the meeting. This was FSER Open Item 16.3-1.

Revision 23 of the AP600 SSAR provided the staff revised TSs 3.9.5 and 3.9.6, the AP600 technical specification LCOs for containment penetrations and the spent fuel pool area ventilation during movement of irradiated fuel, which were acceptable to the staff. Therefore, FSER Open Item 16.3-1 is closed.

# 17 QUALITY ASSURANCE

## 17.1 Quality Assurance During the Design and Construction Phase

The combined license (COL) design and construction phase quality assurance (QA) program is beyond the scope of Westinghouse's application for final design approval and certification of the AP600 design. In the response to RAI 260.17 dated February 2, 1994, Westinghouse stated that the QA requirements for construction are the responsibility of the COL applicant. When completing the detailed design during the COL design phase, the COL applicant is required to submit its design phase QA program for staff review. This will be in addition to the staff review of the COL applicant's QA program for construction of the facility. This was identified as draft safety evaluation report (DSER) Open Item 17.1.3-2 and COL Action Item 17.1.3-1.

In Section 17.5 of the standard safety analysis report (SSAR), "Combined License Information Items," Westinghouse states that the COL applicant will address its QA program for the design phase, as well as its QA program for procurement, fabrication, installation, construction and testing of structures, systems and components in the facility. The COL applicant's QA program will also include provisions for seismic Category II structures, systems, and components (SSCs) consistent with Regulatory Guide (RG) 1.29, "Seismic Design Classification," Revision 3, or the latest revision. The staff finds the information in Section 17.5 of the SSAR regarding the QA program to be acceptable, and therefore, DSER Open Item 17.1.3-2 is closed.

The submittal of the COL applicant's design and construction phase QA program for NRC staff review, previously identified as COL Action Item 17.1.3-1, is redesignated as COL Action Item 17.1-1. Accordingly, COL Action Item 17.1.3-1 is dropped.

## 17.2 Quality Assurance During the Operations Phase

In Appendix 1A of the SSAR, Westinghouse states that the QA program for operations is beyond the scope of Westinghouse's standard design approval and design certification of the AP600 design. In Section 17.5 of the SSAR, "Combined License Information Items," Westinghouse states that the COL applicant will also address its QA program for operations. This is COL Action Item 17.2-1.

## 17.3 Quality Assurance During the Design Phase

### 17.3.1 General

In Chapter 17 of the SSAR, Westinghouse describes the QA program for the design phase of the AP600. The QA program references Westinghouse topical report WCAP-8370/7800, "Energy Systems Business Unit - Nuclear Fuel Business Unit Quality Assurance Plan," Revision 11A/7A, for work performed before November 30, 1992, and WCAP-8370/7800, redesignated as WCAP-8370, "Energy System Business Unit-Power Generation Business Unit Quality Assurance Plan," Revision 12A, dated April 1992, for work performed after

November 30, 1992. The staff previously reviewed these programs and found them acceptable, as documented in the April 23, 1992, letter from Gary Zech, NRC, to Nicholas Liparulo, Westinghouse.

In Revision 5 to Chapter 17 of the SSAR, Westinghouse stated that effective March 31, 1996, activities affecting the quality of items and services for the AP600 Project during design, procurement, fabrication, inspection, and/or testing would be performed in accordance with the quality plan described in Westinghouse's "Energy Systems Business Unit - Quality Management System," (QMS) Revision 1. The staff's review and approval of Revisions 1 and 2 to the Westinghouse QMS were documented in letters from Suzanne Black (NRC) to N. J. Liparulo (Westinghouse), dated February 23, 1996, and April 10, 1997, respectively.

WCAP-12600, "AP600 Quality Assurance Program Plan," Revision 4, dated January 26, 1998, a project-specific quality plan, supplements the topical report for the AP600 application. In the DSER, the staff requested a copy of an earlier version of this report. This was identified as DSER Open Item 17.1.1-1. In a letter dated January 20, 1998, Westinghouse provided a current, unbound version of this document, which was completed on January 16, 1998. The staff reviewed WCAP-12600, Revision 4, and found it to be consistent with Westinghouse's commitments to the applicable QA-related RGs in Appendix 1A to the SSAR for the design phase of the AP600, and also consistent with the Westinghouse QMS, which establishes Westinghouse's compliance with the requirements of 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants." The staff finds this acceptable, and therefore, DSER Open Item 17.1.1-1 is closed.

17.3.2 Organization

Since its initial SSAR submittal in 1992, the Westinghouse Electric Company, previously, Westinghouse Electric Corporation, has undergone several reorganizations. Currently, the New Plant Projects Division is responsible for all design certification and first-of-a-kind engineering (FOAKE) activities associated with the AP600, including control of technical interfaces among external contractors. The line organizations are responsible for establishing and implementing a QA program that meets the requirements of the QMS.

The New Plant Projects Division (formerly the Advanced Technology Business Area) established WCAP-12600, which provides requirements for the application of the QMS to the AP600 design certification and FOAKE programs and supplements the QMS in certain areas. The General Manager of the New Plant Projects Division is responsible for implementing the AP600 QA program. The Quality Systems Projects Manager is responsible for the establishment of WCAP-12600 and for ensuring its effective implementation. Compliance with quality requirements is measured through planned audit activities and self assessments. The Quality Systems Projects organization is independent of other organizations, and the Quality Systems Projects Manager has direct access to the General Manager, New Plant Projects Division, to ensure that appropriate action is taken to resolve all quality-related issues.

Under the direction of Westinghouse, a number of organizations provide design and engineering services in support of the AP600. The major contributors are as follows:

- Societá Progettazione Reattori Nucleari, SpA (SOPREN)/ANSALDO of Italy
- Avondale Industries, Inc.

- Badan Tenaga Atom Nasional (BATAN) of Indonesia
- Bechtel North American Power Corporation
- Burns & Roe Company
- Chicago Bridge and Iron Services, Inc. (CBI)
- ENSA
- Empresa Nacional de Ingeniería y TTecnologia, S.A. (INITEC) of Spain
- NNC
- Southern Company
- TECNATOM
- MK-Ferguson Company

Each of these suppliers is contractually required to establish, implement, and maintain a QA program that meets the requirements of ANSI/ASME NQA-1 "Quality Assurance Program Requirements for Nuclear Facilities" 1989 Edition through NQA-1b-1991 Addenda.

17.3.3 Quality Assurance Program

Through its QA Plan, QMS, Revision 2, Westinghouse adopted a QA program that meets Appendix B to 10 CFR Part 50. In addition, as described in the QMS, Westinghouse has committed to comply with ASME NQA-1-1983, "Quality Assurance Program for Nuclear Facilities," and the applicable RGs identified in Appendix 1A of the SSAR. The QMS is implemented for the AP600 design through the "AP600 Quality Assurance Program Plan," WCAP-12600, which describes those procedures, programs, and commitments applicable to the AP600 design.

WCAP-12600 applies to all safety-related items as described in Section 3.2 of the SSAR. Westinghouse is responsible for ensuring that suppliers establish, implement, and maintain a Westinghouse-approved QA program that meets the requirements of ANSI/ASME NQA-1, "Quality Assurance Program Requirements for Nuclear Facilities," 1989 Edition through NQA-1b-1991 Addenda.

The QA program establishes a system for design control. Procedures and instructions define the design process associated with design interfaces, design controls, identification of design inputs, preparation of design documents, design verification, and design changes. Interface controls include the assignment of responsibility and the use of procedures among participating design organizations. Westinghouse suppliers that perform quality-related AP600 design activities are required to work under the applicable Westinghouse procedures. Design verification with respect to safety-related items is performed using design reviews, alternative calculations, or qualification tests.

The procurement of items and services is controlled by procedures that describe the responsibilities and methods to ensure conformance with specified requirements contained in procurement documents. Suppliers are initially evaluated for the specified items and services to determine the acceptability of their QA programs. Quality Systems Projects reviews purchase requisitions, and suppliers of services are required to have a QA program consistent with the applicable requirements of the Westinghouse QA Plan.

Records that furnish evidence of quality are specified, prepared, and maintained in accordance with established procedures that identify applicable requirements and responsibilities. Each group that generates and collects QA records is responsible for maintaining a retrieval system for those records.

Quality Systems Projects is responsible for planning and performing internal and external audits in accordance with established procedures to verify compliance with the QA Plan. Audits are conducted in accordance with written procedures or checklists. Internal audits are conducted at least once a year, or at least once during the life of the activity, whichever is shorter. External audits are conducted every three years, or more frequently, as determined by the annual supplier performance evaluations. In addition, Westinghouse has a self-assessment process through which functional departments independently review and evaluate overall performance to determine the level of quality that is achieved and compliance to procedures. Westinghouse conducts audits of their suppliers, as provided for in NQA-1, to ensure that the suppliers' QA programs are effectively implemented.

In the DSER, the staff concluded that QA applied to non-safety-related systems identified as important to safety by the regulatory treatment of non-safety systems (RTNSS) process should be comparable to that described in Generic Letter (GL) 85-06 for anticipated transient without scram (ATWS), and Regulatory Position (RP) 3.5 and Appendix A of RG 1.155, for station blackout non-safety-related equipment. This issue was identified as DSER Open Item 17.1.3-1.

In Revision 17 to Chapter 17 of the SSAR, Westinghouse included Table 17-1, "Quality Assurance Program Requirements for RTNSS Systems, Structures, and Components," which outlines the QA program requirements for suppliers of systems, structures, or components to which the requirements for RTNSS apply. The staff finds that the QA requirements in Table 17-1 of the SSAR are comparable to that described in GL 85-06 for ATWS, and RP 3.5 and Appendix A of RG 1.155, for station blackout non-safety-related equipment and are, therefore, acceptable for RTNSS. The staff finds this acceptable, and therefore, DSER Open Item 17.1.3-1 is closed.

17.3.4 Quality Assurance Program For Design Certification Testing Activities

The NRC staff conducted several QA program implementation inspections of the major Westinghouse AP600 design certification testing facilities. The results of these inspections and the NRC's conclusions with respect to these programs are documented in Section 21.7, "Quality Assurance Inspections," of this report.

17.3.5 Quality Assurance Program Implementation

The NRC staff performed a QA design control implementation inspection at Westinghouse's Monroeville, PA offices during the week of November 17, 1997 (NRC Inspection Report 99900404/97-02). The purpose of the inspection was to determine if quality activities performed as part of the design of the AP600 advanced light-water reactor (ALWR) were conducted under the appropriate provisions of the Westinghouse 10 CFR Part 50, Appendix B, QA program of record in the AP600 SSAR (Westinghouse Electric Corporation - Energy Systems Business Unit, Quality Management System, Revision 1, approved by the NRC on February 23, 1996), and to review Westinghouse's corrective actions with respect to findings identified previously in several NRC inspection reports (see discussion below). The inspection

focused on design control activities governing the integrity of computer codes (NOTRUMP, WCOBRA/TRAC, and WGOTHIC), and associated calculation notes, that provide the bases for the SSAR Chapters 6 and 15 analyses.

During the inspection, the team reviewed Westinghouse's corrective and preventive actions with respect to the following Notices of Nonconformance (NONs) and Unresolved Items (URIs) documented in NRC Inspection Reports (IRs) 99900404/95-01, 99900404/95-02, and 99900404/97-01, respectively:

- NON 99900404/95-01-01, "Reactor Systems Design Certification Test Program"
- URI 99900404/95-01-02, "Reactor Systems Design Certification Test Program"
- NON 99900404/95-01-03, "Reactor Systems Design Certification Test Program"
- NON 99900404/95-02-01, "As-Built Drawings for VAPORE Test Facility"
- URI 99900404/95-02-02, "VAPORE Test Facility Calibration Records"
- NON 99900404/97-01-01, "Inadequate Corrective Action"
- NON 99900404/97-01-02, "Inadequate Quality and Technical Oversight of INITEC"
- URI 99900404/97-01-03, "Acceptability of AP600 Design Deliverables"

The inspection team confirmed that corrective and preventive actions associated with each NON and URI had been effectively completed and documented by Westinghouse. Accordingly, NRC IR 99900404/97-02 documents the bases for closure of these issues.

During the November 17, 1997, inspection, however, the NRC also determined that the implementation of the Westinghouse QA program for certain AP600 design certification activities failed to meet NRC requirements. Specifically, the inspection team identified numerous examples of inadequate QA program implementation with respect to design control of calculations which contained errors or unquantified discrepancies, not evaluated by Westinghouse. The team also identified examples of unquantified errors that were allowed to propagate in design calculations, inadequate documentation of design and analysis conclusions, and errors in both WGOTHIC and WCOBRA/TRAC computer codes which Westinghouse failed to evaluate in accordance with its quality assurance program and 10 CFR Part 21 requirements, as applicable. These issues were identified in NRC IR 99900404/97-02 as follows:

- NON 99900404/97-02-01, concerning inadequate design reviews of AP600 calculations, was identified and discussed in Sections 3.2, 3.3 and 3.4 of the IR

- NON 99900404/97-02-02, concerning failure to review and evaluate GOTHIC code errors, was identified and discussed in Section 3.4 of the IR

- URI 99900404/97-02-03, concerning WGOTHIC calculation deficiencies, was identified and discussed in Section 3.4 and 3.6 of the IR

As a result of these issues, the inspection team concluded in the IR that Westinghouse needs to evaluate the impact of these findings on the SSAR Chapter 15 analyses, and all other SSAR AP600 design information on the basis of the results obtained in the affected computer codes and associated calculation notes. In light of the number of discrepancies found by the NRC inspection team on such a small fraction of the total population of documents, Westinghouse

needs to establish, via a comprehensive evaluation and/or assessment, the adequacy of the AP600 QA design review process and the integrity of the AP600 design, particularly containment design. In addition, Westinghouse must demonstrate that the requirements of 10 CFR 50, Appendix B, 10 CFR Part 21, and the applicable design certification provisions of 10 CFR Part 52 are being satisfied. Therefore, the effectiveness of Westinghouse's implementation of the AP600 QA program with respect to design control of SSAR Chapters 6 and 15 analyses, and associated computer codes and calculation notes, remained indeterminate pending an acceptable response to NRC IR 99900404/97-02.

In its February 27, 1998 response to IR 99900404/97-02, Westinghouse described the steps it had taken to correct and prevent the recurrence of the issues identified. Additionally, as a result of concerns identified by the staff with regards to the effectiveness of Westinghouse's review of SSAR Chapters 6 and 15 design calculations, Westinghouse initiated a Design Assurance Review (DAR) to establish that such documentation meets the design verification and quality assurance requirements of Appendix B to 10 CFR Part 50.

In an April 3, 1998, letter to Westinghouse, the staff stated that it found Westinghouse's February 27, 1998, letter responsive to some of the issues identified in the IR. However, the staff had concerns with several of the Westinghouse's responses in that they did not adequately address either the specific issue(s) or the generic implications of the issues identified during the inspection. Furthermore, and subsequent to the inspection, the staff continued to identify Westinghouse-proposed changes to SSAR chapters which were not related to changes effected to resolve issues raised by the NRC. These new changes combined with the issues identified during the inspection caused the staff to question the effectiveness of Westinghouse's AP600 configuration control and design review processes. Consequently, the staff met with Westinghouse on April 13, 1998, to discuss Westinghouse's implementation of corrective actions, including the process governing the DAR and its results, as well as the AP600 design configuration control processes, and the efforts associated with the AP600 Technical Specifications self-assessment . The results of the DAR and other materials presented by Westinghouse during the April 13, 1998 meeting, were formally provided to the staff by Westinghouse via an April 17, 1998 letter.

As a result of an evaluation of the additional information provided by Westinghouse, the staff concluded (with the exception of two issues associated with URI 99900404/97-02-03 and proposed changes to SSAR Chapter 3) in an April 28, 1998 letter that Westinghouse had adequately addressed the staff's concerns relative to the potential generic implications of the issues identified in IR 99900404/97-02. Westinghouse provided its response to these remaining issues in a May 1, 1998 letter. Accordingly, on May 6, 1998, the staff concluded that Westinghouse had satisfactorily addressed all issues identified in IR 99900404/97-02.

17.3.6 Conclusion

On the basis of its inspections and evaluations of the QA program described in WCAP-12600, and by reference to the Westinghouse QMS, the staff concludes that (1) the AP600 QA description in Chapter 17 of the SSAR is consistent with the SRP, and when properly implemented, complies with the criteria of Appendix B to 10 CFR Part 50; and (2) Westinghouse has effectively implemented the WCAP-12600 provisions (and/or taken appropriate corrective measures) during the design phase.

## 17.4 Reliability Assurance Program During the Design Phase

### Introduction

In Section 17.4 of the SSAR, Westinghouse describes the reliability assurance program (RAP) for the design phase of the AP600 design. Westinghouse performed the design RAP (D-RAP) for its scope of design during the detailed design and specific equipment selection phases to ensure that important AP600 reliability assumptions of the probabilistic risk assessment (PRA) will be considered throughout plant life. The D-RAP will identify relevant aspects of plant operation, maintenance, and performance monitoring of important SSCs for the COL applicant's consideration in ensuring safety of equipment, preventing loss of critical function, and limiting risk to the public. A COL applicant referencing the AP600 design will complete the D-RAP for its scope of design and equipment selection. Additionally, the COL applicant will develop and implement an operational reliability assurance process (O-RAP) for risk-significant SSCs. The O-RAP monitors equipment performance and evaluates equipment reliability to provide reasonable assurance that the plant is operated and maintained commensurate with PRA assumptions so that the overall safety is not unknowingly degraded and remains within acceptable limits (see COL action item in Section 17.4.9 in this report). When SSC monitoring and evaluation identifies performance or condition problems, appropriate corrective action will be taken to ensure the SSC remains capable of performing its intended functions. However, the RAP does not attempt to statistically verify the numeric values used in the PRA through performance monitoring.

Westinghouse's initial submittal of its RAP plan was submitted in Revision 0 to Section 16.2 of the SSAR, dated June 26, 1992. The staff evaluated that submittal and responded by providing RAIs dated October 14, 1992. Westinghouse discussed the RAIs with the staff and revised the RAP in Revision 1 to the SSAR, dated January 13, 1994. The staff reviewed Section 16.2, Revision 1, and identified thirteen DSER open items that needed to be addressed by Westinghouse before the staff could complete its final safety evaluation report (FSER). Westinghouse submitted changes to address most of the open items in Revisions 10 and 14 to Section 16.2 of the SSAR. In Revision 19 to the SSAR, dated December 31, 1997, Westinghouse relocated Section 16.2 to Section 17.4 of the SSAR. In Revision 22 to the SSAR dated April 6, 1998, Westinghouse relocated Section 17.4.8 regarding COL activities for O-RAP to Section 17.5 of the SSAR and renumbered parts of Section 17.4 of the SSAR. In Revision 22 to SSAR Section 17.4, the staff found that Westinghouse addressed all thirteen DSER open items in accordance with SECY-95-132 "Policy and Technical Issues Associated With the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," dated May 22, 1995, and the Standard Review Plan Section 17.4, RAP; dated January, 1996; therefore, the staff determined that the AP600 RAP plan is acceptable.

### Background

The NRC identified the need for a safety-oriented reliability effort for the nuclear industry in Section II.C.4 of NUREG-0660, "NRC Action Plan Developed as a Result of the TMI-2 [Three Mile Island Unit 2] Accident," dated August 1980. Initial NRC research in the area of reliability assurance began in the early 1980s. The results of this research showed that an operational reliability program, based on a feedback process of monitoring performance, identifying problems, taking corrective actions, and verifying effectiveness of the actions, was needed and

that other NRC initiatives (e.g., maintenance inspection, performance indicators, aging programs, and technical specification improvement) would address this need. The overall conclusion of this research was that an operational reliability program could be implemented most effectively by performance-based, nonprescriptive regulation, where the NRC mandates the level of safety performance to be achieved. For example, licensees could be required to set availability and reliability criteria for selected systems and to measure performance compared to the criteria.

The TMI task was closed out in October 1988 without further action because several NRC initiatives effectively subsumed the operational reliability program effort. The initiatives that formed the basis for closing out this TMI task included efforts to (1) improve maintenance and better manage the effects of aging, (2) improve technical specifications, (3) develop and use plant performance indicators, and (4) develop an operational reliability program as an acceptable means of meeting the station blackout rule (10 CFR 50.63).

In NUREG-1070, "NRC Policy on Future Reactor Designs," dated 1985, the staff recommends the use of a systems reliability program to ensure that the reliability of components and systems important to safety would remain at a sufficient level. To ensure that reliability objectives are met and to prevent degradation of reliability during operation, it was envisioned that the PRA performed at the design stage would be used as a tool in making detailed design decisions affecting procurement, testing, and the formulation of operations and maintenance procedures.

In a few specific instances, the NRC studied or established reliability targets for systems and components. For example, in draft standard review plan (SRP) Section 10.4.9, "Auxiliary Feedwater System," the staff states that an acceptable auxiliary feedwater system design has an unreliability in the range of 1.0E-4 to 1.0E-5 per demand. Generic Issue B-56, "Diesel Reliability," involved efforts to determine, monitor, and maintain emergency diesel generator reliability levels. Additional regulatory bases for key elements of a RAP can be found in 10 CFR Part 50, Appendix A, and 10 CFR 50.65.

In SECY-89-13, "Design Requirements Related to the Evolutionary Advanced Light Water Reactors," dated January 19, 1989, the staff identified several issues for ALWRs that may exceed the present acceptance criteria defined in the draft SRP. The RAP, as discussed in SECY-89-13, involved the need for a program to ensure that the design reliability of safety-significant SSCs is maintained over the life of a plant. In SECY-89-13, the staff informed the Commission that a RAP would be required for ALWR final design approval/ design certification (FDA/DC). In November 1989, potential applicants for FDA/DC were informed by letter that "the NRC staff was considering matters that went beyond the current Standard Review Plan...that [the NRC] expects these advanced reactor designs to embody." Reliability assurance was identified as one of these matters.

The staff's interim position on RAP was further developed as described in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993. The staff's final position on RAP was presented in SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems," dated March 28, 1994. This policy is subject to implementation of the D-RAP using the inspections, tests, analyses, and acceptance criteria (ITAAC) process, disapproved program requirements for an operational reliability assurance program (O-RAP) and directed the staff to incorporate the objectives of O-RAP into existing regulatory programs

(e.g., maintenance, quality assurance). In the staff requirements memorandum (SRM) dated June 30, 1994, associated with SECY-94-084, the Commission approved an applicable policy for the D-RAP approach.

In SECY-94-084, the staff states that D-RAP is required for design certification, the COL application, and the COL applicant. The SSAR should include the details of the D-RAP, including the conceptual framework, program structure, and essential elements. The SSAR should also include the following items:

- identify, prioritize, and list the risk-significant SSCs based on the design certification PRA, deterministic methods, such as, but not limited to, nuclear plant operating experience and relevant component failure databases

- ensure that the design certification applicant's design organization determines that significant design assumptions, such as equipment reliability and unavailability, are realistic and achievable

- include design assumption information for the equipment procurement process

- provide these design assumptions to the COL for consideration in the O-RAP

The staff's review of the design certification D-RAP is addressed in this section of the FSER. The COL applicant's D-RAP must be approved by the staff prior to granting a COL with all subsequent changes subject to NRC staff approval prior to implementation, which is similar to current QA Programs. The COL applicant's D-RAP should incorporate all aspects of reliability assurance that will be accomplished prior to fuel load (i.e., procurement, fabrication, construction, and preoperational testing phases). The COL applicant's D-RAP will be verified by an ITAAC. The NRC staff will inspect and audit the implementation of the operational reliability assurance process for the duration of the license using maintenance and QA regulations (i.e., 10 CFR 50.65 and Appendix B to 10 CFR 50, respectively).

In SECY-95-132, "Policy and Technical Issues Associated With the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," dated May 22, 1995, the staff modified its approach to the RAP plan in accordance with the guidance provided in the SRM dated June 30, 1994. The staff retained and the Commission approved the two-stage approach. The first stage (D-RAP) would apply before the initial fuel load. The second stage would apply to reliability assurance activities for the operations phase of the plant life cycle. Operational reliability assurance activities would be integrated into existing programs (e.g., maintenance, surveillance testing, inservice inspection, inservice testing, and quality assurance). Since the objectives of O-RAP are incorporated into existing regulatory programs, the staff now refers to O-RAP as either an operational reliability assurance process (O-RAP) or as operational reliability assurance activities. The Commission approved the staff's proposal. In addition, the staff completed draft SRP Section 17.4, "RAP," dated January, 1996, to provide review guidance on acceptable RAP plans for NRC technical reviewers. The staff's evaluation of the Westinghouse AP600 RAP is based on the staff position in SECY-95-132 and Section 17.4 of the draft SRP.

Any SSCs identified as risk-significant in the D-RAP, by a combination of probabilistic and deterministic methods would require performance monitoring under the O-RAP. The reliability performance monitoring of risk-significant SSCs under O-RAP would be the same as that required by the maintenance rule (10 CFR 50.65). The performance measures or goals established and used with the reliability performance monitoring should provide a means to identify problems and equipment degradation prior to failure. Root cause analyses in the O-RAP would be required for risk-significant SSCs that experience problems or failures. Also, corrective actions taken in response to failures or problems and the results of those corrective actions would be monitored as part of the O-RAP.

17.4.1 General

In Section 17.4.1 of the SSAR, Westinghouse states that the AP600 RAP is a program which is implemented as an integral part of the AP600 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP600 PRA will remain valid throughout plant life. The PRA quantifies plant response to a spectrum of postulated initiating events in order to demonstrate the low probability of core damage and resultant risk to the public. PRA input includes specific values for the reliability of the various SSCs in the plant that are used to respond to postulated initiating events.

In Section 17.4.1 of the SSAR, Westinghouse also describes that the RAP is implemented in two major phases: D-RAP and O-RAP. The D-RAP, which is implemented during the design phase, defines the overall structure of the AP600 RAP, implements those aspects of the program which are applicable to the design process, and generates information applicable to the O-RAP. The D-RAP is implemented in three phases. The D-RAP Phase III and O-RAP are implemented by the COL applicant. The O-RAP provides confidence that operations and maintenance activities, performed in the operating plant, support and maintain the reliability assumptions made in the plant PRA.

The NRC position on RAP as specified by SECY-94-084, as modified by the SRM dated June 30, 1994, and as stated above was not adequately addressed in Revision 1 to Section 16.2.1 of the SSAR. In the DSER, the staff concluded that Westinghouse needed to modify Section 16.2 to reflect the NRC position on RAP and, specifically, to revise Section 16.2.1 to include deterministic and other methods with the probabilistic method (i.e., PRA) currently described in Section 16.2.1 for determining risk-significance. This was identified as DSER Open Item 16.2.1-1. This item also applied throughout Section 16.2, primarily to Sections 16.2.1.2, "Relationship to Other Administrative Programs," 16.2.3.4, "Information Available to Combined License Applicant," and 16.2.4, "Combined License Applicant RAP (O-RAP)." The staff also found that the SSAR needed to identify that the COL applicant will be responsible for augmenting and completing the remainder of the D-RAP to include any site-specific design information and identify and prioritize the risk-significant SSCs as required by the D-RAP. This was identified as DSER Open Item 16.2.1-2.

In Section 17.4.1 of SSAR, Westinghouse added the following to address DSER Open Items 16.2.1-1 and 16.2.1-2:

> The D-RAP, as shown in Figure 17.4-1, is implemented in three phases. The first phase, the Design Certification phase, defines the overall structure of the AP600 D-RAP, and implements those aspects of the program which are

applicable to the design process. During this phase, risk-significant SSCs are identified for inclusion in the program using probabilistic, deterministic, and other methods. Phase II, the post-design certification process, develops component maintenance recommendations for the plant's operations and maintenance activities for the identified SSCs. The third phase is the site-specific phase, which introduces the plant site-specific SSCs to the D-RAP process. Phases I and II are performed by the designer. Phase III is responsibility of the Combined License applicant.

Finally, Figure 17.4-1 shows the Operational Reliability Assurance Process (O-RAP). This phase, which is implemented by the Combine License applicant, provides confidence that the operations and maintenance activities performed by the operating plant support should maintain the reliability assumptions in the PRA.

The staff finds the above revisions in accordance with draft SRP 17.4, RAP, dated January, 1996, and therefore, SSAR Section 17.4.1 is acceptable and DSER Open Items 16.2.1-1 and 16.2.1-2 are closed. The NRC needs to review and approve the Phase III portion of D-RAP implementation for the COL applicant. This is COL Action Item 17.4.1-1.

17.4.2 Scope

In Revision 0 to Section 16.2.1.1 of the SSAR, "Scope," Westinghouse stated that both phases (design and operation) of the RAP include the safety-related SSCs which are identified as risk significant in the AP600 PRA, and several non-safety-related systems that provided defense-in-depth or that are used in the PRA evaluation to provide credit for event mitigation. In Table 16.2-1 of the SSAR (Revision 0), Westinghouse provided a list of the non-safety-related systems that support the defense in depth capability. Westinghouse further stated that the AP600 RAP begins during the design phase (D-RAP) and continues throughout plant operations (O-RAP).

RAI 630.1a, 630.1b, and 630.1c regarding the scope of the RAP described in Revision 0 to Section 16.2.1.1 of the SSAR, was submitted to Westinghouse in a letter dated October 14, 1992. The questions included the following:

- The staff's position is that RAP provides a commitment to include all risk-significant SSCs throughout plant life, using PRA and other industry sources to identify and prioritize SSCs that are important to risk. Limiting the RAP to SSCs that are identified in the AP600 is too narrow a scope for the RAP. Other industry sources should be used and considered. (RAI 630.1a)

- It appears that the term "risk-significant SSCs" and "safety-related and important non-safety-related systems that provide defense-in-depth or that are used in the PRA evaluation to provide credit for event mitigation," are used interchangeably. Consistent use of "risk-significant SSCs" is preferred by the staff. (RAI 630.1b)

- The scope should be consistent with the 10 CFR 50.65 (the maintenance rule). Section 1.2.1.1 of the SSAR should be revised to state that the scope of the RAP should be consistent with that of 10 CFR 50.65. (RAI 630.1c)

Westinghouse responded to these RAIs by a letter dated February 9, 1993, and by subsequently revising Section 16.2.1.1 of the SSAR. Neither the Westinghouse RAI response nor Revision 1 to the SSAR resolved RAIs 630.1a, 630.1b, and 630.1c. These were identified as DSER Open Items 16.2.1.1-1, 16.2.1.1-2, and 16.2.1.1-3, respectively. DSER Open Item 16.2.1.1-2 also applied in Sections 16.2.1.2, "Relationship to Other Administrative Programs," 16.2.2, "Objective," 16.2.3.2, "SSCs Identification and Prioritization," and 16.2.3.4, "Information Available to Combined License Applicant."

In addition, the staff determined that in Revision 1 to Section 16.2.6, "Reference," that Reference 2 (i.e., WCAP 13856, "AP600 Implementation of the Regulatory Treatment of Non Safety-Related Systems Process") did not provide an appropriate method for determining risk-significant SSCs for RAP. This was identified as DSER Open Item 16.2.1.1-4. This open item also applied to Section 16.2.3.2, "SSCs Identification and Prioritization."

Westinghouse modified Section 17.4.2, "Scope," to state that the D-RAP includes a design evaluation of the AP600 and identifies the aspects of plant operation, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PRA, deterministic tools, industry sources and expert opinion are utilized to identify and prioritize those risk-significant SSCs.

The staff determined that Westinghouse used several sources of information to determine risk-significant SSCs that should be under the scope of RAP. These changes adequately addressed DSER Open Items 16.2.1.1-1, 16.2.1.1-2, and 16.2.1.1-4. The staff also determined that these open items are adequately addressed in other applicable Section 17.4 subsections. The staff finds this acceptable, and therefore, DSER Open Items 16.2.1.1-1, 16.2.1.1-2, and 16.2.1.1-4 are closed.

With respect to DSER Open Item 16.2.1.1-3, the staff clarified its position on methods used to identify SSCs under the scope of RAP for the AP600 design in a meeting with Westinghouse on November 25, 1996. The staff informed Westinghouse that the methods used to identify SSCs under the scope of RAP should be consistent with the risk determination methods used to identify SSCs under the scope of RAP for an existing ALWR certified design RAP and consistent with industry guidance to implement the maintenance rule, NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."

Westinghouse modified Section 17.4.7.1 of the SSAR, "SSCs Identification and Prioritization," so that D-RAP includes importance measure threshold values consistent with the risk determination methods described in two existing ALWR certified design RAPs and consistent with industry guidance to implement the maintenance rule. The staff finds this acceptable, and therefore, DSER Open Item 16.2.1.1-3 is closed. See Section 17.4.7.1, "SSCs Identification and Prioritization," of this report for more details on this issue. The staff also finds that SSAR Section 17.4.2, "Scope," is in accordance with the review guidance in draft SRP Section 17.4, RAP, and therefore, is acceptable.

In addition, the COL applicant is required to use PRA importance measures, the expert panel process and other deterministic methods to determine the final list of risk-significant SSCs under the scope of RAP. This process is subject to NRC review and approval before a COL is issued. This is COL Action Item 17.4.2-1.

17.4.3 Design Considerations

In Revision 0 to Section 16.2.3.3, "Design Considerations," Westinghouse stated that extensive efforts are involved in optimizing the AP600 design for operational availability, as well as safety. The use of consistent reliability information provides confidence that the calculated system availabilities are based on the same data and assumptions as the PRA evaluation. Whenever an alternative is proposed to improve performance in either area, the revised design is first reviewed to provide confidence that the current assumptions in the other areas are not violated.

As part of the design process, risk-significant components are evaluated to determine their dominant failure modes. For most components, a substantial operating history is available that defines the significant failure modes and their likely causes.

The identification and prioritization of the various possible failure modes for each component leads to suggestions for failure prevention or mitigation. This information is provided as input to the O-RAP because it defines the means by which component reliability can be maintained.

The final design approved for construction reflects the reliability requirements assumed in the design and PRA as part of their procurement specifications.

In RAI 630.4 dated October 14, 1992, the staff stated that although extensive efforts are involved in optimizing the AP600 design for operational availability as well as safety, these objectives may, at times, be conflicting (e.g., operational availability goals in conflict with the plant safety goals). The staff's position is that it should be clearly stated that the safety goals take priority over other goals whenever a potential conflict exist. The staff requested that Westinghouse revise Section 16.2.3.3 of the SSAR to explicitly state the plant safety goals take priority over other goals.

In the response to RAI 630.4 dated February 9, 1993, and subsequently in Revision 1 to Section 16.2.3.3 of the SSAR, Westinghouse added to the first paragraph of Section 16.2.3.3 that whenever a potential conflict exists between safety goals and other goals, these conflicts are resolved without jeopardizing the protection of the health and safety of the public. The staff found the revision acceptable. However, this information was removed from the SSAR in a later revision. As requested by the staff, in Revision 22 to Section 17.4.3, "Design Certification,' Westinghouse returned the information to the SSAR to include that safety goals take precedence over other goals. The staff finds this acceptable and RAI 630.4 is closed. In addition, the staff finds that SSAR Section 17.4.3, "Design Considerations," is in accordance with the review guidance in Section 17.4, "Reliability Assurance Program," of the NRC's draft Standard Review Plan (SRP) and, therefore, is acceptable.

17.4.4 Relationship to Other Administrative Programs

In Revision 1 to Section 16.2.1.2, "Relationship to Other Administrative Programs," Westinghouse stated that the RAP manifests itself in other administrative and operational programs in the AP600. The technical specifications provide surveillance and testing frequencies for certain safety-related equipment which provide confidence that their reliability assumed in the PRA will be maintained during plant operations. In addition, certain non-safety-related systems which provide defense-in-depth or are credited in the PRA

evaluations are included in the scope of the RAP to provide a high degree of confidence in their performance. The SSCs identified by D-RAP and the assumed reliabilities form the basis for the O-RAP in the operating plant. Inservice inspection and testing, as well as the maintenance tasks and frequency are based on reliability needs.

As the staff stated in DSER Open Item 16.2.1-1 above, the applicant needed to modify Section 16.2 of the SSAR to reflect the NRC position on RAP. Specifically, revise Section 16.2.1.2 to include incorporation of the objectives of O-RAP into existing requirements for maintenance and quality assurance. Also as stated in the DSER Open Item 16.2.1.1-2 above, the consistent use of term "risk-significant" is preferred by the staff rather than "safety-related" and "non-safety-related systems which provide defense-in-depth."

In Section 17.4.4, "Relationship to Other Administration Programs," Westinghouse modified the section to state that the D-RAP manifests itself in other administrative and operational programs. The technical specifications provide surveillance and testing frequencies for certain risk-significant SSCs, providing confidence that the reliability values assumed for them in the PRA will be maintained during plant operations. Risk-significant systems that provide defense-in-depth or result in significant improvement in the PRA evaluations are included in the scope of the D-RAP.

Westinghouse further modified this section stating that the O-RAP can be implemented through the plant's existing programs for maintenance or quality assurance. For example, the plant's implementation of the Maintenance Rule, 10 CFR 50.65, can provide coverage of the SSCs that would be included in O-RAP. The COL applicant will be responsible for the submittal of an O-RAP to the NRC. The NRC will review this process as part of the plant's maintenance program, QA program, or other existing programs.

Based on the above modification, the staff finds that Westinghouse adequately addressed DSER Open Items 16.2.1-1 and 16.2.1.1-2 in this section. This also supports the closure of DSER Open Items 16.2.1-1 and 16.2.1.1-2, as described in Sections 17.4.1 and 17.4.2 of this report, respectively. The staff also finds that SSAR Section 17.4.4, "Relationship to Other Administrative Programs," is in accordance with the review guidance in draft SRP 17.4 and, therefore, is acceptable.

17.4.5 The AP600 Design Organization

In Revision 0 to Section 16.2.3.1, "The AP600 Design Organization," Westinghouse stated that the AP600 design organization described in Section 1.4 of the SSAR formulates and implements the AP600 D-RAP. The staff's RAI 630.3 regarding the design organization responsible for RAP was issued to Westinghouse in a letter dated October 14, 1992. In that RAI the staff concluded the following:

- The description of the design organization should include the organizational and administrative aspects applicable to the D-RAP, including a discussion on organizational accountability for implementing the design portion of a RAP, and means for disposition of vendor and plant design organization equipment recommendations.

- The D-RAP should describe the programmatic interfaces (i.e., how various parts of the design organization interface).

- The description of the design organization should include how the performance of risk-significant SSCs, when compared to that specified in PRA, will be fed back to the designer to resolve reliability discrepancies.

In the RAI, the staff provided its position that the D-RAP applies to the certified design applicant and the design entity that completes the site-specific portions of a plant (e.g., an architect/engineer (A/E) under contract or a COL applicant acting as its own A/E). The staff requested that Westinghouse provide a discussion regarding the D-RAP and its applicability to an A/E in Section 16.2.3.1 of the SSAR.

Westinghouse responded to the RAI by a letter dated February 9, 1993, and revised the section in Revision 1 to the SSAR. The staff identified that Westinghouse needed to delete, complete, or explain the meaning of the partial sentence,"evaluation is the responsibility of the risk analysis." that appeared in Section 16.2.3.1 and in the RAI 630.2 response dated February 9, 1993. This was identified as DSER Open Item 16.2.3.1-1.

Westinghouse revised Section 17.4.5, "The AP600 Design Organization," by including the following information:

> The AP600 organization of Section 1.4 formulates and implements the AP600 D-RAP. The AP600 management staff is responsible for the AP600 design and licensing. The AP600 staff coordinates the program activities, including those performed within Westinghouse as well as work completed by the architect-engineers and other supporting organizations listed in Section 1.4. The AP600 staff is responsible for development of Phase I of the D-RAP and the design, analyses, and risk and reliability engineering required to support development of the program. Westinghouse is responsible for the safety analyses, the reliability analyses and the PRA. The reliability analyses are performed using common databases from Westinghouse and from industry sources such as INPO and EPRI.
>
> The Risk and Reliability organization is responsible for developing the D-RAP and has direct access to the AP600 staff. Risk and Reliability is responsible for keeping the AP600 staff cognizant of the D-RAP risk-significant items, program needs, and status. Risk and Reliability participates in the design change control process for the purpose of providing D-RAP-related inputs to the design process. Additionally, a cognizant representative of Risk and Reliability is present at design reviews. Through these interfaces, Risk and Reliability can identify interfaces between the performance of risk-significant SSCs and the reliability assumptions of the PRA. Meetings between Risk and Reliability and the designer are then held to manage interface issues.

The staff concludes that the new information provided in Section 17.4.5 to describe the AP600 Design Organization's implementation of D-RAP requirements is in accordance with draft SRP Section 17.4, RAP, and therefore, is acceptable. The staff verified that Westinghouse deleted the partial sentence as described in DSER Open Item 16.2.3.1-1. The staff finds this acceptable, and therefore, DSER Open Item 16.2.3.1-1 is closed.

In addition, in the DSER, the staff identified that the COL applicant must submit its D-RAP organization for staff review and that Westinghouse needed to revise Section 16.2.3.1, "The AP600 Design Organization," to include this item. This was identified as DSER Open Item 16.2.3.1-2 and COL Action Item 16.2.3.1-1.

Westinghouse revised Section 17.4.6, "Objectives," to include that the COL applicant is responsible for submitting its site-specific (Phase III) D-RAP organization description to the NRC. The staff finds this is in accordance with draft SRP Section 17.4, RAP, and therefore, is acceptable. On this basis, DSER Open Item 16.2.3.1-2 is closed. To reflect the new section numbering, COL Action Item 16.2.3.1-1 is dropped. It is redesignated as COL Action Item 17.4.5-1.

17.4.6 Objective

In Revision 0 to Section 16.2.2, "Objective," Westinghouse stated that the objective of the two-phase RAP is to design reliability into the plant and to maintain the AP600 consistent with the PRA evaluation. In RAI 630.2 dated October 14, 1992, that staff stated its position that the objective of the RAP is to:

(1) identify the plant SSCs that are significant contributors to plant safety, as quantified by the PRA and other sources

(2) ensure that the plant design provides SSCs that are at least as reliable as those assumed in the PRA

(3) ensure the risk-significant SSCs are built and operated throughout plant life as least as reliably as assumed in the PRA

The staff stated that once the risk-significant SSCs have been identified, the D-RAP should describe the process for achieving this overall objective and should also identify key assumptions regarding any operation, maintenance, and monitoring activities that a referencing COL applicant should consider in developing its O-RAP. The staff requested Westinghouse to state in greater detail what the objective of the RAP is in Section 16.2.2 of the SSAR, including the objectives of D-RAP and O-RAP.

Westinghouse responded to the RAI by a letter dated February 9, 1993, and subsequently revised Section 16.2.2 in Revision 1 to state that the objective of the two-phase RAP is to design reliability into the plant and to maintain the AP600 reliability consistent with the NRC safety goals.

The Westinghouse RAI response and Revision 1 to the SSAR only partially responded to RAI 630.2. Establishing baseline reliabilities does not identify the plant SSCs that are significant contributors to plant safety, as quantified by the PRA and other sources. The staff determined that Westinghouse needed to modify the objectives of D-RAP to include the identification of risk-significant SSCs, as determined by probabilistic, deterministic, or other methods. This was identified as DSER Open Item 16.2.2-1.

Also, as stated in the DSER Open Item 16.2.1.1-2, above, the consistent use of term "risk-significant" is preferred by the staff rather than "safety-related" and "non-safety-related systems which provide defense-in-depth."

In Section 17.4.6, "Objective," Westinghouse includes the goals that have been established for the D-RAP.

Phase III of the D-RAP and the O-RAP are the responsibility of the COL applicant. The purpose of the O-RAP is to ensure that reliability is maintained consistent with overall safety goals and that the capability to perform safety-related functions is maintained. Individual component reliabilities are expected to change throughout the course of plant life because of aging and of changes in suppliers and technology. Changes in individual component reliabilities are acceptable as long as overall plant safety performance is maintained within the NRC safety goals and the deterministic licensing design bases.

The staff finds the information in Section 17.4.6 acceptable. DSER Open Items 16.2.2-1 has been adequately addressed in this section. The staff finds this acceptable and therefore, DSER Open Item 16.2.2-1 is closed. Additionally, the staff finds that Westinghouse adequately addressed DSER Open Item 16.2.1.1-2 in this section. This supports the closure of DSER Open Item 16.2.1.1-2, as described in Section 17.4.2 of this report. Based on the resolution of the open items above, the staff finds that SSAR Section 17.4.6 is in accordance with the guidance in draft SRP Section 17.4, RAP; therefore, it is acceptable.

17.4.7 D-RAP, Phase I

In Section 17.4.7, "D-RAP, Phase I," Westinghouse states that Phase I, the definition portion of D-RAP, includes the initial identification of SSCs to be included in the program, implementation of those aspects which are applicable to design efforts, and definition of the scope, requirements, and implementation options to be included in the later phases. The staff finds this section to be in accordance with draft SRP 17.4 and, therefore, is acceptable.

17.4.7.1 SSCs Identification and Prioritization

In Revision 0 to Section 16.2.3.2 of the SSAR, Westinghouse stated that the initial task of the D-RAP was the identification of risk-significant SSCs to be included within the scope of the RAP. The AP600 PRA served as the primary source for identifying these SSC and their critical failure modes. SSCs included in the RAP, the safety-related systems, as well as are those important to non-safety-related systems that provide defense-in-depth or are credited in the PRA (Table 16.2-1). Other sources are available for identifying risk-significant SSC, such as event analyses, information notices, component failure reports, and other failure data.

The staff initially had no RAI questions on this section. However, in Revision 1 to the SSAR, Westinghouse modified Section 16.2.3.2, by stating, that the identification of the safety-related SSCs and the AP600 implementation of the RTNSS process serve as the primary sources for identifying these SSCs and their critical failure modes. Reference 2 [WCAP-13856, AP600 Implementation of the Regulatory Treatment of Non Safety-Related Systems Process] provides a list of the non-safety-related SSCs that perform the functions identified as important in the RTNSS process.

The staff determined that the use of the RTNSS process rather than probabilistic methods (i.e., PRA) as the primary source for identifying risk-significant SSCs and their critical failure modes was unacceptable. This was identified as DSER Open Item 16.2.3.2-1.

The staff also determined that Westinghouse needed to specify the method of prioritizing the risk-significant SSCs. This was identified as DSER Open Item 16.2.3.2-2.

In DSER Open Item 16.2.1.1-4, the staff determined that Reference 2 (i.e., WCAP-13856, "AP600 Implementation of the Regulatory Treatment of Non Safety-Related Systems Process") did not provide an appropriate method for determining risk-significant SSCs for RAP.

Also as stated in DSER Open Item 16.2.1.1-2, the consistent use of term "risk-significant" is preferred by the staff rather than "safety-related" and "non-safety-related systems which provide defense-in-depth."

In Revision 10, Westinghouse provided the following information to Section 16.2.7.1 of the SSAR, "SSC Identification and Prioritization":

- PRA-based measurements provide information that contributes to the identification and prioritization of SSCs. A component's risk achievement worth (RAW) is the factor by which the plant's core damage frequency (CDF) increases if the component reliability is assigned the value of 0.0. In selecting a risk achievement worth threshold for identifying critical components, it was considered that the AP600 has a CDF approximately two orders of magnitude lower than currently operating pressurized water reactors. Thus, a threshold risk achievement worth of at least 10 for any given component supports an AP600 CDF that is 10 times better than that of currently operating reactors. Components with risk achievement worth values of 10 or greater will be included in the D-RAP.

- Risk reduction worth (RRW) is used in the selection process. A component's risk reduction worth is the amount by which the plant's CDF decreases if the component's reliability is assigned the value of 1.0. A threshold measure of 1.2 or greater is used as the appropriate cutoff. Given the low CDF of the AP600, this is considered appropriate. Components with risk reduction of 1.2 or greater will be included in the D-RAP.

- Fussel-Vesely worth (FVW) is also used in the screening process. This is a measure of an event's contribution to the overall plant CDF. Components with Fussel-Vesely worths of 20 percent or greater are included in the D-RAP.

The staff reviewed the PRA for the AP600 design and noted that the medium CDF value for the AP600 design is 2E-7. The staff identified a number on non-conservative assumptions in the PRA. These included very high reliability assumptions for passive plant components without completed testing to verify the reliability assumptions and the lack of an adequate uncertainty analysis for passive components. Several common cause failure modes for safety-related electrical component did not meet Westinghouse importance measure threshold value criteria; however, the staff determined that some of these SSCs should be considered risk-significant. In addition, a review of the risk ranking results revealed that some AP600 non-safety-related SSCs (e.g., RTNSS systems, main feedwater initiating event SSCs, electrical power supply busses and breakers, the diverse actuation scram system, and other initiating event non-safety

related components) had RRW values greater than 1.005 but were below the Westinghouse threshold of 1.2, and RAW values greater than 2 but less than the Westinghouse threshold value of 10.

The staff also determined that the methods used to identify SSCs under the scope of RAP should be consistent with the risk determination methods used in current industry guidance to implement the maintenance rule, NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." In RG 1.160, the NRC endorsed NUMARC 93-01 as an acceptable method for implementing the maintenance rule. NUMARC 93-01, Section 9.3.1, "Establishing Risk Significant Criteria," uses RAW values greater than 2, RRW values greater than 1.005 and cutsets that account for 90 percent of the overall CDF to determine which SSCs are risk significant.

Based on the approved risk determination methods identified for other evolutionary ALWR RAP programs (e.g., General Electric Advanced Boiling Water Reactor and Combustion Engineering System 80+ D-RAP plans), as well as NRC-approved industry guidance (i.e., NUMARC 93-01) used to implement the risk determination methods used under the maintenance rule for existing operating plants, the staff determined that Westinghouse needed to use more conservative importance measure threshold values to determine SSCs which fall under the scope of RAP.

In response to the staff's concerns, Westinghouse modified the information in Section 17.4.7.1, "SSC identification and Prioritization," to change the importance measure threshold values used to identify risk-significant SSCs under the scope of RAP, as follows:

- Components with RAW values of 2 or greater are considered for inclusion in the D-RAP.
- For RRW, a threshold measure of 1.005 or greater is used as the cutoff. Components with RRW of 1.005 or greater are considered for inclusion in the D-RAP.
- Components with FVW values of 0.5 percent or greater are considered for inclusion in the D-RAP.

Westinghouse also modified Section 17.4.7.1, "SSC Identification and Prioritization," to address deterministic methods used to identify risk-significant SSCs under the scope of RAP. Several non-safety-related SSCs (e.g., RTNSS systems, the diverse actuation system, the non-safety-related diesel generators, the feedwater pumps) were also identified as being under the scope of D-RAP using the importance measure threshold values noted above, the expert panel process, industry operating experience, the RTNSS process, and other deterministic methods used to identify risk-significant SSCs. The staff found the description of these different methods used to identify risk-significant SSCs under the scope of RAP to be in accordance with draft SRP 17.4 and, therefore, is acceptable. On this basis, DSER Open Item 16.2.3.2-1 is closed. This information also supports the closure of DSER Open Items 16.2.1.1-2 and 16.2.1.1-4 as described in Section 17.4.2.

Westinghouse modified Section 16.2.7.1 (now Section 17.4.7.1), "SSC Identification and Prioritization," to address prioritization of risk-significant SSCs under the scope of RAP. The staff found the modifications to be in accordance with draft SRP 17.4 and, therefore, is

acceptable for identifying and prioritizing the list of risk-significant SSCs. On this basis, DSER Open Item 16.2.3.2-2 is closed.

In Table 17.4-1 of the SSAR, Westinghouse also provided some Level 2 PRA risk analysis and used engineering judgement of the expert panel to identify SSCs that protect containment as risk significant. These SSCs include the containment recirculation squib valves, the containment recirculation motor-operated valves, the automatic depressurization system (ADS) stages 1, 2, and 3 motor-operated valves, and the containment shell. Based on the staff review of the list of risk-significant SSCs identified in Table 17.4-1, the staff finds the list is in accordance with the guidance contained in draft SRP 17.4 and, therefore, is acceptable.

17.4.7.2 D-RAP, Phase II

In Section 17.4.7.2, D-RAP, Phase II, Westinghouse states that during Phase II of the D-RAP, maintenance assessments and recommendations are developed to enhance reliability and the plant risk-significant components. These activities are shown in Figure 17.4-1 as "Recommended Plant Maintenance Monitoring Activities." The recommendations can take the form of monitoring activities or preventive, predictive or corrective maintenance, and are dependent upon the types of failure modes that a component may experience. These modes are generally determined by a failure modes, effects and criticality analysis (FMECA). The maintenance recommendations address the most risk-significant failure modes of the component. On the basis of the FMECA approach for maintenance recommendations on risk-significant SSCs, which is in accordance with draft SRP 17.4, the staff finds this section acceptable.

17.4.7.2.1 Information Available to Combined License Applicant

In Revision 0 to Section 16.2.3.4, "Information Available to Combined License Applicant," Westinghouse stated that the COL applicant is responsible for performance of the O-RAP, which maintains risk-significant SSCs reliability throughout plant life. The SSAR listed the following information as available to the O-RAP:

- The list of risk-significant SSCs identified during the design phase, and their assumed reliabilities. This includes related assumptions in the PRA.

- The analyses performed for those components identified to be major contributors to total risk, with the dominant failure modes identified and prioritized. The suggested means for prevention or mitigation of these failure modes form the basis for the plant surveillance, testing, and maintenance programs.

- Table 16.2-2 of the SSAR provides a list of design recommendations for the non-safety-related systems. These recommendations include operational modes when the systems are required to be available, the defense-in-depth functions performed by each system, the recommended modes for extended maintenance operations on the system, and remedial actions if the system is not available.

The staff initially had no RAI questions on this section. However, in Revision 1 to Section 16.2.3.4 of the SSAR, Westinghouse revised the section to state the COL applicant is

responsible for performance of the O-RAP, which maintains risk-significant SSCs reliability throughout plant life and listed the following information as available to the O-RAP:

- the list of risk-significant SSCs identified during the design phase
- the PRA assumptions for component unavailability and failure data, provided in Table F-4 of the PRA report
- the analyses performed for those components identified to be major contributors to total risk, with the dominant failure modes identified and prioritized (The suggested means for preventing or mitigating these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.)
- recommended short-term availability controls in Table 16.2-2 of the SSAR for those non-safety-related SSCs that perform the functions identified as important in the RTNSS process (These recommendations include the operational modes when the systems are risk significant, the recommended modes for extended maintenance operations on the system, and remedial actions if the system is not available.)

As stated in DSER Open Item 16.2.1-1, above, Westinghouse needed to modify Section 16.2 of the SSAR, in particular, Section 16.2.3.4, "Information Available to Combined License Applicant," to reflect the NRC position on RAP. Additionally, Section 16.2.3.4, should be revised to include that the COL applicant is responsible for augmenting and completing the remainder of the D-RAP to include any site-specific design information and identify and prioritize the risk-significant SSCs as required by the D-RAP applicable regulation. Also, as stated in DSER Open Item 16.2.1.1-2, the consistent use of term "risk-significant" is preferred by the staff rather than "safety-related" and "non-safety-related systems which provide defense-in-depth."

Westinghouse modified Section 17.4.7.2.1, "Information Available to Combined License Applicant," to state that to support the COL applicant's D-RAP Phase III and O-RAP, the following information is provided:

- the list of risk-significant SSCs identified during the design phase
- the PRA assumptions for component unavailability and failure data
- the analyses performed for components identified to be major contributors to total risk, with the dominant failure modes identified and prioritized (The suggested means for prevention or mitigation of these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.)

On the basis of the above modification to Section 17.4.7.2.1 and other RAP subsections, the staff finds the information available to the COL applicant acceptable. This supports the closure of DSER Open Items 16.2.1-1 and 16.2.1.1-2, as described in Sections 17.4.1 and 17.4.2 of this report, respectively. The staff also finds SSAR Section 17.4.7.2 in accordance with the review guidance in draft SRP 17.4 and, therefore, is acceptable.

17.4.7.3 D-RAP, Phase III

Westinghouse states in Section 17.4.7.3, "D-RAP, Phase III," that site-specific activities of the D-RAP are the responsibility of the COL applicant. In Figure 17.4-1, Westinghouse shows these activities in the Phase III area of the figure. At this stage, the COL applicant modifies or appends the D-RAP package based on considerations specific to the site.

The staff found the addition of Section 17.4.7.3 acceptable. The COL applicant will need to determine site-specific information which affects the list of risk-significant SSCs under the scope of RAP. This information must also be reviewed and approved by the NRC. In Revision 18 to Section 16.2.7.3 of the SSAR, "D-RAP, Phase III," Westinghouse revised this section to add that the COL applicant will establish PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP. The staff finds this section to be in accordance with draft SRP 17.4 and, therefore, is acceptable. However, Westinghouse removed this commitment in Revision 19 of the SSAR. Upon request by the staff, Westinghouse returned it in Revision 22 to Section 17.4.7.3 and Section 17.5, "Combined License Information Items." This is COL Action Item 17.4.7.3-1.

17.4.7.4 D-RAP Implementation

In RAI 630.5 dated October 14, 1992, the staff stated that in order to ensure a workable reliability assurance program has been proposed at the design stage, Westinghouse needed to provide an example of how the AP600 RAP would be implemented (e.g., from the design phase through the end of the operating phase) using a specific SSC identified as risk-significant in the PRA. In the example, Westinghouse needed to identify where the interface occurs between the D-RAP (including the architect engineer) and the O-RAP. In addition, the staff asked Westinghouse if the AP600 RAP description differed from the Utility Requirements Document (URD), Volume III, description of RAP. If so, the staff requested that Westinghouse describe the differences.

Westinghouse responded to the RAI by a letter dated February 9, 1993, and stated the SSAR would not be revised to include the example. The RAI response and the refusal to provide an example was unacceptable. This was identified as DSER Open Item 16.2.6-1.

In Section 17.4.7.4, "D-RAP Implementation," Westinghouse added information on the ADS which had a major design change as a result of the D-RAP (i.e., explosive squib valves replaced motor operated valves). Information was added that identified FMECA associated with the squib valves and recommended maintenance and inservice testing activities to maximize valve reliability. The FMECA approach is also not described in the URD RAP description but it is another acceptable method of determining common mode failures, recommending maintenance, and minimizing unavailability for risk significant SSCs. The staff finds this example approach of D-RAP implementation to be in accordance with draft SRP 17.4 and, therefore, is acceptable. On this basis, DSER Open Item 16.2.6-1 is closed.

17.4.8 Glossary of Terms

In Revision 1 to Section 16.2.5 of the SSAR, "Glossary of Terms," Westinghouse defined risk-significant as "any SSC determined in the PRA or by significant other analysis to be a major contributor to overall plant risk." The staff determined that the definition of risk significant should be modified to more clearly define the risk-significant analysis being used. In Section 17.4.8, "Glossary of Terms," Westinghouse modified the definition of risk significant to state "Any SSC determined in the PRA or by risk-significance analysis (e.g., Level 2 PRA and shutdown risk analyses) to be a major contributor to overall plant risk." Based on this modification, the staff found all of the definitions in the glossary of terms to be in accordance with the guidance contained in draft SRP 17.4 and, therefore, is acceptable.

17.4.9 Evaluation of DSER Items for COL Activities O-RAP

In Revision 0 of Section 16.2.4 of the SSAR, Westinghouse stated that the COL applicant is responsible for performing those tasks necessary to maintain the reliability of risk-significant SSCs. Reference 1 in that section (NUREG/CR-5695, "A Process for Risk-Focused Maintenance") contained examples of cost-effective maintenance enhancements, such as increasing condition-monitoring and shifting time-directed to condition-directed maintenance.

In addition to performing the specific tasks necessary to maintain SSCs reliability at its required level, the O-RAP includes consideration of the following elements:

- Reliability database - Historical data is available on equipment performance. The compilation and reduction of this data provides the plant with an initial key source of component reliability information. After plant operation begins, this database will grow and become more useful in the O-RAP.

- Surveillance and testing - In addition to maintaining the performance of those components necessary for plant operation, this also provides a high degree of reliability for the safety-related SSCs.

- Maintenance plan - Intended to provide high equipment reliability by taking into account manufacturer's recommendations, and operating experience, this plan describes the nature and frequency of maintenance activities to be performed on plant equipment. The plan includes the selected SSCs identified in the D-RAP, which are periodically evaluated.

The staff initially had no RAI questions on this section. However, as stated in DSER Open Item 16.2.1-1, the applicant should modify Section 16.2 of the SSAR to reflect the NRC position on RAP. Specifically, revise Section 16.2.4, "Combined License Applicant RAP (O-RAP)," to include existing requirements for quality assurance into O-RAP. Additionally, the COL applicant will need to provide reasonable assurance that the risk-significant SSCs do not degrade to an unacceptable level during plant operations, through implementation of reliability performance monitoring, problem and failure identification, and a comprehensive corrective action program. This was identified as DSER Open Item 16.2.4-1. Westinghouse adequately addressed COL applicant O-RAP activity issues in Section 17.5, "Combined License Information Items." The

staff finds SSAR Section 17.5 to be in accordance with draft SRP 17.4 and, therefore, is acceptable. On this basis, DSER Open Item 16.2.4-1 is closed.

The staff determined that NRC will need to review COL information in Section 17.5 of the SSAR on existing requirements for QA that should be included in the O-RAP. This information also supports the closure of DSER Open Item 16.2.1-1, as described in Section 17.4.1 of this report. The NRC will review related QA activities in the COL applicant's O-RAP during the operational phase of plant life. This is COL Action Item 17.4.9-1.

The staff determined that NRC will need to review the COL process for determining risk-significant SSCs as described in NUMARC 93-01. This guidance contains acceptable methods for determining the list of risk-significant SSCs under the scope of RAP and to implement the monitoring requirements of the maintenance rule. In addition, this guidance describes acceptable methods for the COL to establish reliability and availability measures for risk-significant SSCs under the scope of RAP. In addition, if the measures are not met, the COL must implement corrective actions to improve SSC performance. This assumes that the COL will have an O-RAP which provides reasonable assurance that the risk-significant SSCs do not degrade to an unacceptable level during plant operations, through implementation of reliability performance monitoring, problem and failure identification, and a comprehensive corrective action program. This is COL Action Item 17.4.9-2.

17.4.10 COL Action Items

In Revision 5 to the SSAR, Westinghouse added Section 17.5, "Combined License Information Items," to describe how the COL applicant will address its QA program for design, construction, and operations phases. The information requirements identified in this section of the SSAR provide the basis for COL Action Items 17.1-1 and 17.2-1. In Revision 22 to the SSAR, Westinghouse relocated Section 17.4.8 regarding COL activities for D-RAP, Phase III and O-RAP to Section 17.5 of the SSAR. The information requirements identified in this section also provide the basis for the COL action items identified in Section 17.4 of this report. The staff identified COL Action Items 17.4.1-1, 17.4.2-1, 17.4.5-1, and 17.4.7.3-1 that must be completed during Phase III of plant life. In addition, the staff identified COL Action Items 17.4.9-1 and 17.4.9-2 that must be completed during the O-RAP phase of plant life.

17.4.11 Conclusions

On the basis of its review of SSAR Section 17.4, "Design Reliability Assurance Program," the staff concludes that D-RAP for design certification meets the guidance provided in Appendix E to SECY-95-132 and draft SRP 17.4 and, therefore, is acceptable.

## 18 HUMAN FACTORS ENGINEERING

The staff reviewed Chapter 18, "Human Factors Engineering," of the AP600 Standard Safety Analysis Report (SSAR) on the basis of current regulatory requirements and NRC guidance, including the criteria of NUREG-0711, "Human Factors Engineering Program Review Model," which provides additional guidance for reviewing aspects of the AP600 Human Factors Engineering (HFE) Program not fully addressed by previously available documents. The staff's review also included aspects of the organizational structure of the applicant, training and plant procedures contained in SSAR Sections 13.1, "Organizational Structure of the Applicant," 13.2, "Training," and 13.5, "Plant Procedures," and additional human factors engineering materials submitted by Westinghouse.

In Section 18.1 of this report, the staff provides an overview of the general methodology and review criteria used in this evaluation, including the HFE Program Review Model (PRM). Sections 18.2 through 18.13 describe the results of the staff's review of the following HFE topics, the first ten of which are the elements of NUREG-0711. The last requirement, minimum inventory, addresses the challenges posed by the lack of control room detail provided in applications for advanced reactor designs:

- Human Factors Engineering Program Management (Section 18.2)
- Operating Experience Review (OER) (Section 18.3)
- Functional Requirements Analysis and Allocation (Section 18.4)
- Task Analysis (Section 18.5)
- Staffing (Section 18.6)
- Human Reliability Analysis (HRA) (Section 18.7)
- Human-System Interface (HSI) Design (Section 18.8)
- Procedure Development (Section 18.9)
- Training Program Development (Section 18.10)
- Human Factors Verification & Validation (V&V) (Section 18.11)
- Minimum Inventory (Section 18.12)

In Section 18.13, the staff provides a summary of the review findings and overall conclusions.

### 18.1 Review Methodology

#### 18.1.1 HFE Review Objective

The overall purpose of the HFE review is to ensure the following:

- HFE has been satisfactorily integrated into the AP600 development and design.

- The AP600 HSIs and procedures reflect "state-of-the-art human factors principles" [10 CFR 50.34(f)(2), as required by 10 CFR 52.47(a)(1)(ii)] and satisfy all other

appropriate regulatory requirements as stated in Title 10 of the Code of Federal Regulations (CFR).

- The AP600 HSIs, procedures, and training make possible safe, efficient, and reliable performance of operation, maintenance, test, inspection, and surveillance tasks.

18.1.2 Review Criteria

The review criteria used to assess Westinghouse's HFE program were primarily based on the criteria of NUREG-0711. In addition, the review criteria included current regulatory requirements established in 10 CFR 50.34(f), 10 CFR 50.34(g), 10 CFR 52.47, and the HFE review guidance contained in NUREG-0800, "Standard Review Plan," and NUREG-0700, "Human System Interface Design Review Guideline." For selected review topics, the staff used guidance from other NRC documents as well. These documents are identified in the appropriate review sections of this report. In addition, the staff developed additional criteria to provide a basis for reviewing aspects of the AP600 HFE program that were not fully addressed by the previously mentioned documents. These criteria are documented in NUREG-0711.

18.1.3 Procedure for Reviewing AP600 Human Factors Engineering

HFE for the AP600 design is described in the SSAR, in responses to the staff's requests for additional information (RAIs), and in several related Westinghouse topical reports (WCAPs). These materials describe a design and implementation process for an AP600 HFE program, and some preliminary products of that process. At the time the staff completed this Final Safety Evaluation Report (FSER) for design certification, Westinghouse had not completed the final AP600 HFE design. The review criteria identified in Section 18.1.2 of this report are the basis for the AP600 HFE review. The design certification evaluation is based on a design and implementation process plan that describes the HFE program elements required to develop the detailed design, and on partial completion of NUREG-0711 criteria. Generally, NUREG-0711 can be used to conduct three types of reviews of applicant submittals:

(1) the programmatic review,

(2) implementation plan review, and

(3) complete element review.

All three types of reviews were used for the AP600 design. For a programmatic review, the SSAR does not include appropriate detailed methodologies; therefore, detailed evaluations using NUREG-0711 acceptance criteria are beyond the scope of the staff's review for design certification. At a programmatic review level, NUREG-0711 criteria are used to determine whether the program provides a top-level identification of the substance of each review criterion that, after design certification, will be developed by the COL applicant into a detailed implementation plan. The value of the programmatic review is that it provides assurance that the implementation plan will address all NUREG-0711 review criteria. The commitment to develop such a detailed implementation plan is described in the AP600 Tier 1 information, which includes the Inspections, Tests, Analyses and Acceptance Criteria (ITAAC). The staff will review this plan in the context of specific applications. The ITAAC are also needed for completing the

implementation plan and providing the results to the staff for review. Westinghouse's AP600 ITAAC for HFE is evaluated in Section 14.3 of this report.

For the staff to perform an implementation plan review, the applicant's submittals should describe the proposed methodology in sufficient detail for the staff to determine if the methodology will lead to products that meet NUREG-0711 acceptance criteria for the element. An implementation plan review affords the design certification applicant the opportunity to obtain staff review and concurrence on the full method before design certification. The actual completion of the plan will then likely take place after design certification. Such a review is desirable from the staff's perspective because it presents the opportunity to resolve methodological issues and provide input early in the analysis or design process. The staff's concerns can be addressed more easily at that time than when the applicant's effort is completed. While some implementation plans can be reviewed on their own merits, the staff may request a sample analysis that demonstrates the application of the methodology and its results. The ITAAC are needed for completing the implementation plan and providing the results to the staff for review.

A complete element review can only be performed when the finished products (e.g., main control room (MCR) design) are available for the staff to evaluate. This means that the design certification applicant has submitted the analysis results report(s) and design team review report(s). An analysis results report provides the results of the design certification applicant's efforts to complete a NUREG-0711 element with respect to the review criteria. Reviewers will use the report as the main source of information for assessing compliance with the review criteria. A design certification applicant's design team review report provides the independent evaluation of the activities addressed for the element by the design team. When the staff's concerns regarding the analysis or its results are resolved, the review topic can then be closed before design certification.

The staff assessed the level of review detail for each topic based on

- an examination of the AP600 material submitted for review in advance of this report
- material referenced in the AP600 application and received before preparing this report
- meetings and discussions held with Westinghouse
- Westinghouse's response to RAI 620.51 (Rev. 2)

The results of the assessment are provided in Table 18.1-1 of this report. Note that some changes in the level of review for specific elements were made between the DSER and FSER.

In addition to the NUREG-0711 elements identified in Table 18.1-1, the staff reviewed Westinghouse's minimum inventory (18.12) of controls, displays, and alarms required to adequately implement Emergency Operating Procedures (EOPs) and address critical and risk-important operator actions identified from the AP600 Probabilistic Risk Assessment (PRA). The staff also reviewed the AP600 Emergency Response Guidelines (ERGs).

The remaining sections of this chapter present a review of each topic with the following four subheadings:

(1) *Objectives* — This section describes the overall review objectives for the topic.

(2) *Methodology* — While the general review methodology is described in this section, specific review topics sometimes have unique aspects to the review methodology. Such details are provided in the methodology section on that topic. This section identifies the specific Westinghouse material used in the safety determination (e.g., SSAR sections or RAI responses) and the materials used to support the technical basis of the evaluation (e.g., NUREG-0711 or NUREG-0700). In addition, the section summarizes the activities leading to resolution of the DSER open items.

(3) *Results* — The results section is divided into the following two components:

a. Criterion — This states the criterion being evaluated, usually based on NUREG-0711 or a regulatory document.

b. Evaluation — This describes the staff's evaluation of the Westinghouse material for its acceptability with respect to the review criterion. The basis for the assessment is documented, including documented materials and discussions with Westinghouse that may have resulted in modifications or clarifications to Westinghouse material that led to the assessment. Any questions, additional information, or discrepancies that were identified are documented in the evaluation.

The evaluation section is further subdivided into two parts: DSER evaluation and FSER evaluation. The DSER evaluation identifies the open item and the FSER Evaluation part describes the resolution of the item. Where Westinghouse addressed the criteria acceptably in the DSER, there were no open items and the FSER evaluation consisted of a verification that the material that served as the basis for the DSER evaluation was present in the final documentation and that it had not been modified in a way that could alter the staff's conclusions.

(4) *Conclusions* — This section summarizes the staff's findings for the review topic.

## 18.2 Element 1: Human Factors Engineering Program Management

### 18.2.1 Objectives

The objective of the staff's review of the AP600 HFE Program Management is to ensure that the design certification applicant has described an adequate HFE program, and that it will be implemented by a qualified HFE design team. The HFE design team should have the responsibility, authority, placement within the organization, and composition to ensure that the

design commitment to HFE is achieved. Also, the team should be guided by an HFE program plan to ensure the proper development, execution, oversight, and documentation of the HFE program. This plan should describe the technical program elements, ensuring that all aspects of the HSI are developed, designed, and evaluated based upon a structured, top-down, systems analysis using accepted HFE principles.

18.2.2 Methodology

18.2.2.1 Material Reviewed

The following Westinghouse documents were used in this review:

- SSAR (through Revision 23)
- WCAP-9817 (Revision 2) dated June, 1991
- WCAP-12601 (Revision 15) dated April 1, 1995
- WCAP-14396 (Revision 2) dated January 27, 1997
- WCAP-14401 (Revision 3) dated May 8, 1997
- WCAP-14644 (Revision 0) dated October 9, 1996
- WCAP-14645 (Revision 2) dated January 1, 1997
- WCAP-14701 (Revision 1) dated May 9, 1997
- WCAP-14822 (Revision 0) dated February 25, 1997
- Westinghouse Procedure AP-3.1, AP600 System Specification Documents (SSDs) (Revision 1), February 28, 1991
- Westinghouse Procedure AP-3.2, Design Configuration Change Control (Revision 3), March 11, 1994
- Westinghouse Procedure AP-3.5, Design Reviews (Revision 1), August 9, 1991
- Westinghouse Procedure AP-3.6, AP600 Design Criteria Documents (Revision 2), March 11, 1994
- Westinghouse Procedure AP-3.7, Interface Control Document, Revision 0, February 8, 1991
- Westinghouse Procedure AP-3.12, AP600 Engineering Data Base (EDB) Access and Control, Revision 0, October 31, 1991
- Westinghouse Procedure AP-3.14, AP600 Plant I&C Systems (PI&CS), Revision 0, October 31, 1991
- Westinghouse Procedure AP-7.2, Control of Subcontractor Submittals, Revision 0, August 9, 1991
- RAI 620.15 (Revision 1)
- A sample design review report

18.2.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 1 of NUREG-0711. The staff reviewed Westinghouse's HFE program management at a complete element review level. That is, finished products from the element are available for review using NUREG-0711 criteria.

18.2.2.3 DSER Item Resolution

To address Element 1 open items, a number of review activities occurred:

1. The staff conducted a review of Westinghouse design files. During that review, conducted on April 5, 1995, and April 6, 1995, at the Westinghouse office in Rockville, Maryland, the following types of information were included:

   - Design procedures
   - Design review procedures
   - A sample of a design review report

   The design files review produced a number of questions that were addressed in a conference call on April 18, 1995, between the NRC, Brookhaven National Laboratory (BNL), and Westinghouse in which the issues were discussed and where additional information was presented.

2. Westinghouse submitted the following documents to address Element 1 issues:

   - Draft Revision 4 to SSAR Section 18.4, "Man-Machine Interface System (M-MIS) Design Team," June 30, 1995

   - Draft Revision 4 to SSAR Sections 18.4.4, "Human Factors Engineering Issues Tracking," June 30, 1995

   - Response to Open Item 18.2.3.3-6: HFE Subcontractor Efforts, April 25, 1995

These review activities addressed Open Items 18.2.3.2-1, 18.2.3.2-2, 18.2.3.3-1 through -6, and 18.2.3.4-1 through -4. The results of the review were documented in a letter dated March 22, 1996, from the NRC. Numerous telephone conversations were conducted to discuss and clarify NRC comments and Westinghouse technical information. Westinghouse further addressed Element 1 open items in Revision 9 of the SSAR. In addition to reviewing the material noted above, the staff conducted an audit of the HFE Issues Tracking System Database.

18.2.3 Results

18.2.3.1 General HFE Program Goals and Scope

Criterion 1: HFE Program Goals

*Criterion:* The general objectives of this program should be stated in human-centered terms. As the HFE program develops, the terms should be objectively defined and serve as criteria for test and evaluation activities. Generic human-centered HFE design goals are listed in General Criterion 1 of NUREG-0711.

*Evaluation:*

DSER Evaluation

Section 18.4.3 of the SSAR described the design team's approach as user-centered. This description is supported throughout Chapter 18 of the SSAR for all phases of the HFE program:

- Section 18.8.1 of the SSAR identified the mission of the M-MIS design effort to be "to improve the means that are provided to the users of the plant operation and control centers for acquiring and understanding plant data and in executing actions to control the plant's processes and equipment."

- The process described in Sections 18.6 and 18.8.2.1.2 of the SSAR for functional task analysis emphasized the identification of detection, monitoring, decision, and control requirements for crew task performance to support HSI development.

- The verification and validation process described in Section 18.8.2.3 of the SSAR focused on the evaluation of user-centered issues (see Table 18.8.2-1 of the SSAR) that are consistent with NUREG-0711-identified goals, such as crew awareness of plant condition.

The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

The SSAR (Revision 23), Section 18.2, "Human Factors Engineering Program Management," acceptably incorporates the HFE Program Goals previously reviewed and accepted by the staff in the DSER. Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 2: Assumptions and Constraints

*Criterion:* The design assumptions (or constraints) should be clearly identified. An assumption or constraint is an aspect of the design, such as a specific staffing plan or the use of specific HSI technology, that is an input to the HFE program rather than the result of HFE analyses and evaluations. For example, if a design constraint imposed by a utility requirement (rather than by design analysis) is that the entire plant operation, including emergencies, is to be accomplished by a single operator, that constraint will impact all other human factors analyses, such as allocation of function (much greater automation than is typical in commercial nuclear power plants would be required) and workstation design (a single operations console containing all plant monitoring and control function would be required). The staffing design constraint may drive the design without an acceptable HFE rationale, and may negatively impact the integration of plant personnel into the overall plant design. The purpose of this criterion is to make such "design drivers" explicit.

*Evaluation:*

DSER Evaluation

The SSAR (Revision 0) addresses the assumptions and constraints of the design by identifying them as inputs to the HFE program. The overall HFE design and implementation process is described in Section 18.8 of the SSAR (Revision 0). This section presents the inputs to the program (e.g., specific system details such as those represented by piping and instrumentation diagrams). Also, see Figure 18.8.2-2 of the SSAR (Revision 0). While the high-level inputs are identified, the starting points for selected aspects of the detailed HFE program activities are unclear, specifically in the areas of function allocation and control room resource selection. The following paragraphs discuss the staff's concerns with the function allocation and control room resource selection. These concerns are provided as examples of the staff's overall concerns with these starting points.

- Function Allocation

  Westinghouse has made many decisions based on allocating functions as discussed in Chapter 7 of the SSAR (Revision 0). However, the applicant has not performed function allocation for the AP600 design. Nonetheless, a "baseline" allocation of functions (i.e., the function allocations identified in Section 7 of the SSAR, Revision 0) appears to be an input to the HFE program. Also, WCAP-14075 states that "...the assumption has been made that the AP600 will have instrumentation and control similar to that of two-loop low pressure PWR's previously designed by Westinghouse (Reference Plant). This information will be used as input to the task analysis as part of the man-machine interface design" (p. 38). Further, Table 4 of WCAP-14075 provides a detailed comparison showing that much of the instrumentation and controls (I&C) in the AP600 design is "similar" to the reference plant. This reinforces the concern that the design of the I&C is already predetermined before any of the detailed HFE design program has begun. Thus, the contributions of the HFE program to function allocation are unclear. However, the second sentence of the quote indicates that this detailed information is only a starting point in the design that will take place after the design certification, as part of the HFE design process. Detailed information is needed from Westinghouse to determine which is the case, and how the information in WCAP-14075 will be used as an input to the overall HFE design process. Westinghouse should clarify the basis used for making the function allocations identified in Chapter 7 of the SSAR (Revision 0) and the role of function allocation in the AP600 design process.

- Control Room Resource Selection

  The use of a wall panel information station is not presented as a result of design analyses; rather, this design option appears to be an input to the HFE program. Section 18.9.1.1.1 of the SSAR (Revision 0) states that the wall panel information station is "important to maintaining situation awareness of the crew and for supporting crew coordination." However, these functions may be alternatively served using a similar display presented at the operators' workstations where there would be no requirements to look away from the workstation to the wall panel. It is unclear why physical separation of the system overview display for the workstations is desirable. Also, it is plausible that the effect of such a separation on operator performance will not have the desired result,

and that operators focusing on the tasks at their workstations will fail to attend to the wall panel information. Conversely, the wall panel may serve crew integration purposes. Westinghouse should clarify the intent and reason for selecting the panel design.

These examples illustrate that Westinghouse should further clarify the assumptions (or inputs) to the HFE program.

Westinghouse should identify the starting point of the HFE program for each appropriate HFE activity (i.e., those aspects of the analysis or design that are inputs to the HFE program, rather than the result of HFE analyses and evaluations). For example, if functions have been allocated to plant personnel, not as part of the HFE analysis, the allocations should be identified. This was Open Item 18.2.3.1-1.

FSER Evaluation

This open item was addressed in SSAR Section 18.2.1.2 (Revision 23), "Assumptions and Constraints." Assumptions and constraints stem from regulatory guidance, utility groups, and AP600 plant system design specifications. The SSAR provides an overview of the types of requirements associated with each. For example, it is a utility requirement that a single reactor operator control major plant functions performed from the main control room during normal plant operations.

With respect to the specific concerns noted in the DSER, the process of function allocation was briefly discussed in SSAR Section 18.2.1.2 and further clarified in WCAP-14644 (Revision 0). Initial allocations are made by system engineers based on operating experience of previous designs.

With respect to control room resources, the inclusion of a wall panel display is an approach to meeting a utility requirement for an integrating overview and mimic display. While alternative approaches are possible, the wall panel approach will be designed and evaluated as part of the AP600 HFE program.

Appropriately, Westinghouse indicates that while all assumptions and constraints are provisionally treated as requirements, they are ultimately evaluated as part of the HFE design process for their appropriateness.

Note that the DSER review referenced Figure 18.8.2-2 of the SSAR (Revision 4) and that Figure was removed in SSAR Revision 19. However, SSAR (Revision 23) Section 18.2.1.2 adequately provides the information needed.

Based on this information, Open Item 18.2.3.1-1 is closed and the NUREG-0711 criterion is satisfied.

Criterion 3: Applicable Facilities

*Criterion:* The HFE program should address the main control room (MCR), remote shutdown facility, technical support center (TSC), emergency operations facility (EOF), and local control stations (LCSs).

*Evaluation:*

DSER Evaluation

Section 18.8.1 of the SSAR (Revision 0) and the responses to RAI 620.6 and RAI 620.88 indicated that the scope of the HFE program encompasses the facilities identified in this criterion. The response to RAI 620.88 indicated that Westinghouse will define the EOF information systems and communications necessary for the plant to interface to the EOF. The design of the facility will be the responsibility of the COL applicant. This is acceptable because the site-specific requirements on the EOF necessitate final design by the COL applicant. However, the presentation of the plant data should be consistent with the M-MIS design, and the Westinghouse approach will achieve this compatibility and consistency.

The SSAR acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23), Section 18.2.1.3, "Applicable Facilities," indicates that the following facilities are included in the AP600 human factors engineering program: main control room, technical support center, remote shutdown room, operational support center, emergency operations facility, and local control stations. The COL applicant is responsible for designing the EOF, including specification of a location, in accordance with the AP600 human factors engineering program. This is COL Action Item 18.2-2. Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 4: Applicable HSIs

*Criterion:* The applicable HSIs included in the HFE program should encompass all operations, accident management, maintenance, test, inspection, and surveillance interfaces (including procedures).

*Evaluation:*

DSER Evaluation

Section 18.8 of the SSAR (Revision 0) indicated that the mission of the HFE program includes the HSIs identified in this criterion. Section 18.13 of the SSAR (Revision 0) identifies the general programmatic approach to system and equipment interfaces. The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23), Section 18.2.1.4, "Applicable Human System Interfaces," states that the scope of human systems interfaces covered by the AP600 human factors engineering program includes instrumentation and control systems that perform the monitoring, control, and protection functions associated with all modes of plant operation as well as off-normal, emergency, and accident conditions. Physical and cognitive requirements of plant personnel involved in the use, control, maintenance, test, inspection, and surveillance of plant systems are addressed by Westinghouse's human factors engineering program. Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 5: Applicable Plant Personnel

*Criterion:* Plant personnel who should be included in the HFE program include licensed control room operators, as defined in 10 CFR Part 55, and the following categories of personnel defined in 10 CFR 50.120:

- nonlicensed operator
- shift supervisor
- shift technical advisor
- instrument and control technician
- electrical maintenance personnel
- mechanical maintenance personnel
- radiological protection technician
- chemistry technician
- engineering support personnel

In addition, other plant personnel who perform tasks that are directly related to plant safety should also be included.

*Evaluation:*

DSER Evaluation

In addition to operations personnel, Section 18.8.1.1 of the SSAR (Revision 0) identified the following personnel types to be within the mission and scope of the HFE program: management, engineering, maintenance, health physics, and chemistry. The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23) Section 18.2.1.5, "Applicable Plant Personnel," acceptably incorporates the applicable plant personnel previously reviewed and accepted by the staff in the DSER.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 6: Technical Basis

*Criterion:* The applicant's Human Factors Engineering Program should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

The Westinghouse HFE program incorporated accepted industry standards, guidelines, and practices. Sections 18.1.2, 18.5.3, 18.6.8, and 18.8.3 of the SSAR (Revision 0) provide references for the basis of the HFE program. In addition, the response to RAI 620.72 provides additional information on the technical basis for AP600 function allocation considerations. The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23) incorporates accepted industry standards, guidelines, and practices. These references are cited in the SSAR (e.g., Sections 18.2.7, 18.5.5) and in accompanying WCAPs (e.g., WCAP-14645 (Revision 2); WCAP-14644, Revision 0; WCAP-14701 (Revision 1)). Based on this information, the NUREG-0711 criterion is satisfied.

18.2.3.2 HFE Design Team and Organization

The staff reviewed the responsibility, organizational placement and authority, composition, and staffing of the HFE design team addressed in the SSAR to determine whether it acceptably addresses these topics as defined by NUREG-0711. NUREG-0711 refers to an HFE design team, while the equivalent Westinghouse organizational unit is called the Human System Interface (HSI) Design Team (SSAR Revision 0 referred to this team as the M-MIS Design Team). The two terms are used interchangeably in this report.

Criterion 1: Responsibility

*Criterion:* The team should be responsible (with respect to the scope of the HFE program) for the following activities:

- developing all HFE plans and procedures
- overseeing and reviewing all HFE design
- development, test, and evaluation activities
- initiating, recommending, and providing solutions through designated channels for problems identified in the implementation of the HFE activities
- verifying implementation of team recommendations

- ensuring that all HFE activities comply with the HFE plans and procedures
- scheduling activities and milestones

*Evaluation:*

DSER Evaluation

In Section 18.4.3 of the SSAR (Revision 0), Westinghouse described the design team's role in the AP600 design effort, stating that the purpose of the team is to "provide technical guidance, and to organize, manage, and review the design of the MCR and the associated plant interfaces." The Westinghouse response to RAI 620.13 identified the responsibilities of the M-MIS Design Team management and component groups, which include the M-MIS Design Group, Procedures Group, Training Group, Control Analysis System Group, Plant Instrumentation and Control System (PI&CS) Group, and Human Sciences Group. In addition, an Advisors/Reviewers Team is available to the design groups for consultation and to oversee the M-MIS design process. The Advisors/Reviewers team addresses problems identified in the implementation of the HFE activities through a design change proposal system (described in Westinghouse's response to RAI 620.15). The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

In SSAR (Revision 23), Section 18.2.2, Human System Interface Design Team and Organization, the function of the human system interfaces design team is described as being part of the AP600 systems engineering function and having similar responsibilities, authority, and accountability as other segments of the design team. The responsibilities of the human system interfaces design team (18.2.2.1) address the responsibilities identified by this NUREG-0711 criterion. Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 2: Organizational Placement and Authority

*Criterion:* The primary HFE organization(s) or function(s) within the organization of the total program should be identified, described, and illustrated (e.g., charts to show organizational and functional relationships, reporting relationships, and lines of communication). When more than one organization is responsible for HFE, the lead organizational unit responsible for the HFE program plan should be identified. The team should have the authority and organizational placement to ensure that all of its areas of responsibility are accomplished, and to identify problems in the implementation of the HSI design.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.13, Westinghouse discussed the AP600 HFE organization. As discussed in the evaluation of compliance of the AP600 M-MIS Team with Criterion 1, "Responsibility," the team is comprised of six design and analysis groups and an Advisors/Reviewers Team. These groups report to a PI&CS manager, who is responsible for

the overall M-MIS design and its integration with the rest of the plant design. This relationship is illustrated in Figure 620.13-1 in the Westinghouse response to RAI 620.13. The M-MIS design team is part of the AP600 system engineering function, and has the same responsibility, authority, and accountability as other AP600 design teams. The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

Section 18.2.2.2, "Organizational Placement and Authority," of SSAR (Revision 23), discusses the organization of the human system interface design team and its relationship to the AP600 design organization. Although the SSAR reviewed by the staff in its FSER evaluation was changed from the SSAR reviewed for the DSER, the staff's evaluation and conclusions were not altered. Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 3: Composition

*Criterion:* NUREG-0711 specifies that the HFE design team should have specific expertise in the following areas:

- technical project management
- systems engineering
- nuclear engineering
- control and instrumentation engineering
- architect engineering
- human factors
- plant operations
- computer system engineering
- plant procedure development
- personnel training
- systems safety engineering
- reliability, availability, maintainability, and inspectability (RAMI) engineering

*Evaluation:*

DSER Evaluation

Section 18.4 of the SSAR (Revision 0) specified the composition of the M-MIS Design Team. Each of the areas of expertise identified in NUREG-0711 is represented in the M-MIS design team, with the exception of the following:

- Plant procedure development - While this expertise is identified in Section 18.4.1 of the SSAR (Revision 0) and a procedures group is identified as a component of the M-MIS design team, no design team members with procedures backgrounds are identified in Section 18.4.2 of the SSAR (Revision 0).

- Systems safety engineering - No reference is identified to system safety engineering.

- RAMI engineering - Maintainability engineering expertise is identified on the M-MIS design team; however, the reliability, availability, and inspectability engineering skills are not identified.

The specific qualifications of the team members were not identified to the level of detail specified by NUREG-0711 (i.e., education and years of relevant experience). The staff requested Westinghouse to provide the following information:

- identify team members with procedures background.
- identify team members with safety system engineering background.
- identify team members with RAMI background.
- provide the specific qualifications of the team members.

This was Open Item 18.2.3.2-1.

FSER Evaluation

Draft Revision 4 of the SSAR (June 30, 1995) provided more detail concerning the composition and qualifications of the M-MIS design team. In Section 18.4.1, the disciplines of plant procedure development, systems safety engineering, and reliability/availability/maintainability/inspectability were identified. The staff reviewed the qualifications using Appendix A of NUREG-0711. The Westinghouse qualifications met the criteria of NUREG-0711, with one exception. The System Safety Engineering function did not identify certification by the Board of Certified Safety Professionals in System Safety. This exception was found acceptable because the qualifications presented in SSAR were based on the experience requirements for system safety engineering, which included acceptable background areas of experience.

SSAR (Revision 23) Section 18.2.2.4, "Team Staffing Qualifications," incorporates the information provided by Westinghouse in their draft SSAR (Revision 4). Based on this information, Open Item 18.2.3.2-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 4: Team Staffing

*Criterion:* Team staffing should be described in terms of job descriptions and assignments of team personnel.

*Evaluation:*

DSER Evaluation

Job descriptions and assignments were not provided in the SSAR (Revision 0). The staff requested job descriptions and assignments of key personnel in RAI 620.13. Westinghouse's response to this RAI was provided in general terms by describing the responsibilities of the groups that comprise the M-MIS design team. Westinghouse should provide job descriptions and assignments of team personnel. This was Open Item 18.2.3.2-2.

FSER Evaluation

Draft Revision 4 of the SSAR (June 30, 1995) provided more detail concerning the M-MIS team personnel responsibilities. Section 18.4.3, "M-MIS Design Team Role," identified the organization of the team into functional engineering design groups. This information was subsequently incorporated into the SSAR. A description of the responsibilities of each technical discipline (as identified in SSAR Section 18.2) is provided in SSAR (Revision 23) Section 18.2.2.3, "Composition," which was reviewed and accepted by the staff. Based on this information, Open Item 18.2.3.2-2 is closed and this NUREG-0711 criterion is satisfied.

18.2.3.3 HFE Process and Procedures

Criterion 1: General Process Procedures

*Criterion:* The process should be identified through which the team will execute its responsibilities, including procedures for the following:

- assigning HFE activities to individual team members
- governing the internal management of the team
- making management decisions regarding HFE
- making HFE design decisions
- governing equipment design changes
- conducting design team review of HFE products

*Evaluation:*

DSER Evaluation

Section 18.8.2 of the SSAR (Revision 0) describes the programmatic aspects of the design process; however, the staff requested additional information in RAI 620.5, RAI 620.14, RAI 620.15, and RAI 620.56, because the SSAR (Revision 0) did not fully describe the general HFE process and procedures. In its response to RAI 620.56, Westinghouse indicated that the process and documentation requirements are described in design process files and documentation. In addition, Westinghouse's response to RAI 620.51 identified unnamed "Design Reviews and Configuration Control Documents." During a December 1993 meeting, Westinghouse also referred to an M-MIS Program Plan for first-of-a-kind engineering (FOAKE). These documents were not available in time for the staff to complete the DSER review; therefore, the staff did not complete its review of the HFE process and procedures.

In its response to RAI 620.51, Westinghouse stated that design reviews are an integral part of the design process. These reviews will be documented, but Westinghouse stated that separate HFE Design Team Evaluation Reports, as described in the program review model, are not necessary. NUREG-0711 does not identify that specific reports must be submitted. It states that the type of information addressed in the criterion should be available for review. A documented review process may satisfy this criterion, but there is not sufficient information in the Westinghouse material to make such a determination.

Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe the aspects of the HFE design process identified in this criterion, such

as the "Design Reviews and Configuration Control Documents" identified in Westinghouse's response to RAI 620.51. This was Open Item 18.2.3.3-1.

FSER Evaluation

*Introduction*

The Westinghouse documents identified in the open item were proprietary. Thus, the staff conducted a design files audit on April 5 and April 6, 1995, and reviewed the following Westinghouse documents:

- WCAP-12601, AP600 Program Operating Procedures (Revision 15, dated April 1, 1995)
- WCAP-9817, Design Review Manual (Revision 2, dated June 1991)
- A sample of a design review report

The design files review produced a number of questions that were addressed in a conference call on April 18, 1995, between NRC, BNL, and Westinghouse in which the issues were discussed and where additional information was presented.

The documents reviewed address, in part, NUREG-0711 criteria covered by this open item. However, additional information was still needed to resolve Open Item 18.2.3.3-1. The documents also addressed, to varying extent, other open items of Element 1, as will be discussed in the following section. It should be noted that all of the design documentation discussed below that contributed to the staff's safety determination were published in WCAP-14822, "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8," (Revision 0).

*Discussion of Reviewed Documents*

Westinghouse Procedure AP-3.1, "AP600 System Specification Documents (SSDs)," Revision 1, dated February 28, 1991, establishes requirements for SSDs. SSDs identify specific system design requirements and show how the design satisfies the requirements. They provide a vehicle for controlling and documenting the design process. They also address information transmittal between and interfaces among the various design groups. General Step C states that the SSDs provide for the control room HSI design. Step E and Appendix C provide a list of the AP600 systems for which SSDs are required, which includes the Operation and Control Centers (OCS). Appendix A provides a top-level Table of Contents by section for each SSD and Appendix B provides a summary description of what should go into sections of the SSD. Under Section 2, "System Design Criteria & Objectives," there is a requirement for a discussion of HSI considerations. Section 7, "I & C requirements," should include alarms and status indicators. Attachment 2 contains questions related to HSI and components.

Westinghouse Procedure AP-3.2, Design Configuration Change Control (Revision 3), March 11, 1994, provides the required process and actions in order to implement a design change in a document that is under configuration control. The scope of the procedure includes SSDs, drawings, and so forth. It has considerable information on responsibilities, procedures, documentation, and approvals.

Westinghouse Procedure AP-3.5, Design Reviews (Revision 1), August 9, 1991, specifies the method for preparing, conducting, and documenting formal design reviews (DRs) for the purpose of design verification. The DR is a systemic overall evaluation of the design (of particular systems) by the DR committee. The three levels of DR generally performed are preliminary, intermediate, and final. The procedure also identifies the Action Item Chit (AIC), which is a form used to document reviewers' concerns, recommended corrective actions, and resolutions. Appendix A contains a DR checklist that addresses items such as human factors, system boundaries, I & C, control requirements, and interfacing system requirements.

Westinghouse Procedure AP-3.6, AP600 Design Criteria Documents (Revision 2), March 11, 1994, specifies requirements for the preparation, review, approval, and revision of Design Criteria Documents, which define the requirements for specific aspects of the AP600 design, typically in a single discipline or subdiscipline. Item D on Page 2 requires that Westinghouse review and approve contractor documents.

Westinghouse Procedure AP-3.7, Interface Control Document, Revision 0, February 8, 1991, identifies the responsibilities of organizations (including contractors) at the design interfaces and ensures that design changes affecting the interfaces are properly coordinated.

Westinghouse Procedure AP-3.12, AP600 Engineering Data Base (EDB) Access and Control, Revision 0, October 31, 1991, discusses requirements and responsibilities for preparing and approving movement of design data into the AP600 EDB. The EDB serves as the repository of AP600 design data for parties involved in the engineering design of the plant, so that all parties can be assured of using up-to-date data in their design tasks.

Westinghouse Procedure AP-3.14, AP600 Plant I & C Systems (PI&CS), Revision 0, dated October 31, 1991, addresses the following areas: a) HSI design of control rooms and control boards; b) I&C design; c) control room/equipment design. The Westinghouse PI&CS group has the responsibility for coordinating and integrating AP600 I&C and HSI with groups that support the AP600 organizations. A process is specified and elaborated upon for PI&CS engineering work that includes: definition of an engineering plan, review of inputs, production of system documentation, verification of work, procurement and manufacturing followup, and acceptance testing. An iterative feature is built into the process.

Westinghouse Procedure AP-7.2, Control of Subcontractor Submittals, Revision 0, August 9, 1991, establishes the method for receipt, review, control, and issue of subcontractor design document submittals. It calls for the review of all subcontractor documents, but does not specify criteria for acceptance. Further information on this topic is presented under Open Item 18.2.3.3-6 below.

The Design Review Manual (WCAP-9817 (Revision 2)) describes the DR process, which is a method for identifying design problems during product development. It includes a preliminary, intermediate, and final DR and has a rough schedule. Section 3.0 specifies the formal documentation required in the DR reports. Section 5.0 includes the DR checklists, including Figure 5.5, the Human Factors Checklist, which contains 27 detailed questions to be answered by the DR team. Section 8.0, "Action Item Chits (AIC)," describes how these chits document issues raised by the DR team. It defines responsibilities for the AIC process. In the telephone

conversation on April 18, 1995, Westinghouse stated that WCAP-9817 is a higher level, more general document and that the detailed criteria for a given project may vary. For the AP600 project, the detailed criteria are contained in WCAP-12601 (Revision 15).

The staff identified several questions and forwarded them to Westinghouse for response. Some of these questions were addressed in the telephone conversations on April 18, 1995. Pertinent questions to the review and the Westinghouse answers (where available) are summarized below.

WCAP-9817/DSER Item 18.2.3.4-2 - Section 8.0 addresses AICs; however, a clear method for tracking them to closure was not provided.

Westinghouse Procedure AP-3.14/DSER Items 18.2.3.3, 1c, 1d, and 3. - This procedure details what goes into the SSD for the I&C and HSI of the control room; however, it lacked details of the human factors and HSI aspects. Further, from the information provided in this AP, it was not clear how the PI&CS SSD discussed here relates to the OCS SSD in Appendix C of AP-3.1 (particularly the Appendix B table of contents of AP-3.14).

Westinghouse responded to these questions by telephone (April 18, 1995) noting that AP-3.14 tailors the requirements of AP-3.1 for I&C/MMI systems. Also, they noted that the design documents for MMI resources are the Functional Requirements documents. The OCS SSD will refer to these Functional Requirements documents (e.g., the Alarm System documents). Therefore, the concerns raised by the staff in its review of these documents were resolved.

Sample Design Review/DSER Item 18.2.3.3-1f and 18.2.3.4-2, 3, and 4. - The staff reviewed a sample DR document, as an example of the process. It was examined in conjunction with WCAP-9817 (Revision 2). During a telephone conversation on April 18, 1995, Westinghouse clarified that some differences exist between the sample DR package and the procedures identified in WCAP-9817 (Revision 2). The document was incomplete when compared to the information specified for a DR in WCAP-9817 (Revision 2). For example:

1. Not all of the AICs were signed off as complete or had clear action identified, e.g., item numbers 2, 3, 4, 10, 11, & 14. The status and tracking of these AICs were not identified. Attachment 3 was missing.

2. All of the items required by Section 3.0 of WCAP 9817 (Revision 2) were not included, e.g.:

   - findings (3.1)
   - reference to minutes (3.3)
   - reference to calculations (3.4)
   - copy of each action item with resolution or assigned completion date and tracking (3.5)
   - copies of each action item not accepted (e.g., item no.1 was missing) (3.6)

3. The DR data package per Section 2 and completed checklists per Section 5, as specified by WCAP-9817 (Revision 2) were not included.

4. The information also did not match that called for in Appendix B of AP-3.5.

Westinghouse stated in the telephone conversation that the sample DR package was produced following a process that was slightly different from the AP600 process. Hence, it did not precisely comply with the AP procedures for the AP600. Also, WCAP-9817 (Revision 2) is a top-level guidance document that is used to write the detailed project level documents. Thus, an individual project DR will not necessarily meet all of the requirements of WCAP-9817 (Revision 2). They further stated that at the completion of the DR, before the product is turned over to the customer, all AICs and other paperwork will be complete. The Westinghouse responses from the telephone conversation of April 18, 1995, resolved the staff's concerns related to this document.

*Comparison to NUREG-0711 Criteria*

Items 1a and 1b of the NUREG-0711 criterion regarding general process procedures address the assignment of HFE activities to individual team members and the internal management of the team. SSAR (Revision 23), Section 18.2.2.2, "Organizational Placement and Authority," discussed the organization of the team (Figure 18.2-2) and its relationship to the overall AP600 organization. The internal workings of the organization were also described. The key people of the HSI design team consist of an I&C Manager, an HSI Design Function Manager, the HSI technical lead, a review team, and the core HSI design team. The technical lead works in the HSI Design Function and reports to the Manager of the HSI Design Function, who in turn reports to the I&C Manager, who reports to the AP600 Project Manager. Responsibilities are defined in Section 18.2.2.1. The organization is depicted on SSAR (Revision 23) Figure 18.2-2, which lists individual technical skills that are related to the Project and coordinated by the technical lead. These disciplines include: Technical Project Management, Systems Engineering, Nuclear Engineering, I&C Engineering, Architect Engineering, Human Factors, Plant Operations, Computer Systems, Plant Procedures, Training, Systems Safety Engineering, Maintainability or Inspectability, and Reliability or Availability Engineering. These activities are acceptably detailed and Westinghouse has gained experience in implementing such an organization over the past several years.

NUREG-0711 items 1c and 1d address management and design decisions relative to HFE. These topics are generally covered in the AP600 design procedures, as previously discussed. Also, they are further addressed in SSAR (Revision 23), Section 18.2.2.2, "Organizational Placement and Authority," which covers the roles of the various managers associated with the project. One outstanding concern was related to AP-3.1 and AP-3.14. These procedures detail what goes into the SSDs for the I&C and HSI of the control room; however, they lack any details of the human factors and HSI aspects. Further, it was not clearly documented how the System Functional Requirements Documents addressed this and were properly linked and coordinated.

The outstanding issues related to items 1c and 1d noted above were addressed in SSAR Section 18.2.3.1 (Revision 23). The SSAR indicates that SSDs document human factors and HSI requirements by including task requirements, information requirements, and operations requirements. They provide a mechanism to document and track HFE requirements. A functional requirements document is developed for each HSI resource, e.g., alarm system and wall panel information system. Design specification documents document design specifications and integration. This information acceptably provided an indication of how HFE information is documented and coordinated.

NUREG-0711, items 1e and 1f address equipment design changes and design team review of HFE products. These areas are covered by WCAP-9817 (Revision 2), AP-3.2, AP-3.5. These documents acceptably discuss the Westinghouse design change control and DR process, as noted previously. Thus, based on the review of Westinghouse design files and the revised SSAR, all criteria were resolved and these aspects of the NUREG-0711 criterion are considered resolved.

The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822 (Revision 0), AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8. The WCAP incorporates the following procedures: AP3.1, AP3.2, AP3.5, AP3.6, AP3.7, AP3.12, AP3.14, and AP7.2.

Several of the procedures had been slightly modified since the time at which they were initially reviewed. The most significant revision was to AP3.5, which was revised to include a HFE checklist based on the checklist reviewed from WCAP-9817 (Revision 2).

The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, Open Item 18.2.3.3-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: Process Management Tools

*Criterion:* Tools and techniques (e.g., review forms) to be used by the team to ensure they fulfill their responsibilities should be identified by the applicant.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "General Process Procedures." Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe the tools and techniques to be used by the team during the HFE design process as identified in this criterion. This was Open Item 18.2.3.3-2.

FSER Evaluation

As discussed in Criterion 1 of this section, the staff reviewed Westinghouse design process documentation. This documentation addressed most of the NUREG-0711 criteria covered by this open item, as noted in the discussion of Open Item 18.2.3.3-1 above. However, two areas were not satisfactorily addressed.

First, WCAP-9817 (Revision 2), Section 8.0, and AP-3.5 addressed AICs, but there was not a clear method discussed for tracking them to closure; and, an actual example seemed to substantiate this concern. Namely, the sample DR was reviewed as an example of Westinghouse's DR process, in conjunction with WCAP-9817 (Revision 2) and AP-3.5. Some AICs appeared to be missing or incomplete. For example, not all of the AICs were signed off as complete or had clear action identified. Further, some of the positive features of WCAP-9817 (a

top-level document) had not been carried forward to requirements for the project, for which a sample DR product was being built. Thus, the completed Human Factors checklists, required by Section 5 of WCAP-9817 (Revision 2), were not included in the DR data package. Thus, it was possible that the same would be the case for AP600.

Both of these issues were addressed in SSAR (Revision 23) Section 18.2.3.1, "General Process and Procedures." The SSAR indicated that Action Items resulting from DRs are tracked to closure through the design issues tracking database. SSAR (Revision 23) Section 18.2.4, "Human Factors Engineering Issues Tracking," indicated that the database receives issues to track from several sources, including DRs. The responsibility for entering DR action items into the database and tracking them is the manager responsible for the system reviewed. This method is an acceptable approach to tracking the DR action items.

The issue associated with the use of HFE checklists was addressed in SSAR (Revision 23) Section 18.2.3.1, "General Process and Procedures." HFE checklists are included in the DR package provided for each DR. An action item is defined for each issue identified through use of the checklist. This information acceptably addresses the staff's concern about the application of the HFE checklists to AP600.

Based upon the information reviewed by the staff, Westinghouse has acceptably addressed this DSER open item. The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822 (Revision 0), AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8. (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures.)

The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, Open Item 18.2.3.3-2 is closed and this NUREG-0711 criterion is satisfied.

Criterion 3: Integration of HFE and Other Plant Design Activities

*Criterion:* The integration of design activities should be identified, including inputs from other plant design activities to the HFE program, and outputs from the HFE program to other plant design activities. The iterative nature of the HFE design process should also be addressed.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "General Process Procedures." Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe the integration of the design activities of the HFE design process as identified in this criterion. This was Open Item 18.2.3.3-3.

FSER Evaluation

As discussed in Criterion 1 of this section, the staff reviewed Westinghouse design process documentation and, for this section, SSAR (Revision 0) Chapter 18 and draft SSAR (Revision 4) Section 18.4, "M-MIS Design Team," dated June 30, 1995.

As discussed previously with respect to Open Item 18.2.3.3-1, WCAP-12601 (Revision 15) provides an overall AP600 structure under which the AP600 is designed. This procedural structure provides for an integration of design activities among the various entities, both within and external to Westinghouse. Procedure AP-3.1, "AP600 System Specification Documents (SSDs)," provides for SSDs that identify specific system design requirements and show how the design satisfies the requirements. SSDs provide a vehicle for controlling and documenting the design process. SSDs also address information transmittal between and interfaces among the various design groups.

Procedure AP-3.2, "Design Configuration Change Control," provides the required process and actions in order to implement design changes. Procedure AP-3.7, "Interface Control Document," identifies the responsibilities of organizations (including contractors) at the design interfaces. Procedure AP-3.12, "AP600 Engineering Data Base (EDB) Access and Control," discusses requirements and responsibilities for preparing and approving movement of design data into the AP600 EDB. The EDB serves as the repository of AP600 design data for parties involved in the engineering design of the plant, so that all parties can be assured of using up-to-date data in their design tasks.

Procedure AP-3.14, "AP600 Plant I&C Systems (PI&CS)," addresses MMI and equipment design of control rooms, and I&C design. The PI&CS function has the responsibility for coordinating and integrating AP600 I&C and HSI with groups that support the AP600 organizations. A process is specified for PI&CS engineering work that includes the definition of an engineering plan, review of inputs, production of system documentation, verification of work, procurement and manufacturing followup, and acceptance testing. An iterative feature is built into the process.

Additionally, SSAR (Revision 0) Figures 18.4-1, 18.4-2, 18.8.2-1, and 18.8.2-9 depict organization and design process flows that include iterative and feedback features. SSAR (Revision 0), Section 18.12 discusses the integration of the Westinghouse designed components of the HSI with those portions that are site-specific and the responsibility of the COL applicant. This includes areas such as the Operations Support Center (OSC) and the Emergency Operations Facility (EOF). The staff concludes that Westinghouse has acceptably addressed the integration of HFE and other plant design activities. The information was provided in final form in SSAR (Revision 23) Section 18.2.3.3, "Integration of Human Factors Engineering and Other Plant Design Activities."

Based upon the information provided and reviewed by the staff, Westinghouse has acceptably addressed this DSER open item. The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822 (Revision 0), "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8." (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures.)

The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, Open Item 18.2.3.3-3 is closed and this NUREG-0711 criterion is satisfied.

Criterion 4: HFE Program Milestones

*Criterion:* HFE program milestones should be identified so that the effectiveness of the HFE effort can be evaluated at critical check points, and to show the relationship to the integrated plant sequence of events. A relative schedule should be available for staff review of HFE program tasks showing the relationships among HFE elements and activities, products, and reviews.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "General Process Procedures." Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe the HFE program milestones as identified in this criterion. This was Open Item 18.2.3.3-4.

FSER Evaluation

As discussed in Criterion 1 of this section, the staff reviewed Westinghouse design documentation. Based upon the high-level design process obtained and the conference call on April 18, 1995, between NRC, BNL, and Westinghouse, the program schedule of HFE tasks, which was provided in the SSAR (Revision 0), showing the relationships among the various HFE elements and activities, products, and reviews was clarified. This relative schedule is summarized in SSAR (Revision 23) Figure 18.2-3, "Overview of the AP600 Human Factors Engineering Process." The program is described in some detail in SSAR (Revision 23) Section 18.2, "Human Factors Engineering Program Management."

Internal DRs that are to be performed throughout the design process are described in WCAP-12601 (Revision 15), AP-3.5, "Design Reviews," which specifies the method for preparing, conducting, and documenting formal DRs for the purpose of design verification. The Design Review is a systemic overall evaluation of the design (of particular systems) by the Design Review Committee. Three levels of Design Review are normally performed: a preliminary, an intermediate, and a final review. The information provided by Westinghouse acceptably addresses the relative program schedule.

Based upon the information provided and reviewed by the staff, Westinghouse has acceptably addressed this DSER open item. The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822 (Revision 0), "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8." (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures.)

The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, the DSER item is resolved and this NUREG-0711 criterion is satisfied.

Criterion 5: HFE Documentation

*Criterion:* HFE documentation items should be identified and briefly described along with the procedures for retention and access.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "General Process Procedures." Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe the HFE documentation and associated procedures as identified in this criterion. This was Open Item 18.2.3.3-5.

FSER Evaluation

As discussed previously, WCAP-12601 (Revision 15) provides an overall structure under which the AP600 is designed. A number of the procedures contained within WCAP-12601 (Revision 15) address documentation, including retention and access. Typically the requirements and controls apply to all AP600 areas and are not specific to the HFE area; however, some of the procedures of WCAP-12601 (Revision 15) are more specifically oriented to HFE areas.

Procedure AP-3.1, regarding AP600 SSDs, establishes requirements for SSDs. SSDs will be written for all systems and will contain the design information for that system. They identify specific system design requirements and show how the design satisfies the requirements. Other WCAP-12601 (Revision 15) procedures that also address documentation are as follows:

- AP-3.2, "Design Configuration Change Control,"
- AP-3.5, "Design Reviews,"
- AP-3.6, "AP600 Design Criteria Documents,"
- AP-3.12, "AP600 Engineering Data Base (EDB) Access and Control," and
- AP-7.2, "Control of Subcontractor Submittals."

SSAR (Revision 23) Section 18.2.3.4, "Human Factors Engineering Documentation," provided an overview of the HFE documentation process. Thus, Westinghouse has established a documentation process, including procedures, that address the requirements of the criterion.

Based upon the information provided and reviewed by the staff, Westinghouse has acceptably addressed this DSER open item. The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822 (Revision 0), "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8." (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures.)

The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, Open Item 18.2.3.3-5 is closed and this NUREG-0711 criterion is satisfied.

Criterion 6: HFE in Subcontractor Efforts

*Criterion:* HFE requirements should be included in each subcontract and the subcontractor's compliance with HFE requirements should be periodically verified.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "General Process Procedures." Westinghouse should provide WCAP-12601, WCAP-9817, OCS-GES-011, and any additional documents that describe how the subcontractor's compliance with HFE requirements is verified as identified in this criterion. This was Open Item 18.2.3.3-6.

FSER Evaluation

As discussed in Criterion 1 of this section, the staff reviewed Westinghouse design process documentation. This information addressed only a small part the NUREG-0711 criteria covered by this open item as noted in the previous discussion of Item 18.2.3.3-1. Thus, additional information was required to close the item.

Procedure AP-3.6, "AP600 Design Criteria Documents," Revision 2, March 11, 1994, specified requirements for the preparation, review, approval, and revision of Design Criteria Documents, which defined the requirements for specific aspects of the AP600 design, typically in a single discipline or subdiscipline. Item D on Page 2 requires that contractor documents be reviewed and approved by Westinghouse. No criteria were given for this review.

Procedure AP-3.7, "Interface Control Document," Revision 0, February 8, 1991, identified the responsibilities of organizations (including contractors) at the design interfaces and ensures that design changes affecting the interfaces are properly coordinated.

Procedure AP-7.2, "Control of Subcontractor Submittals," Revision 0, August 9, 1991, established the method for receipt, review, control, and issue of subcontractor design document submittals. It called for the review of all subcontractor documents. However, no review criteria were specified.

Thus, this information addressed only part of the NUREG-0711 criterion covered by this open item. Additional information was provided in an April 25, 1995, Westinghouse response to this open item in which they indicated that WCAP-12601 is sent to all subcontractors of the AP600 and that they must follow its procedures. This requirement places subcontractor operating procedures and DRs under the same procedures as those governing the rest of the AP600 design.

SSAR (Revision 9) Section 18.2.3.5, "Human Factors Engineering in Subcontractor Efforts," did not clearly indicate that subcontractors must follow Westinghouse design and review

procedures. In fact, it stated that these organizations follow their own procedures, which is in apparent contradiction of the information received on April 25, 1995.

Westinghouse addressed this concern in SSAR (Revision 23) Section 18.2.3.5. The revision indicated that the procedures of WCAP-14822 (Revision 0) that describe the design documentation apply to subcontractor design organizations. The WCAP contains all procedures used in the staff's review. The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue. Based on this information, Open Item 18.2.3.3-6 is closed and this NUREG-0711 criterion is satisfied.

18.2.3.4 HFE Issues Tracking

Criterion 1: Availability

*Criterion:* A tracking system should be available to address human factors issues that are known to the industry (defined in Element 2, "Operating Experience Review," of NUREG-0711) and identified throughout the life cycle of the HFE/HSI design, development, and evaluation. Issues are those items that need to be addressed at some later date, and thus need to be tracked to ensure that they are not overlooked. An existing tracking system may be adapted to serve this purpose.

*Evaluation:*

DSER Evaluation

RAI 620.15 requested a description of how Westinghouse tracks and documents HFE-related issues. Westinghouse's response indicated that HFE issues are addressed and resolved through design change proposals (DCPs). DCPs are maintained in a computerized database. Because DCPs address proposed resolutions, they are part of an issues tracking process, but such a system does not address the documentation and tracking of unresolved issues. RAI 620.54 reiterated the staff's request for information on an issues tracking system. Westinghouse's response indicated that "no formal system exists to track future issues." In its response to RAI 620.80, Westinghouse indicated that HFE issues are tracked using a "human factors checklist."

In the December 1993 meeting, Westinghouse indicated that a tracking system is in place and is more fully described in WCAP-9565 and WCAP-12601. The checklists are more fully described in WCAP-9817. However, these documents were not available for review at the time this review was performed. Thus, it as not clear whether a tracking system meeting NUREG-0711 criteria was available. The staff requested Westinghouse to submit WCAPs- 9565, -12601, and -9817, as well as any additional documents that describe the tracking system and checklists as identified in this criterion. This was Open Item 18.2.3.4-1.

FSER Evaluation

Westinghouse's response to RAI 620.15 (Revision 1) indicated that two methods are used to identify, track, and resolve design issues: (1) the Design Configuration Change Control process and (2) the Design Review process. The revised response did not address documentation and

tracking of unresolved issues. In addition, the response indicated that issues are identified and tracked through the DR process. The design review board includes a representative of the HSI design team. The board uses Human Factors checklists (described in WCAP-9817 (Revision 2)). For each issue identified, action items are identified and documented. The DR is not considered complete until all items are closed. The DR is documented in a report.

On April 5, 1995, and April 6, 1995, the following Westinghouse proprietary documents were reviewed:

- WCAP-12601, "AP600 Program Operating Procedures" (Revision 15, April 1, 1995)
- WCAP-9817, "Design Review Manual" (Revision 2, dated June, 1991)
- a sample of a design review report

WCAP-12601, Procedure AP-3.1, "AP600 System Specification Documents (SSDs)," Revision 1, dated February 28, 1991, establishes requirements for the SSDs. The SSDs identify specific system design requirements and show how the design satisfies the requirements. They provide a vehicle for controlling and documenting the design process. At the March 1995 meeting at Westinghouse, Westinghouse stated that they were considering using the SSDs for a HFE tracking system. The mechanism for this was not clear.

WCAP-12601, Procedure AP-3.5, "Design Reviews," Revision 1, dated August 9, 1991, specifies the method for preparing, conducting, and documenting formal DR. The procedure also identifies the AIC, which is a form used to document reviewers' identified concerns, recommended corrective actions, and the resolutions.

These documents addressed, in part, the NUREG-0711 criteria covered by this open item (and the following three open items). Additional information was needed to close the item.

Further information was provided in SSAR Draft Revision 4 (June 30, 1995), Section 18.4.4, "HFE Issues Tracking," which described the types of issues tracking methods and how each is used. Issues tracking was accomplished using a combination of four processes:

(1) the design configuration change control process
(2) the design review process
(3) SSD
(4) Electric Power Research Institute (EPRI) Utility Requirements Document (URD) compliance database

While the URD compliance database may be an important activity, because many of its requirements were the result of HFE issues and concerns, the staff considered it outside the scope of an issues tracking system with respect to this NUREG-0711 criteria. URD compliance tracks requirements conformance. The appropriate technique depended on the stage of the design process and on how the issue was identified. The combination of these approaches to issue tracking seemed to provide an acceptable means of identifying and resolving HFE concerns. Westinghouse described a generally acceptable approach to the tracking of HFE issues and the staff requested an audit of the system to verify its implementation and use.

However, a tracking system was described in SSAR (Revision 9) Section 18.2.4, "Human Factors Engineering Issues Tracking," which differed from that reviewed earlier. The SSAR

(Revision 9) described the use of a database to track AP600 issues to resolution. The database receives inputs from OER, DRs, and design issues identified by AP600 designers. The staff considered the establishment of a single mechanism to track issues a better approach than the collection of mechanisms previously described. However, as noted in the discussions of the more detailed aspects of the tracking system below, the tracking system was not described in sufficient detail to establish that the tracking system criteria are satisfied. Therefore, resolution of tracking system open items required a staff audit of the tracking system availability, description, and operating procedures.

In response to these concerns, Westinghouse submitted a letter dated December 16, 1996, that included a sample of the HFE Issues Tracking System database entries. The staff reviewed the sample entries and determined that an acceptable tracking system has been established and that the general procedures described in the SSAR (Revision 23) have been acceptably implemented. Based on this information, Open Item 18.2.3.4-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: Method

*Criterion:* The method should document and track HFE issues from identification until elimination or reduction to an acceptable level.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "Availability." Westinghouse should submit WCAPs-9565, -12601, and -9817, as well as any additional documents that describe the method for handling HFE issues as identified in this criterion. This was Open Item 18.2.3.4-2.

FSER Evaluation

SSAR Section 18.4.4, "HFE Issues Tracking," (Draft Revision 4, June 30, 1995), described the methods used to track and resolve such issues for each issue tracking technique. As indicated in the discussion of Open Item 18.2.3.4-1 above, issues tracking was to be accomplished using several processes, each with its own methodology. The design configuration change control process was to track issues through a formal database. The process was to be used to track proposed design changes from initiation to implementation of a design solution.

The DR process followed the formal procedures specified in Westinghouse DR procedures. Issues arising from DRs are tracked through AICs until they are resolved. Westinghouse procedures generally prohibit field implementation of a product until all such items are satisfactorily resolved and documented. While several questions remained concerning specific aspects of the Westinghouse DR process (see discussion under Open Item 18.2.3.3-1: HFE Process and Procedures above), it was an acceptable means of tracking HFE issues.

The SSD is used to track HFE issues prior to configuration control (when the other methods are used). Issues are tracked by entering them into the functional requirements and design-basis document.

SSAR (Revision 23) Section 18.2.4, "HFE Issues Tracking," described a database for tracking issues. The general method by which issues are tracked was not specifically identified. It stated that design issues are entered, and that the actions taken to address the issue and the final resolution are documented. An audit of the tracking system was needed to establish the procedures that are used to enter and track issues in the database.

As discussed in the resolution of Criterion 1 above, the staff performed an audit of the tracking system and determined that an acceptable tracking system has been established and that the general procedures described in the SSAR have been acceptably implemented. Based on this information, Open Item 18.2.3.4-2 is closed and this NUREG-0711 criterion is satisfied.

Criterion 3: Documentation

*Criterion:* Each issue or concern that meets or exceeds the threshold established by the design team should be entered into the system when first identified, and each action taken to eliminate or reduce the issue or concern should be thoroughly documented. The final resolution of each issue or concern should be documented in detail, along with information regarding design team acceptance.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "Availability." Westinghouse should submit WCAPs -9565, -12601, and -9817, as well as any additional documents that describe the method for documenting HFE issues as identified in this criterion. This was Open Item 18.2.3.4-3.

FSER Evaluation

The documentation of HFE issues was identified in the discussion of each HFE tracking method described in the discussion of Open Item 18.2.3.4-2 above. However, SSAR (Revision 9) Section 18.2.4, "HFE Issues Tracking," did not specifically identify what information concerning an issue is documented. It stated that design issues are entered, and that the actions taken to address the issue and the final resolution are documented. An audit of the tracking system was needed to establish the precise documentation provided for issues in the database.

As discussed in the resolution of Criterion 1 above, the staff performed an audit of the tracking system and determined that an acceptable tracking system has been established and that the general procedures described in the SSAR (Revision 23) have been acceptably implemented. Based on this information, Open Item 18.2.3.4-3 is closed and this NUREG-0711 criterion is satisfied.

Criterion 4: Responsibility

*Criterion:* When an issue is identified, the tracking procedures should describe individual responsibilities for issue logging, tracking, and resolution, as well as resolution acceptance.

*Evaluation:*

DSER Evaluation

See the previous evaluation in this section under Criterion 1, "Availability." Westinghouse should submit WCAPs-9565, 12601, and 9817, as well as any additional documents that describe the responsibilities of personnel involved in the tracking and resolution of HFE issues as identified in this criterion. This was Open Item 18.2.3.4-4.

FSER Evaluation

SSAR (Revision 23) Section 18.2.4, "HFE Issues Tracking," identified the HSI technical lead as the one central person responsible for tracking HFE issues to resolution, and indicated that the engineer responsible for each issue is identified in the database. DR issues, for example, are the responsibility of the manager who is responsible for the system under review. It is the AP600 project manager who is responsible for the overall maintenance and documentation of the tracking system. Based on this information, Open Item 18.2.3.4-4 is closed and this NUREG-0711 criterion is satisfied.

18.2.3.5 HFE Technical Program

The evaluation of the HFE technical program, as part of Element 1 of NUREG-0711, addresses scoping, resources, and management details. Actual technical details are addressed in the respective element reviews.

Criterion 1: Plans and Analyses

*Criterion:* The general development of implementation plans, analyses, and evaluation for each of the following areas should be identified and described:

- operating experience review
- functional requirements analysis and allocation
- task analysis
- staffing
- human reliability analysis (HRA)
- HSI design
- procedure design
- training program development
- human factors verification and validation

*Evaluation:*

DSER Evaluation

Westinghouse's technical program, as presented in Chapters 13 and 18 of the SSAR (Revision 0), incorporates all of the identified NUREG-0711 elements, except HRA. HRA activities are addressed in the PRA report, and other HRA-related materials (see Section 18.7 of this report). The HFE program plan should identify the interface between the HRA effort and the HFE analysis, design, and evaluation activities. This interface is not addressed in the AP600 HFE program. It is discussed in Westinghouse's response to RAI 720.117, but the programmatic relationship for information exchange is not described. For example, the use of HRA insights does not appear as an input on Figure 18.8.2-1 of the SSAR (Revision 0). Additional information on the relationship between PRA/HRA and HFE activities is needed.

Figures 18.8.2-1, 18.8.2-2, and 18.8.2-3 of the SSAR (Revision 0) identify the inputs and outputs (documentation) for the major activities of the HFE program. The documentation is complete with the following exceptions:

- OER
- HRA (see the previous discussion)
- documentation of the test and evaluation (T&E) program (e.g., test plan and reports)

Additional information on the documentation requirements for these aspects of the HFE program is needed. The staff requested Westinghouse to describe the programmatic relationship between the HFE program and PRA/HRA related activities, as well as the HFE program documentation for OER, HRA, and T&E activities. This was Open Item 18.2.3.5-1.

FSER Evaluation

SSAR (Revision 23) Section 18.2.5, "Human Factors Engineering Technical Program and Milestones;" SSAR (Revision 23) Figure 18.2.3, "Overview of the AP600 HFE Process;" and an individual section of Chapter 18 addressed this issue. HRA has been identified as part of the HFE effort. The relationships between the technical program elements and their technical outputs were identified. Based on this information, Open Item 18.2.3.5-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: HFE Requirements

*Criterion:* The HFE requirements imposed on the design process should be identified and described. List the standards and specifications that are sources of HFE requirements.

*Evaluation:*

DSER Evaluation

HFE requirements are addressed in numerous places in the SSAR (Revision 0), and the definition of HFE requirements is a major activity of the HFE program. Section 18.8 of the SSAR

lists the requirements to be identified in the HFE program. The requirements will flow from the function-based task analysis, as illustrated in Figure 18.8.2-1 of the SSAR (Revision 0). The general requirements for the major HFE resources are described in Section 18.9 of the SSAR (Revision 0).

Section 18.8.2.1.3 of the SSAR (Revision 0) states that guidance documents are provided to designers of the alarm system; the information display system; the controls interface; and the workstation and control room layout, arrangement, and environment. Figure 18.8.2-1 of the SSAR (Revision 0) (see Westinghouse's response to RAI 620.59) identifies a set of six guideline documents, including alarm guidelines, display guidelines, controls guidelines, training guidelines, anthropometric guidelines, and guidelines for integration of subsystems. In its response to RAI 620.59, Westinghouse stated that the guidance will be developed from existing guideline documents, supplemented as necessary "to address issues that are not covered sufficiently." The guidance will be "tailored to the AP600 interface," and "may include guidance and principles developed from Westinghouse human factors research." Guidance for procedures is addressed in Section 18.9.8 of the SSAR (Revision 0). Included in the referenced documents are RG 1.33, NUREG-0899, Supplement 1 to NUREG-0737, and NUREG-1358. A more detailed evaluation of the guidelines used as part of the AP600 design process is provided in Sections 18.8.3 and 18.9.4 of this report.

FSER Evaluation

SSAR (Revision 23) incorporates references to the HFE requirements in several places (e.g., Section 18.2.7; 18.4.2; 18.8; WCAP-14644, Revision 0; WCAP-14396 (Revision 2)). Based on this information, this NUREG-0711 criterion is satisfied.

Criterion 3: Facilities and Tools

*Criterion:* HFE facilities, equipment, tools, and techniques (such as laboratories, simulators, and rapid prototyping software) to be used in the HFE program should be specified.

*Evaluation:*

DSER Evaluation

Westinghouse provided an acceptable description of the facilities, equipment, tools, and techniques supporting the HFE program. For example, Section 18.6.4 of the SSAR (Revision 0) identifies the software supporting the functional task analysis; the Westinghouse response to RAI 620.15 describes the use of UNIX and DOS databases to support the design and documentation; and Sections 18.5 and 18.8 of the SSAR (Revision 0) identify the test requirements for mockups, prototypes, and simulation, including the fidelity requirements of each test.

FSER Evaluation

SSAR (Revision 23), Section 18.2.3.2, "Process Management Tools," provides a description of a design database and tracking system that are used to facilitate communications across AP600 design disciplines and organizations. In WCAP-14401 (Revision 3), "Programmatic Level

Description of the AP600 Human Factors Verification and Validation Plan," Westinghouse identifies the use of various tools to evaluate dynamic task performance, supported by further detailed descriptions in WCAP-14701 (Revision 1), "Methodology and Results of Defining Evaluation Issues for the AP600 Human Systems Interfaces Design Test Program," and WCAP-14396 (Revision 2), "Man-in-the-Loop Test Plan Description." Based on this information, this NUREG-0711 criterion is satisfied.

18.2.4 Conclusions

The objective of the HFE program management review is to ensure that the applicant has described an adequate HFE program plan and a qualified HFE design team to implement the plan. The plan should describe the technical program elements ensuring that all aspects of the HSI are developed, designed, and evaluated based on a structured, top-down systems analysis using accepted HFE principles. The staff reviewed Westinghouse's HFE program management at a complete element review level. That is, finished products from the element are available for review. The SSAR provides an acceptable basis for a human factors program plan. Westinghouse has acceptably completed this NUREG-0711 element. The COL applicant referencing the AP600 certified design is responsible for the execution of the NRC approved human factors engineering program. This is COL Action Item 18.2-1.

18.3 Element 2: Operating Experience Review

18.3.1 Objectives

The objective of the staff's review of the AP600 operating experience review (OER) is to ensure that the applicant has identified and analyzed HFE-related problems and issues encountered in previous designs that are similar to the design under review so that they are not repeated in the development of the current design or, in the case of positive features, to ensure their retention.

18.3.2 Methodology

18.3.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-13559 (Revision 0) dated December 10, 1992
- WCAP-14075 (Revision o) dated May 20, 1994
- WCAP-14644 (Revision 0) dated October 9, 1996
- WCAP-14645 (Revision 1) dated October 17, 1996
- WCAP-14645 (Revision 2) dated January 1, 1997
- WCAP-14477 (Revision 1) dated May 7, 1997

18.3.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 2, "Operating Experience Review," of NUREG-0711. The staff reviewed Westinghouse's OER at a complete element review level. That is, finished products from the element were available for review using NUREG-0711 criteria.

18.3.2.3 DSER Item Resolution

To address the Element 2 DSER open items, Westinghouse submitted draft WCAP-14645 (Revision 0), "Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant," dated May 10, 1996. Westinghouse also submitted draft WCAP-14644, "AP600 Functional Requirements Analysis and Function Allocation," dated May 1996. These documents were reviewed and the DSER open items re-evaluated based upon their contents. The results of this review were documented in a letter from the NRC to Westinghouse dated August 12, 1996.

The August 12, 1996, letter was clarified during a conference call between the NRC, Westinghouse, and BNL on September 17, 1996. Westinghouse then responded with letter NSD-NRC-96-4845, dated October 17, 1996. Included with this letter was WCAP-14645 (Revision 1), "Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant." Also considered in this review was Section 18.3 of the SSAR (Revision 14). These new documents were reviewed and the DSER open items re-evaluated based upon their contents. The results are described below.

In response to the staff's evaluation of Element 2 submitted to Westinghouse on December 4, 1996, the staff conducted additional discussions with Westinghouse on December 9 and 11, 1996. On December 16, 1996, Westinghouse submitted a letter, "Progress Towards Resolving Element 2 and 4 Open Items for AP600." On December 20, 1996, Westinghouse submitted SSAR Revision 10 to the NRC and, on January 6, 1997, they submitted WCAP-14645 (Revision 2) to address the open issues that remained from the staff's December 4, 1996, review. The results of the staff's review of Westinghouse's latest submittals are described below.

18.3.3 Results

18.3.3.1 Scope

Criterion 1: Predecessor Plant and Systems

*Criterion:* The OER should include information pertaining to the human factors issues related to the predecessor plant(s) or highly similar plants and plant systems.

*Evaluation:*

DSER Evaluation

Section 18.9.8.1.1 of the SSAR (Revision 0), WCAP-14075, and the Westinghouse responses to RAI 440.32 and RAI 620.89 discuss the Westinghouse low-pressure reference plant. WCAP-14075 provided a comparison between the AP600 and the low-pressure reference plant, and documents the major functional, system, and I&C similarities with the AP600 design. This low-pressure reference plant is a composite consisting of 25 (or 26) separate systems, having generic applicability to a broad range of Westinghouse pressurized-water reactor (PWR) plants. It is not clear from the documentation how to apply this concept to the OER. The documentation

provided by Westinghouse did not clearly address whether the operating experience of a given selected plant or type of plant was reviewed (as predecessors to the AP600) for the OER or whether experience was reviewed at the systems level, considering the 25 (or 26) systems that comprise the low-pressure reference plant. Tables 1 and 4 of WCAP-14075 could potentially be used for this type of process.

Particular attention should be given to operating experience at predecessor plants. If the design is considered to be completely new (without any predecessor), more emphasis must be given in the design stage to prototyping, trade studies, and validation testing. A new plant without any predecessor has implications for underlying assumptions that impact the staffing, training, and procedures.

Westinghouse should describe how they will apply the low-pressure reference plant concept to the OER, and then apply it appropriately in the performance of a review of operating experience. This was Open Item 18.3.3.1-1.

FSER Evaluation

In Section 1.4.2 of WCAP-14644 (Revision 0) Westinghouse clarified the predecessor plant for the AP600 as "the generic PWR design for currently licensed Westinghouse nuclear power plants." Table 1 illustrates in detail how the Critical Safety Functions for the AP600 are the same as for current Westinghouse PWR plants. The other portions of this WCAP then illustrate the differences between the predecessor plants and the AP600. Thus, current Westinghouse PWRs, in general, serve as the predecessor for the AP600 nuclear power plant.

In the AP600 OER, Westinghouse addressed current Westinghouse PWRs. This is illustrated in WCAP-13559 (Revision 0), as well as the additional documents listed in the Westinghouse response to RAI 620.53. Further, WCAP-14645, as noted in Section 2.0 of that WCAP, includes both Westinghouse and non-Westinghouse PWRs. It also addresses pertinent boiling-water reactor (BWR) issues and a pressurized heavy-water reactor, where applicable to the AP600 design. Thus, Westinghouse has included information in their OER pertaining to the human factors issues related to both the AP600 predecessor plant(s) and highly similar plants and plant systems. Based on this information, Open Item 18.3.3.1-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: Recognized Industry HFE Issues

*Criterion:* Appendix B of NUREG-0711 describes recognized nuclear power industry issues, organized into the following categories:

- unresolved safety issues (USIs)
- generic safety issues (GSIs)
- Three Mile Island (TMI) issues
- NRC generic letters (GLs) and information notices (INs)
- studies by the NRC Office of Analysis and Evaluation of Operational Data (AEOD)
- low power and shutdown issues
- operating plant event reports

In addition, TMI Item I.C.5 of NUREG-0737 was included as an HFE issue.

*Evaluation:*

DSER Evaluation

The Westinghouse documents listed in Section 18.3.2.1 of this report, as well as the additional documents listed in the Westinghouse response to RAI 620.53, indicated that the overall approach to an OER for review of recognized industry issues appeared to be thorough. Westinghouse performed extensive literature reviews and has maintained up-to-date knowledge of advanced systems and HSI research and experience. Further, it appeared that Westinghouse has, to some extent, addressed each of the categories listed above.

The staff reviewed the Westinghouse documents to determine if individual issues within these categories were adequately treated. The review was somewhat difficult to conduct because the information was distributed across several documents and was not very detailed. In particular, much of the discussion of how these industry issues are addressed in the AP600 design was presented as systems-related descriptions and did not address human factors or operator performance issues. Westinghouse has not provided a consolidated OER that discusses these issues in detail.

As examples of the above-noted lack of human factors detail for industry issues, a discussion of the review of one item from each category is provided below. These items are only examples, and Westinghouse should ensure that the OER addresses the human factors aspects of the issues identified in Appendix B of NUREG-0711, and those issues in Chapter 20 of this report that are related to human factors engineering.

- USIs - USI A-47, "Safety Implications of Control Systems," relates to the implications of failures of non-safety-related control systems and their interaction with the control room operators. Chapter 1 of the SSAR only discusses the I&C aspects, and does not discuss how the AP600 design will help the operators in the event of a loss or failure of non-safety-related control systems. Sections 7.1.3 and 7.7 of the SSAR discuss the AP600 control systems, but from an I&C perspective only. The level of automation appears to be higher than in current plants, and the type of controls differ in that they are primarily soft controls. An operator in the AP600 MCR will be more of a supervisory controller and plant monitor than in current plants. On a loss of portions (or all) of the automatic control systems, the operator will have to have an accurate understanding of the plant's status, and will then make the transition to an active controller under conditions that may be much less than optimal because of a loss of indications and a plant transient in progress. This transition was problematic in current plants, and will be different and potentially more difficult in the AP600. The human factors aspects of USI A-47 were not discussed in the Westinghouse documentation reviewed by the staff.

- GSIs - GSI-57, "Effects of Fire Protection System Actuation," addresses spurious and inadvertent actuations of fire protection systems. Such actuations have often been caused by operator errors during testing or maintenance. There does not appear to be any discussion of the ways in which the AP600 HSI will help to minimize these problems.

- TMI Issues - 10 CFR 50.34(f)(2)(vi), "Venting of Noncondensible Gases (II.B.1)," addresses the capability to vent gases from the reactor coolant system. Plant operators should be capable of monitoring the status of noncondensible gases in the reactor coolant system, and should have clear, unambiguous indication of the conditions under which gas release must be initiated. They should then be able to easily control any necessary venting. The discussion of human factors or HSI issues associated with this operation in Chapter 1 and Section 5.4.12 of the SSAR is very limited, and should be expanded to address these issues.

- NRC generic letters - In GL 91-06, "Resolution of Generic Issue A-30, 'Adequacy of Safety-Related dc Power Supplies,' Pursuant to 10 CFR 50.54(f)," the NRC outlines certain monitoring, surveillance, and maintenance provisions for safety-related direct current (dc) systems. Westinghouse addresses this item in Chapter 1 and Section 8.3.2 of the SSAR; however, not all of the items identified in Enclosure 1 to the generic letter were addressed. The control room design does not appear to contain all of the listed, separately and independently annunciated, alarms and indications. Also, the presence of bypassed and inoperable status indication for circuit breakers and other devices could not readily be verified. There are many recommendations for maintenance, surveillance, and test procedures. Some means for tracking these recommendations needs to be established, because these procedures are not yet written for the AP600. One method is the HFE issues tracking system.

- NRC Information Notices - IN 93-47, "Unrecognized Loss of Control Room Annunciators," and 93-81, "Implications of Engineering Expertise on Shift," have not been addressed in the documentation reviewed to date.

- AEOD studies - Westinghouse has reviewed a number of AEOD reports as listed in WCAP-13559. These reports were judged by Westinghouse either to be not applicable to the AP600 design, or to pertain to a section of the SSAR other than Chapter 18 (except one 1989 report that did pertain to Chapter 18). NUREG-1275 summarizes a number of earlier AEOD studies in the human performance area. This report should be carefully reviewed by Westinghouse and applied to the AP600 design.

- Low power and shutdown issues - A current area of active NRC work is that of the risk associated with operation during low power and shutdown. The NRC has identified the operator-centered and human factors issues as particularly important in this area. The current status of these issues is contained in NUREG-1449. The applicant has referred to a Westinghouse low power and shutdown report, but that report was unavailable to the staff in time to support this stage of the review.

- Industry-based operating experience documents - In its response to RAI 620.04, Westinghouse indicated that it has reviewed some Institute for Nuclear Power Operations (INPO) documents that provide an important insight into operating experience as they apply to advanced reactors. However, the results of the Westinghouse review of these documents were not submitted to the staff in time to support this stage of the review.

Before preparing the final SSAR, Westinghouse should ensure that the OER addresses the human factors aspects of all issues identified in Appendix B of NUREG-0711 and additional

HFE-related operating experience issues (e.g., NRC Bulletins and GLs) identified in Chapter 20 of this report. This was Open Item 18.3.3.1-2.

FSER Evaluation

As noted in the DSER evaluation, Westinghouse performed a thorough review of various industry issues that would have pertinent operating experience to the AP600. They performed extensive literature reviews and have continued to maintain an up-to-date knowledge of advanced systems and HSI research and experience, as illustrated by their reference lists contained in WCAP-14645 (Revision 2). However, the original documentation submitted was lacking with respect to how the human factors and operator performance aspects were reviewed and addressed. As a result, Westinghouse developed WCAP-14645 (Revision 2) to address this concern. Table 1 of the WCAP provides a detailed summary of the results of the Westinghouse OER relative to the industry operating experience issues identified in NUREG-0711, Appendix B. Specifically, Table 1 of WCAP-14645 (Revision 2) addresses Appendix B, Sections B.1-USIs/GSIs, B.2-TMI Issues, B.3-NRC Generic Letters and Information Notices, and B.4-AEOD Studies. Table 1 also covers B.5-Low-Power and Shutdown Issues and B.6-Operating Plant Event Reports by addressing the BNL Technical Report E2090-T4-3-1/95, "HFE Insights for Advanced Reactors Based Upon Operating Experience."

In Table 1, Westinghouse discusses how the human factors/human performance issue is addressed by the AP600 design. The table also identifies whether the item is: (1) not applicable to the AP600, (2) input into the Design Issues Tracking System, or (3) the responsibility of the COL. The staff reviewed Section 3.0 and Table 1 of the draft WCAP-14645 to determine if Westinghouse had satisfactorily addressed each of the issues listed in Appendix B of NUREG-0711. Table 18.3-1 lists the results of this review.

Based on this review, the staff considered it necessary for Westinghouse to do additional work on the 21 items in the last column. Westinghouse performed additional analysis and documented it in WCAP-14645 (Revision 1), the Westinghouse OER Report. The staff's concerns with the draft WCAP-14645 and the status of this open item, based on the staff's review of WCAP-14645 (Revision 1), are discussed below.

For ten of these 21 items the draft WCAP-14645 referred only to the general HSI design process and did not tie the process to the specific issue being described or provide tracking to later ensure that the process had in fact addressed the issue. These ten items are Table 1, Item 43 (TMI item 2xxi); Table 2, ref. 2.1, items 4, 6, and 7, and Ref. 2.2, items 1 through 4; and Table 3, Ref. 3.3, items 1 and 2. For two of these items (Table 1, Item 43 and Table 2, Ref. 2.1, Item 6) WCAP-14645 (Revision 1) provides additional satisfactory information; for the other eight items, Westinghouse incorporated each issue into the Design Issues Tracking System. This approach is acceptable.

The additional 11 items in the "Not acceptably Addressed" column were:

| | |
|---|---|
| USI/GSIs: | 1 (A-44), 2 (A-47), 4 (B-32), 7 (GI-51), 20 (GI-130) |
| TMI items: | 35 (2v), 37 (2xi), 46 (2xxvii) |
| BNL OER Report: | 78, 157, 165 |

Of these 11 items, nine have been acceptably addressed by WCAP-14645 (Revision 1). Two items, 7(GI-51) and 165, remained open. Each of these items is discussed below.

- Item 1 (A-44) - WCAP-14645 (Revision 1) provides a significant amount of detail on the AP600 design to address station blackout (SBO). The passive systems provide the main defense against SBO, with a one-time realignment of valves. Regarding monitoring instrumentation, the qualified data processing system (QDPS) is powered from a Class 1E dc UPS with sufficient battery capacity for 72 hours. More detail on the DC power system is provided in SSAR Section 8. As a result of the additional information provided by Westinghouse in WCAP-14645 (Revision 1) related to the AP600 SBO and associated human performance issues, this item is acceptably addressed.

- Item 2 (A-47) - Specific issues were noted in DSER Open Item 18.3.3.1-2, A-47. The draft WCAP-14645 discussed the reliability and diversity of the plant control system, which is also described in the SSAR. WCAP-14645 (Revision 1) discussed analyses performed in WCAP-14477 (Revision 1), "Adverse Systems Interactions Report," related to plant control system failures, and the emergency response guidelines (ERGs), which provide contingency actions for system failures, including control systems. The discussion of system interactions provided in WCAP-14477, which include human performance and interface with plant equipment, together with the application on ERGs, satisfactorily respond to the staff's previous concern in the DSER that human factors aspects of this issue were not discussed by Westinghouse. Based on the information provided in the above-mentioned WCAPs, this item is acceptably addressed.

- Item 4 (B-32) - The draft WCAP-14645 stated that this item was N/A because service water in the AP600 design is non-safety-related. WCAP-14645 (Revision 1) stated that the Service Water System temperature is monitored and alarmed in the control room on low temperature. This provides a warning of potential icing conditions. This item is acceptably addressed.

- Item 7 (GI-51) - The draft WCAP-14645 did not address the instrumentation to be used by operators for monitoring for the buildup of clams, mussels, and corrosion products. GI-51 also references GL 89-13, which has more detail about the testing and instrumentation needed to ensure continued operability of open cycle service water systems. This item was not adequately addressed by WCAP-14645 (Revision 1) or for Chapter 18 of the SSAR (Revision 9).

- Item 20 (GI-130) - A potential for applicability to single unit sites was noted in Appendix B of NUREG-0711, but was not addressed by the draft WCAP-14645. WCAP-14645 (Revision 1) addresses internal cross ties for a single unit AP600. This item is acceptably addressed.

- Item 35 (2v) - This item deals with automatic indication of bypassed and inoperable systems, which is an important aspect of the operators' situation awareness. The draft WCAP-14645 only addressed protection systems, which was too narrow of an interpretation, because the item relates more generally to safety systems. WCAP-14645 (Revision 1) generally discussed the manner in which the AP600 provides for situation awareness, including the wall panel information system and bypassed and inoperable systems information. SSAR Revision 9, in Sections 1.9.3 (2v) and 1A, states that the

AP600 meets all the recommendations of RG 1.47 for bypassed and inoperable indication of plant safety systems. This item is acceptably addressed.

- Item 37 (2xi) - WCAP-14645 (Revision 1) clarified that the indication provided for safety/relief valves is "direct." This, together with the added discussion for this item in WCAP-14645 (Revision 1) acceptably addresses this item.

- Item 46 (xxvii) - WCAP-14645 (Revision 1) discussed the broad range of routine and accident conditions that are addressed by the radiation monitoring system (RMS). It also discusses how the RMS is integrated into the control room displays. This item is acceptably addressed.

- Item 78 - This item addresses change in control modes during transient situations. WCAP-14645 (Revision 1) discussed an example new system and new automation that will help in this area. The WCAP also discussed the use of the function-based task analyses to assist in the design in this area. Further, the AP600 design has an operator alert when a control system switches from automatic to manual. In this case, the computerized alarm response procedure will provide the operator with prompt access to the associated soft control. This item is acceptably addressed.

- Item 157 - WCAP-14645 (Revision 1) adequately addressed this item for all noted systems' heat exchangers with the exception of the open cycle service water system. The service water system is covered by item 7 above. This item is acceptable.

- Item 165 - This item relates to local valve position indication (VPI). NUREG/CR-6146 found that many manual valves, even those found to be the most risk-significant manual valves, lacked local position indication. Without such explicit indication, the position of the valve is inferred from stem position (for rising stem valves) or determined by checking the valve in the closed direction. Both methods have potential problems, as discussed in the NUREG/CR. OER also identified incidents that were caused by poor or missing local VPI. Valve manufacturers reported that the cost of providing a position indicator on a new valve was relatively small, whereas the costs of backfitting such indication on in-place valves would vary considerably and could be prohibitive. Thus, while adding position indication in an existing plant might only be feasible for a selected set of valves, it could be specified for many (or all) valves in the design of a new plant for relatively low cost. It should be noted that the nature of the position indication should be appropriate to the use of the valve. WCAP-14645 (Revision 1) only commits to local VPI for valves "where appropriate" and states that "most valves" will show their position by their mechanical properties. This item was not acceptably addressed.

Additional information addressing the staff's concerns for the items 7 and 165 above was required from Westinghouse.

During the review of draft WCAP-14645, the staff reviewed only 50 percent of the items from the BNL OER report and three were found to be inadequately addressed. As a result, in the August 12, 1996, letter from the NRC, the staff asked Westinghouse to review the remaining items in WCAP-14645 that responded to this report and correct any with deficiencies similar to

those noted for items 78, 157, and 165 above. Revision 1 of the WCAP did not appear to have addressed this item.

The staff also noted that Westinghouse should explain how they will assure that all of the items noted as COL responsibility will be effectively and specifically transferred over to the COL. In Section 3.0 of WCAP-14645 (Revision 1), Westinghouse summarized the 17 items from Table 1 that are totally or partially the responsibility of the COL. The exact transfer mechanism was not specified.

Still open on this item were items 7 and 165, re-review by Westinghouse of 50 percent of the BNL report items, and describing the COL transfer mechanism.

Based on concerns identified by the staff in their evaluation of WCAP-14645 (Revision 1) and provided to Westinghouse on December 4, 1996, the staff conducted additional discussions with Westinghouse on December 9, 1996, and December 11, 1996. Westinghouse submitted a letter on December 16, 1996; SSAR (Revision 10) on December 20, 1996; and WCAP-14645 (Revision 2) on January 6, 1997, to address the open issues that remained from the staff's review of WCAP-14645 (Revision 1). WCAP-14645 (Revision 2), transmitted on January 6, 1997, acceptably addressed the staff's concerns related to items 7 and 165. Specifically, WCAP-14645 described instrumentation related to monitoring for build-up of clams, mussels, and corrosion products which addressed the staff's concerns related to item 7. In addition, WCAP-14645 satisfactorily addressed the staff's concern related to item 165 by citing an AP600 valve design specification which identifies certain valves requiring local position indication and further specifies that manual valves identified as risk-significant will have valve position indication. In WCAP-14645 (Revision 2), Westinghouse stated that they had reviewed the remaining 50 percent of the items from the BNL OER report and had determined that there were no additional deficiencies, which satisfied the staff's request for a complete review of the BNL OER report items. In SSAR Revision 14, Westinghouse acceptably addressed the staff's concern for the transfer mechanism specifying where the COL action items in the OER report are identified in the SSAR. Additional information related to the staff's evaluation of generic issues pertaining to human factors engineering can be found in Chapter 20 of this report. Based on this information, Open Item 18.3.3.1-2 is closed and this NUREG-0711 criterion is satisfied.

Criterion 3: Related HSI Technology

*Criterion:* The OER should address related HSI technology. For example, if touch screen interfaces are planned, HFE issues associated with their use should be reviewed.

*Evaluation:*

DSER Evaluation

Westinghouse will use some HSI technologies that are not typically used in currently operating nuclear plants (e.g., large screen displays and touch screens). A comprehensive list is needed of the new HSI technologies planned for use in the AP600 design; then pertinent HFE issues may be reviewed and addressed, as appropriate. The staff recognizes that Westinghouse is aware of research in this area and activities associated with HSI technology in other industries (see Westinghouse's response to RAI 620.53). Further, Westinghouse has proposed V&V evaluations (in Section 18.5 and Table 18.8.2-1 of the SSAR) that would help to address these

issues. However, the materials received from Westinghouse before preparing this report did not directly address this aspect of the OER. Westinghouse should describe how they have included related HSI technologies in the OER. This was Open Item 18.3.3.1-3.

FSER Evaluation

Draft WCAP-14645 addresses this criterion in Section 4.0, "Related Human System Interface (HSI) Technologies Where Little or No Nuclear Plant Experience Exists," and in Table 2. The WCAP identifies three such HSI technologies for use in the AP600, which are soft controls, computerized procedures, and large screen (wall panel) displays. Westinghouse reviewed the operating experience of soft controls and large overview type displays to identify human factors issues. There are 38 identified issues from these two areas listed in Table 2 of the WCAP. However, in the draft OER there was no information related to operating experience in the area of computerized procedures. A review of Table 1 and the information provided for procedure-related items indicated that Westinghouse had performed some such reviews. In WCAP-14645 (Revision 2), Westinghouse clarified this by adding a discussion in Section 4.0 about the AP600 computerized procedure system (CPS). This states that the AP600 CPS is dynamic and interactive with the remaining AP600 HSI. No comparable system with relevant operating experience was found in other industries. If any such experience is published, Westinghouse has committed to reviewing it and identifying any human factors issues to be addressed.

Additionally, there were nine issues in Table 2 of the draft WCAP that required further information from Westinghouse. These items were satisfactorily addressed in WCAP-14645 (Revision 2), as discussed in the above item. Also, in Section 4.0 of WCAP-14645 (Revision 2), Westinghouse summarized the seven items from Table 2 that are the responsibility of the COL applicant. Based on this information, Open Item 18.3.3.1-3 is closed and this NUREG-0711 criterion is satisfied.

Criterion 4: Operator Interviews

*Criterion:* Operator interviews should be conducted to determine operating experience related to predecessor plants or systems. The following topics should be included in the operator interviews:

- plant operations
  - normal plant evolutions (e.g., startup, full power, and shutdown)
  - instrument failures (e.g., safety-related system logic and control unit, fault tolerant controller for NSSS, local "field unit" for multiplexer (MUX) system, MUX controller for balance of plant, and break in MUX line)
  - HSI equipment and processing failure (e.g., loss of video display units, loss of data processing, and loss of large overview display)

- transients (e.g., turbine trip, loss of offsite power, station blackout, loss of all feed water, loss of service water, loss of power to selected buses and control room power supplies, and safety/relief valve transients)

- accidents (e.g., main steamline break, positive reactivity addition, control rod insertion at power, control rod ejection, anticipated transient without scram, and loss-of-coolant accidents of various sizes)

- reactor shutdown and cooldown using the remote shutdown system

• HFE/HSI design topics

- alarm/annunciation
- display
- control and automation
- information processing and job aids
- real-time communications with plant personnel and other organizations
- procedures, training, staffing, and job design

*Evaluation:*

DSER Evaluation

Westinghouse's responses to RAI 620.12 and RAI 620.52 discussed some of the interviews that have been conducted by Westinghouse to date. Complete documentation of the content and results of the interviews have not yet been made available to the staff. The references contained in the response to RAI 620.52 contain some advanced and potentially applicable material in this area; however, Westinghouse should relate the work discussed in these papers and reports to the AP600 design. Further, the appropriateness of the subjects and the content of the interviews must still be determined after the information discussed for Criterion 1 ("Predecessor Plant and Systems") and Criterion 3 ("Related HSI Technology") of this section is provided. Westinghouse should provide the content and results of the operator interviews to the staff and demonstrate how they address this criterion. This was Open Item 18.3.3.1-4.

FSER Evaluation

WCAP-14645 (Revision 1) addresses operator interviews in Section 5.0 and Table 3. Westinghouse states that interviews have been conducted during plant operations and after events. Eight specific reports are cited that document the operator interviews. These reports are two NUREG/CRs, two Westinghouse proprietary reports, one Westinghouse non-proprietary WCAP, one EPRI report, one utility (PG&E) letter, and one Canadian report. The staff reviewed these reports to determine the scope of the operator interviews. All of the topics above were addressed to some extent in the eight reports, with the exception of remote shutdown and staffing. A number of issues were identified based on the interviews, as documented in Table 3 of the WCAP. The issues cover many areas including emergency situations, cognitively demanding situations, procedures, soft controls, alarms and alarm systems, SPDS, plant startup, and feedwater control. The Westinghouse treatment of the issues is primarily based on references to earlier information in the OER report. Westinghouse should discuss how the

issues identified in column 2, Table 3, were selected (and the criteria used to determine their applicability to the AP600 design) from the numerous issues covered by the eight reports.

This item remained open pending Westinghouse's response to the two topics not addressed in the scope of the interviews (remote shutdown and staffing) and a discussion of how issues were selected from the eight reports for inclusion in column 2, Table 3 of WCAP-14645 (Revision 1).

Based on concerns identified by the staff in their evaluation of WCAP-14645 (Revision 1) which were provided to Westinghouse on December 4, 1996, the staff conducted additional discussions with Westinghouse on December 9, 1996, and December 11, 1996. Westinghouse submitted a letter on December 16, 1996, and WCAP-14645 (Revision 2) on January 6, 1997, to address the open issues that remained from the staff's review of WCAP-14645 (Revision 1). Enclosure 1, "AP600 Open Item Tracking System: Design Issues Tracking," item number 4179, of the Westinghouse December 16, 1996, letter acceptably addressed the staff's concerns related to the scope of operator interviews. Specifically, WCAP-14645 (Rev. 2) provided an explanation of how the operator interview issues were selected and Item # 4179 of Westinghouse letter dated December 6, 1996, provided a commitment to address operator interviews on the topics of remote shutdown and staffing. Based on this information, Open Item 18.3.3.1-4 is closed and this NUREG-0711 criterion is satisfied.

18.3.3.2 Issue Analysis, Tracking, and Review

Criterion 1: Analysis Content

*Criterion:* Issues should be analyzed with regard to the identification of the following:

- human performance issues, problems, and sources of human error
- design elements that support and enhance human performance

*Evaluation:*

DSER Evaluation

The review process discussed in Section 18.3 of the SSAR (Revision 0) and the Westinghouse response to RAI 620.41 appears thorough and generally addresses the criterion. However, from the review of a number of items, summarized in Section 18.3.3.1, "Criterion 2: Recognized Industry HFE Issues," of this report, it appears that the OER performed to date did not sufficiently analyze the experience with regard to these criteria. As the OER is completed, Westinghouse should ensure that these aspects are addressed and documented in the OER review. Westinghouse should describe how the OER will address issues related to human performance and problems and sources of human error. In addition, Westinghouse should describe how the HFE design addresses the issues raised by the OER. This was Open Item 18.3.3.2-1.

FSER Evaluation

In draft WCAP-14645, Westinghouse identified human performance issues and problems, and sources of human error. They also identified the various aspects of the AP600 design and

design process that will address these problems by supporting and enhancing human performance. During review of the draft OER a small percentage of the responses to the issues were identified by the staff for further follow up by Westinghouse; however, those responses appeared to be the exception to a well-researched and thorough analysis. Furthermore, Westinghouse reanalyzed those responses identified by NRC as needing follow up and documented the results in WCAP-14645 (Revision 1). All but two of the issues were satisfactorily resolved with the submission of WCAP-14645 (Revision 1). These two items (7, 165) needing further follow up were tracked by another open item.

Additionally, in Section 1 of WCAP-14645 (Revision 2), Westinghouse stated that they will continue to review current plant operating experience and as new HFE issues are identified, they will address and track to resolution those issues applicable to the AP600. Based on this information, Open Item 18.3.3.2-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: Documentation

*Criterion:* The analysis of operating experience should be documented in an evaluation report.

*Evaluation:*

DSER Evaluation

From the review performed on the documentation received before preparing this report, it appears that the OER had not yet been fully completed or documented into one integrated report. As an example, WCAP-13559 discusses many industry documents that were reviewed, but little detail is provided and it is not clear how or if Westinghouse used the results of this review for the AP600 HFE design. Westinghouse should provide an OER report that adequately documents the results of the reviews and how the findings are (or will be) addressed by the AP600 design. This was Open Item 18.3.3.2-2.

FSER Evaluation

As described in the above sections, Westinghouse consolidated their operating experience review work into a single document, WCAP-14645 (Revision 2) titled, "Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant." This report addresses all of the areas and issues identified in NUREG-0711, Appendix B, as well as the additional related industry issues in BNL Technical Report E2090-T4-3-1/95, "HFE Insights for Advanced Reactors Based Upon Operating Experience." Also, see the staff's evaluation of HFE-related issues in Chapter 20 of this report. Based on this information, Open Item 18.3.3.2-2 is closed and this NUREG-0711 criterion is satisfied.

Criterion 3: Incorporation into the Tracking System

*Criterion:* Each operating experience issue determined to be appropriate for incorporation into the design (but not already addressed in the design) should be documented in the HFE issue tracking system.

*Evaluation:*

DSER Evaluation

As discussed in Section 18.2.3.4 of this report, Westinghouse had not yet described an acceptable HFE issues tracking system (Open Item 18.2.3.4-1). Additionally, this tracking system should already have items pertinent to the AP600 design entered into it. For example, the tracking system should include human factors items or issues that were identified during the development of the OER, but for which design (or procedural) resolutions have yet to be determined. The maintenance and testing issues noted in GL 91-06 and discussed in Section 18.3.3.1 of this report are examples of this type of issue. Therefore, any identified items that have not been incorporated into the design documentation in some fashion should be entered into the HFE issues tracking system when the OER is completed. Westinghouse should describe how each operating experience issue determined to be appropriate for incorporation into the design is entered into the system. This was Open Item 18.3.3.2-3.

FSER Evaluation

Westinghouse should provide the staff with evidence that the tracking system has been successfully implemented for HFE issues. At a minimum, database entries that have been made by Westinghouse to date, for those HFE issues that require tracking, should be provided for staff review. Related design file documents that support the database entries should be provided for a sample of the HFE entries that have been made to date in the database.

Based on concerns identified by the staff in their evaluation of WCAP-14645 (Revision 1) which were provided to Westinghouse on December 4, 1996, the staff conducted additional discussions with Westinghouse on December 9, and 11, 1996. Westinghouse submitted a letter on December 16, 1996, and WCAP-14645 (Revision 2) on January 6, 1997, to address the open issues that remained from the staff's review of WCAP-14645 (Revision 1). In their December 16, 1996, letter, Westinghouse acceptably addressed the staff's request for entries of HFE issues that have been included in the HFE Issues Tracking System as evidenced by Enclosures 1 through 3. Enclosure 1 provided a copy of the design issues tracking system database report for HFE issues identified as a result of the operating experience review. Enclosure 2 was a copy of the tracking system database report for HFE issues which resulted from design reviews. Enclosure 3 provided the database report for HFE issues identified by the human systems interface designers as important HSI design issues. Therefore, Open Item 18.3.3.2-3 is closed and this NUREG-0711 criterion is satisfied.

18.3.4 Conclusions

The objective of the AP600 OER review is to ensure that the applicant has identified and analyzed HFE-related problems and issues encountered in previous designs that are similar to the current design under review so that they are not repeated in the development of the current design or, in the case of positive features, to ensure their retention. The staff reviewed Westinghouse's OER at a complete element review level. That is, finished products from the element were available for review. Overall, Westinghouse has discussed a comprehensive approach to operating experience review. Westinghouse has also completed fairly extensive reviews, both in the general nuclear power experience area and in the particular area of HSI

technology. Westinghouse acceptably completed this NUREG-0711 element. Also, see the staff's evaluation of HFE-related issues in Chapter 20 of this report.

## 18.4 Element 3: Functional Requirements Analysis and Allocation

Element 3 is presented differently than the other HFE PRM elements. Because of significant changes made to the material presented by Westinghouse as part of DSER issue resolution, the staff modified its treatment of the NUREG-0711 criteria for this element. Thus, the discussion of DSER review and FSER resolution are presented in two separate sections (rather than including both within the discussion of individual NUREG-0711 criteria). The rationale for the change and relationship between the two phases of the review is discussed in Section 18.4.2.3, "DSER Item Resolution," of this report.

### 18.4.1 Objectives

The objective of the functional requirements analysis and allocation review for the AP600 is to ensure that the applicant has defined the plant's safety functional requirements, and that the function allocations take advantage of human strengths and avoid allocating functions that would be negatively influenced by human limitations.

The functional requirements and function allocations of a new design are typically based on one or more predecessor designs. Many of the functional requirements and function allocations for the new plant may be the same as those of the predecessor. This reflects the evolutionary nature of technology development in complex, high-reliability systems like nuclear power plants. In such cases, operating experience becomes an essential component of the technical basis and rationale for the functional requirements and function allocations. Functions and their allocations are described in NUREG-0711 as "modified," in comparison to the predecessor design. It is acceptable for functions and allocations that are not modified to be justified based upon the successful operating experience of predecessor designs. The review criteria below reference the concepts of unmodified and modified functions and function allocations.

### 18.4.2 Methodology

#### 18.4.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-13957 (Revision 0) dated January 1994
- WCAP-14075 (Revision 0) dated May 20 1994
- ET-NRC-92-3748 (Westinghouse letter dated September 15, 1992)
- WCAP-14644 (Revision 0) dated October 9, 1996

#### 18.4.2.2 Technical Basis

The staff focused its DSER review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 3, "Functional Requirements Analysis and Allocation," of NUREG-0711.

18.4.2.3 DSER Item Resolution

Element 3 of NUREG-0711 provides criteria for the staff's review of an applicant's functional requirements analysis and function allocation (i.e., the definition and then assignment of functions to human and automatic control systems). In the AP600 DSER review of Element 3, 14 open items were identified.

As part of a meeting held between the staff and Westinghouse on March 8 through 10, 1995, Element 3 open items were addressed. At that meeting, the staff committed to clarify its position concerning the Element 3 open items. To meet this commitment, the staff developed a document entitled "Review of the Westinghouse AP600 Functional Requirements Analysis and Function Allocation," which was transmitted to Westinghouse on May 15, 1995. The staff's report identified the information needed to address issues related to functional requirements analysis and functional allocation for the AP600. As a result of the staff's effort, the DSER open items were revised into four new open items. These four items serve as the basis for completing the Element 3 review. The new open items were developed from tailoring the generic NUREG-0711 criteria to apply to the specific circumstances of the AP600. Because the open items are being used in place of the NUREG-0711 criteria, the new open items are referred to as criteria in the evaluation below.

To provide the information requested by the staff in the May 15, 1995 letter, Westinghouse submitted draft WCAP-14644 (Revision 0), "AP600 Functional Requirements Analysis and Function Allocation," in May 1996. In addition, the staff and Westinghouse held a meeting in Rockville on May 21 and 22, 1996, during which Westinghouse provided a briefing on their approach.

The staff reviewed the Element 3 open items based on the draft WCAP provided by Westinghouse. The level at which the Element was evaluated was changed from an implementation plan review to a complete element review. The staff agreed that this was justified on the basis that the results of the functional requirements analysis and function allocation were available and documented in the WCAP. This is acceptable, though the function allocations may be somewhat modified as a result of later HFE analyses and evaluations. As with any HFE activity, it is necessary to provide a methodology that accommodates modifications as a result of new findings or later design activities. This reflects the iterative nature of design.

The results of the review of the draft WCAP-14644 (Revision 0) were documented in a letter from the NRC to Westinghouse dated August 8, 1996. By letter to the NRC dated October 9, 1996, Westinghouse responded to the open items and transmitted Revision 0 of WCAP-14644, "AP600 Functional Requirements Analysis and Function Allocation." Table 18.4-1 shows the relationship between NUREG-0711 criteria, DSER open items and the new criteria (discussed in Section 18.4.3.2 of this report).

The four new items/criteria below were slightly modified from their description in the staff's May 15, 1995 document. These changes included (1) removal of material that served as reference to the technical basis for the staff's information request (that is part of the detailed technical discussion contained in the May document and is not needed in this document), (2) cross references to other parts of the May document were changed to be correct for the present

document, and (3) slight editorial modifications. This revision of the items was transmitted to Westinghouse in the August 8, 1996, letter and is unchanged below.

18.4.3 Results

18.4.3.1 DSER Evaluation

Note that this section provides a documentation of the DSER evaluation only. Section 18.4.3.2, FSER evaluation, discusses the staff's review of the four new open items listed in Table 18.4-1.

18.4.3.1.1 General Criteria

Criterion 1: Process

*Criterion:* Functional requirements analysis and allocation should be performed using a structured, documented process reflecting HFE principles.

*Evaluation:* Sections 18.6, 18.8, and 18.9 of the SSAR (Revision 0) describe Westinghouse's approach to the AP600 functional requirements analysis. The process is based on a decision sets model that involves decomposition of plant functions from global, abstract functions, such as "prevent radiation release"; to lower level decision sets, such as "control reactor coolant system (RCS) boron concentration." For each decision set, questions are addressed that provide information for accomplishing the goal of the decision set, such as what information is needed, what decisions need to be made, and where the results must go. The results are presented in both graphic and tabular form with the aid of a computer-aided software engineering tool. At the lower levels, cognitive task analysis is performed to provide the requirements for the HSI design. The cognitive task analysis is reviewed in Section 18.5 of this report. While the analysis is performed using a structured, documented process, several questions concerning this methodology have been identified and are discussed in Section 18.4.3.2 of this report.

Section 18.8.2.1.2.4 of the SSAR provides Westinghouse's general approach to function allocation. This approach is expanded in Westinghouse's response to RAI 620.72. Westinghouse used a structured approach based on the methodology developed by the International Atomic Energy Agency (IAEA) that is described in IAEA-TECDOC-668. This document is based on the methodology developed in NUREG/CR-3331. These documents are described as appropriate sources of function allocation methodology in NUREG-0711.

Applying the methodology, Westinghouse first identified those function assignments that are mandatory (required by regulation) and assessed human performance requirements based on task characteristics. For many functions, a combination of human and automated systems are identified. A seven-level categorization scheme developed by Billings (1991) is used, and the initial set of allocations are documented. The allocations are reevaluated, iteratively, as the design becomes more detailed. Westinghouse will document modifications made to the allocations as the design process continues.

For tasks assigned to personnel, Westinghouse considers approaches to support the crew's task performance by reducing the workload. Sample techniques provided in

Section 18.8.2.1.2.4 of the SSAR (Revision 0) include synthesizing plant parameters and accessing plant data from previous operational situations that have been stored in the system.

When a task is automated, Westinghouse defines human task requirements in order for plant personnel to properly monitor the automated activities. In addition, Westinghouse provided high-level principles for making the automation "human-centered" (see Westinghouse's response to RAI 620.72). Consideration of the requirements associated with the task of monitoring automation is an especially positive aspect of the described approach.

While the general function allocation methodology is structured, documented, and based upon HFE principles, several questions concerning the details of the methodology are identified in Section 18.4.3.3 of this report. In summary, the staff concludes that the applicant's general approach to functional requirements analysis and allocation is acceptable. Questions regarding details of the methodology are identified in Sections 18.4.3.2 and 18.4.3.3 of this report, and will need to be addressed by Westinghouse.

Criterion 2: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's functional requirements analysis should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:* The AP600 functional requirements analysis was completed using typical industry practice; however, it was not clear what standards or guidelines were used to complete the analysis. The technical basis for Westinghouse's function allocation methodology is based on documents referenced in NUREG-0711, including IAEA-TECDOC-668. This is acceptable.

Westinghouse should identify the industry standards, guidelines, or practices used to perform the functional requirements analysis. This was Open Item 18.4.3.1-1.

18.4.3.1.2 Functional Requirements Analysis

Criterion 1: Safety Functions

*Criterion:* Safety functions (e.g., reactivity control) should be defined. These include functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant processes (plant system configurations or success paths)that are responsible for or capable of carrying out the function should be clearly defined.

*Evaluation:* High-level safety functions have been defined and are displayed in Figures 18.6-9 and 18.6-10 of the SSAR (Revision 0). These include the functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. Figures 18.6-9 and 18.6-10 of the SSAR (Revision 0) show the top four levels in the functional decomposition. For example, Level 1, containing "Prevention of Radiation Release," is decomposed in Level 2 into "Fuel Integrity," "RCS Boundary Integrity," etc. In Level 3, "Fuel Integrity" is decomposed into "Reactivity Balance" and "Fuel Clad Heat Balance." In Level 4, "Reactivity Balance" is decomposed into "Control Gross Reactivity" and

"Control RCS Boron Concentration." The following examples demonstrate the staff's concern with completeness:

- Level 1 of these figures only includes "Prevention of Radiation Release," and not other safety functions such as site personnel protection (e.g., from exposure to high radiation sources) or protection of the environment from various releases such as toxic chemicals. It is not clear whether these safety functions are covered in the decision sets in Figures 18.6-1 through 18.6-8 of the SSAR.

- At Level 2, the box for radioactive waste management is not developed, and it is not clear if this will include monitoring routine radioactive releases. These items should be considered because they also contribute to the specification of requirements for controls, displays, and alarms.

- At Level 4 in Figure 18.6-10 of the SSAR, it is not clear why there are no functions identified for "steam generator (SG) water inventory" and "control containment temperature."

It is not clear, based on the methodology presented, how the results are verified for completeness and accuracy.

The safety processes themselves will be defined at the next level when the function-based task analyses (FBTAs) are completed. This has been done in WCAP-13957 (Revision 0) for the one example case, which shows a reasonably detailed process that appears acceptable. A few minor items were noted and are discussed in the evaluation of Criterion 4, "Summary Description," later in this section. Westinghouse should describe the process for addressing functional analysis completeness and accuracy. This was Open Item 18.4.3.2-1.

Criterion 2: Predecessor Plant and Systems

*Criterion:* Safety functions and processes of the new plant should be compared to the predecessor plant, if applicable, to document functions and processes that are new, changed, or deleted. These should be referred to as the "modified" processes. Safety processes that have not been modified should be documented as unchanged.

*Evaluation:* Table 1 of WCAP-14075 (Revision 0) provides a comparison between the systems of the predecessor plant (the Westinghouse low-pressure reference plant) and the systems of the AP600. This information is further expanded in Table 3 of WCAP-14075 (Revision 0), with a comparison of the more detailed system design features, such as actuation signals and components. At the systems level, this type of approach appears acceptable. However, at the functional and plant process levels (see Criterion 1, "Safety Functions," earlier in this section), Westinghouse has not made a comparison between the predecessor plant and the AP600 design. Westinghouse should expand the comparison between the predecessor plant and the AP600 to include an analysis of plant safety functions and processes. This was Open Item 18.4.3.2-2.

Criterion 3: Technical Basis (Modified Processes) Documentation

*Criterion:* The technical basis for modified plant processes (e.g., rationale for a passive cooling system) should be documented.

*Evaluation:* Some information to address this criterion is contained in Chapter 1 of the SSAR and in WCAP-14075 (Revision 0); however, the relevant technical bases are not clear because Westinghouse has not clearly identified the modified processes. Westinghouse should identify and describe the basis for the modified functions and processes. This was Open Item 18.4.3.2-3.

Criterion 4: Summary Description

*Criterion:* A summary description should be provided for each plant process (unchanged or modified), and should include the following:

- purpose of the process
- conditions that indicate that the process is required
- parameters that indicate that the process is available
- parameters that indicate that the process is operating (e.g., flow indication)
- parameters that indicate that the process is achieving its purpose (e.g., reactor vessel level returning to normal)
- parameters that indicate that operation of the process can or should be terminated

Parameters may be described qualitatively (e.g., high or low). Specific data values or setpoints are not necessary at this stage.

*Evaluation:* This information will be contained in the FBTAs, when they are completed. The FBTA for Reactor Coolant System Mass Inventory (WCAP-13957, Revision 0) was reviewed as an example of Westinghouse's methodology. This document provides a basic understanding of the methodology; however, it is not complete. For example, in many instances, the information was simply listed as "later." Some specific questions were noted in the review of WCAP-13957 (Revision 0):

- Page 4 mentions an index, but it is not included.
- On page 14, there is no basic goal for high mass inventory (e.g., for CV-1, not exceeding a maximum volume that would lead to pressurizer (PZR) overfill and possibly a solid PZR). There are overfill problems in CV-2 and CV-3, also.
- Referring to Table 10-1 on page 20, there is no "ultimate cooling" injection supply as would be found in current nuclear power plants. This should be explained and justified.

- In the appendices, the function of listed valves is not always apparent, because they are not described or shown on a flow diagram.

Westinghouse should address methodological concerns to provide assurance that there are no generic problems with the analysis method. Specifically, (1) the RCS mass inventory FBTA should be completed, (2) the topical report referenced on page 4 should be included, (3) the basic goal for high mass inventory should be addressed, (4) omission of the "ultimate cooling" injection supply should be explained and justified, and (5) the function of listed valves should be provided. This was Open Item 18.4.3.2-4.

Criterion 5: Function Diagraming

*Criterion:* Safety functions should initially be described in graphic form (e.g., using functional flow block diagrams). Function diagraming should be done at several levels, starting at "top level" functions, where a very general picture of major functions is described, and continuing through the plant process level to lower levels until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or an operator). The functional decomposition should address the following levels:

- high-level functions (e.g., maintain RCS integrity) and critical safety functions (e.g., maintain RCS pressure control)
- individual plant processes
- specific plant systems and components

*Evaluation:* A method for doing this has been established and implemented as illustrated by the sample case in WCAP-13957 (Revision 0).

Criterion 6: Description

*Criterion:* Detailed narrative descriptions should be developed for each of the identified modified processes and for their relationship to the overall plant configuration design. Information provided for Criterion 4, "Summary Description," earlier in this section should be described in greater detail.

*Evaluation:* Information provided by Westinghouse in the summary description for Criterion 4 is incomplete. Westinghouse should first complete the summary descriptions, and then develop detailed narrative descriptions for each of the modified processes they identify and their relationship to the overall plant configuration design. Westinghouse should provide the detailed narrative descriptions. This was Open Item 18.4.3.2-5.

Criterion 7: Updating Requirements

*Criterion:* The functional analysis should be kept current over the life-cycle of design development and held until decommissioning so that it can be used for design when modifications are considered.

*Evaluation:* Updating of the functional analysis is not addressed in the material reviewed. Westinghouse should provide a commitment for updating the functional analysis as part of the functional analysis methodology. This was Open Item 18.4.3.2-6.

Criterion 8: Verification Requirements

*Criterion:* Verify that all of the processes necessary for achieving safe operation are identified, and all requirements of each process are identified.

*Evaluation:* See the discussion earlier in this section under Criterion 1, "Safety Functions." Westinghouse should verify that all of the processes necessary for achieving safe operation are identified and all of the requirements of each process are identified. This was Open Item 18.4.3.2-7.

18.4.3.1.3 Function Allocation Analysis

Criterion 1: Unchanged Plant Processes

*Criterion:* Plant processes that were identified as unchanged (relative to predecessor designs) should be reviewed to identify (1) those for which the control function allocation between personnel and system elements is unchanged, and (2) those for which the function allocation has changed (e.g., through the increased use of automation). This latter group is referred to here as "modified" function allocations. The level of automation should be briefly described (e.g., fully automatic, fully manual, automatic with manual backup) for each unchanged function with unchanged allocation.

*Evaluation:* As discussed under Criterion 2, "Assumptions and Constraints," in Section 18.2.3.1 of this report, the basis for the baseline function allocation for the AP600 appears to be an input to the HFE program. The design of the I&C appears to have been determined before any of the detailed HFE design program has begun. Therefore, the contributions of the HFE program to function allocation are unclear. Section 18.2.3.1 of this report provides a more detailed discussion of this concern. The basis for the initial allocation needs to be clarified (e.g., whether the basis is in terms of the operating experience of predecessor designs, or are the result of mandatory, preferential, or other allocations per the function allocation methodology described in Westinghouse's response to RAI 620.72). Changes in the level of automation from the predecessor plant need to be defined. Until such clarification, a full evaluation of this criterion could not be performed.

WCAP-14075 (Revision 0) states that "...the assumption has been made that the AP600 will have instrumentation and control similar to that of the reference plant. This information will be used as input to the task analysis as part of the man-machine interface design" (p. 38). Also, Table 4 of WCAP-14075 provides a detailed comparison showing that much of the I&C in AP600 is "similar" to the reference plant. This reinforces the concern that the design of the I&C is already predetermined before any of the detailed HFE design program has begun. Therefore, the contributions of the HFE program to function allocation are unclear. However, the second sentence of the quote indicates that this detailed information is only a starting point in the design that will take place after design certification as part of the HFE design process. More detailed

information is needed from Westinghouse to determine which is the case, and how the information in WCAP-14075 will be used as input to the overall HFE design process.

Also related to this criterion was Open Item 18.4.3.2-2 regarding the determination of the new, changed, or deleted functions and processes. Westinghouse should describe the basis for the initial allocations, as well as the process that will address the level of automation (e.g., fully automatic, fully manual, or automatic with manual backup) for each *unchanged* function with *unchanged* allocation. This was Open Item 18.4.3.3-1.

Criterion 2: Modified Function Allocations

*Criterion:* Unchanged processes that have *modified* function allocations should be analyzed in terms of resulting human performance requirements based on the expected user population. A rationale for the resulting allocation should be provided. This analysis should reflect, as much as possible at this stage of design, (1) sensitivity, precision, time, and safety-related requirements; (2) required reliability; and (3) the number of personnel and level of skills required to operate and maintain the system.

*Evaluation:* The evaluation of function assignments is discussed in Westinghouse's response to RAI 620.72. The allocations are evaluated along multiple dimensions that determine workload demands on the crew. Also, Table 3 of WCAP-14075, (Revision 0), provides some discussion of allocations at the system level and some at the plant process level. These discussions should be expanded to cover all functions and plant processes, including the identification and analysis of any unchanged processes that have modified function allocations. In addition, evaluations of allocations will occur during the AP600 test program, as described in Section 18.8.2.3.1.5 of the SSAR. Therefore, while questions remain concerning the initial allocation, the analysis of human performance requirements appears to be addressed adequately in the Westinghouse methodology. However, such adequacy should be verified by a sample analysis with associated documentation. Westinghouse should describe how the program will develop the rationale and level of automation for each *unchanged* function or process with *modified* allocation. This was Open Item 18.4.3.3-2.

Criterion 3: Changed Plant Processes

*Criterion: Modified* plant processes should also be analyzed in terms of resulting human performance requirements based on the expected user population. A rationale for the resulting allocation should be provided. This analysis should also reflect, as much as possible at this stage of design, (1) sensitivity, precision, time, and safety requirements; (2) required reliability; and (3) the number and level of skills of personnel required to operate and maintain the system.

*Evaluation:* See the discussion earlier in this section under Criterion 2, "Modified Function Allocations." Westinghouse should describe the process that will address the rationale, allocation, and level of automation for modified plant processes. This was Open Item 18.4.3.3-3.

Criterion 4: Criteria Documentation

*Criterion:* The allocation criteria, rationale, analyses, and rules used in the analysis of function allocation should be documented.

*Evaluation:* In its response to RAI 620.72, Westinghouse indicated that, as part of the function allocation process, the initial set of allocations is documented, as are the modifications that will be made iteratively as the allocations are evaluated and modified. When function allocation is completed, the documentation will include the basis and justification for the allocation or its modification.

Criterion 5: Analyses Results

*Criterion:* The results of analyses and trade-off studies should support the adequate configurations of personnel- and system-performed control functions. Analyses should confirm that the personnel can properly perform tasks allocated to them while maintaining operator situation awareness, workload, and vigilance. Proposed function assignment should take maximum advantage of the capabilities of humans and machines without imposing unfavorable requirements on either.

*Evaluation:* See the discussion earlier in this section under Criterion 2, "Modified Function Allocations." Westinghouse should describe the analyses that will confirm that the personnel can properly perform tasks allocated to them while maintaining operator situation awareness, workload, and vigilance. This was Open Item 18.4.3.3-4.

Criterion 6: OER Issues - Modified Processes

*Criterion:* The OER should be used to address the case of *modified* processes. Problematic OER issues should be considered during the function allocation analyses for modified functions.

*Evaluation:* The role of operating experience in the identification of acceptable allocations, or for allocations that need to be addressed, is an essential part of initial allocations (as identified in the basis for the Westinghouse approach, IAEA-TECDOC-668). However, the role of the OER has not been clearly identified. Westinghouse should describe the use of the OER in the identification and evaluation of function allocations for those modified processes that have been identified as problematic, based on operating experience, and how past problems will be addressed. This was Open Item 18.4.3.3-5.

Criterion 7: OER Issues - Unchanged Functions

*Criterion:* The OER should be used to address the case of *unchanged* functions that have *unchanged* function allocations. If problematic OER issues are identified, an analysis should be performed to (1) justify the original analysis of the function; (2) justify the original human-machine allocation; and (3) identify solutions (such as training, personnel selection, and procedure design) that will be implemented to address the OER issues.

*Evaluation:* See the discussion earlier in this section under Criterion 6, "OER Issues - Modified Processes." Westinghouse should describe how unchanged functions with unchanged function

allocations that have been identified as problematic based on operating experience will be addressed. This was Open Item 18.4.3.3-6.

Criterion 8: New Control Function Allocations

*Criterion:* All function allocations should be reviewed to evaluate the effect of new control function allocations on unchanged control function allocations.

*Evaluation:* The evaluation of the effect of new control function allocations on unchanged control function allocations is not explicitly addressed in the AP600 method description. Westinghouse should describe how function allocations will be reviewed to evaluate the effect of new control function allocations on unchanged control function allocations. This was Open Item 18.4.3.3-7.

Criterion 9: Control Function Re-allocation

*Criterion:* Control functions should be reallocated in an iterative manner, in response to developing design specifics, operating experience, and the outcomes of ongoing analyses and trade studies.

*Evaluation:* In its response to RAI 620.72, Westinghouse indicated that, as a result of the function allocation evaluations, the allocation will be addressed iteratively to "correct problems, reduce the likelihood of error, and enhance overall performance."

Criterion 10: Technical Basis (Control Function Allocation) Documentation

*Criterion:* The technical basis on which the control function allocation analysis was performed should be documented.

*Evaluation:* As stated in the evaluation in this section of Criterion 4, "Criteria Documentation," Westinghouse's response to RAI 620.72 indicated that, as part of the function allocation process, the initial set of allocations is documented, as are the modifications that will be made iteratively as the allocations are evaluated and modified. When function allocation is completed, the documentation will include the basis and justification for the allocation or its modification.

18.4.3.2 FSER Evaluation

New Open Item/Criterion 1

*Criterion:* (a) A description should be provided of the "methodology" that was used by Westinghouse to arrive at the current AP600 level of automation, including function definition and allocation assignments already made. The application of industry standards, guidelines, and practices should be identified. (b) The description should seek to revise or clarify the documented material already reviewed by the staff in the SSAR and RAI responses.

*Evaluation:* The discussion below addresses each of the two subitems (a and b) of Criterion 1, separately .

(a) A description should be provided of the "methodology" used to date by Westinghouse to arrive at the current AP600 level of automation, including function definition and allocation assignments already made. The application of industry standards, guidelines, and practices should be identified.

Section 1.2 of WCAP-14644, (Revision 0), provides an overview of the AP600 functional requirements and allocation methodology. Sections 2.1 and 3.1 present detailed treatment of both aspects of the methodology. In general, the approach is quite similar to that found acceptable in the DSER, with several clarifications provided. These clarifications are summarized below.

The initial set of functional requirements and allocations are based upon operating experience with the reference systems that make up the AP600 predecessor or reference plant (see New Open Item 2 for a discussion of the AP600 reference plant). The discussion in the WCAP provides significantly improved documentation of the initial allocation basis, as compared to that provided in the SSAR (Revision 0). The initial analysis was made by system designers based on knowledge of the operational performance of the systems and considering the relative capabilities of human and system resources.

Westinghouse developed a methodology to "document the rationale for initial allocation decisions" (p. 1-3). This methodology is based on NUREG/CR-3331 and provides a structured approach, conducted by an interdisciplinary team that includes HFE and systems expertise. NUREG/CR-3331 is identified as an appropriate source of function allocation methodology in NUREG-0711. (Note also that it has been adapted by the International Atomic Energy Agency for function analysis in IAEA TECDOC-66-8).

The detailed review of NUREG-0711 Element 3 criteria 1 and 2 was presented in the DSER. The DSER evaluations have been modified to reflect the new information provided by Westinghouse. The modified discussion is presented below.

As indicated in Section 2.1 of WCAP-14644, (Revision 0), functional requirements analysis was initially performed by system engineers. The WCAP sought to document the requirements analysis. In summary, the objective of the analysis was to identify the functions that must be performed to satisfy plant safety objectives (i.e., to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public). The scope of Westinghouse's functional requirements analysis included both design-basis and beyond-design-basis accidents but not severe accident events.

For each AP600 critical safety function (CSF), the success paths for function achievement were defined (i.e., combinations of safety-related and non-safety-related, defense-in-depth structures, systems, and components (SSCs)). Table 1 of WCAP-14644 (Revision 0) identifies the CSFs. Table 2 describes the success paths to satisfy each of the CSFs of the AP600 and the generic reference plant. While the CSFs

are the same for both, this comparison enables the identification of the differences between the SSCs that achieve the functions (in Table 3). The information and action requirements for each CSF success path were identified and documented in the WCAP.

Based on this analysis, the differences between the AP600 and the reference plant were identified. Differences were considered for (1) the overall system design configuration or system arrangement, and (2) allocation of function. The success paths were identified (in Table 3) as unchanged, modified, or new (consistent with the definition used in NUREG-0711). Where a success path was unchanged, operating experience became a technical basis for the functional requirements (and their allocation).

The HSI design team performs a related, supporting, functional requirements analysis activity ("goal-means decomposition"). In revisions of the SSAR prior to Revision 19, this was described in SSAR Sections 18.6, 18.8, and 18.9. In SSAR (Revision 23), Section 18.4 covers "Functional Requirements Analysis and Allocation," and refers to WCAP-14644 (Revision 0). Section 18.5 generally covers task analysis, but also now briefly addresses the goal-means decomposition. This process is based on a decision sets model that involves decomposition of plant functions from global, abstract functions, such as "prevent radiation release" to lower level decision sets, such as "control reactor coolant system (RCS) boron concentration." For each decision set, questions are addressed that provide information for accomplishing the goal of the decision set, such as what information is needed, what decisions need to be made, and where the results must go. The results are presented in both graphic and tabular form with the aid of a computer-aided software engineering tool. At the lower levels, cognitive task analysis is performed to provide the requirements for the HSI design (the cognitive task analysis is reviewed in Section 18.5 of the DSER). Westinghouse stated in WCAP-14644, (Revision 0), that this analysis is consistent with the functional requirements analysis described in the WCAP. They intend, however, to address the details as part of Element 4, "Task Analysis," which is only being reviewed at an implementation level for AP600.

Westinghouse further clarified this approach to function allocation in their response to RAI 620.72 (Revision 1, February 7, 1995). WCAP-14644, (Revision 0), Section 3.1, further clarifies the analysis methodology. Currently, SSAR Revision 19, Section 18.4, provides the overview and WCAP-14644 (Revision 0) provides the details. As indicated above, the preliminary allocations were performed by the system engineers. Westinghouse then developed a structured approach based upon the methodology developed in NUREG/CR-3331.

Applying the methodology (illustrated in Figure 1 of WCAP-14644, Revision 0), Westinghouse first identified those function assignments that are mandatory for automatic control and whether automation is technically feasible. Mandatory allocations were identified based on a review of documents such as 10 CFR Part 50 (especially GDC 20, Protection System Functions), the SRP, and the URD (e.g., to meet time criteria). Following these assignments, the allocations are made based on preference for human or automatic control. Preference may be derived from different bases, such as operating experience, PRA sensitivity, operator workload, the inherent nature of the process (passive systems are inherently automatic), or the need for operator judgement prior to actuation.

If the allocation cannot be clearly identified based on these considerations, the function is further broken down to smaller units for which the allocation process is performed. When this initial allocation is completed, the allocations are subject to further analysis, such as analyses to determine the HSI requirements for successful operator interaction with automated systems (e.g., to manually preempt an automated function or to successfully monitor and, if necessary, manually back up an automated function). Because of the dynamic and interactive nature of human performance, the methodology provides for the allocation to be reevaluated during the design process.

The discussion of AP600 functional requirements and allocation methodology provided in WCAP-14644 (Revision 0) acceptably clarifies the staff's concerns about functional requirements analysis and allocation methodology identified in the staff's open item.

(b) The description should seek to revise or clarify the documented material already reviewed by the staff in the SSAR and RAI responses.

Westinghouse issued updated documents, including Revision 14 of the SSAR; Revision 0 of WCAP-14644; and RAIs 620.91, 620.92, 620.93, and 620.94. These documents are consistent and acceptably address Element 3 and the open items. Based on this information, Open Item 18.4.3.3-1 is closed and the criterion is satisfied.

New Open Item/Criterion 2

*Criterion:* (a) A description should be provided of the AP600 functions, processes, and systems and a comparison made to the reference plants/systems so that one can identify areas of difference that exist. (b) The response should address the staff's specific concerns identified in the evaluation section of DSER Section 18.4.3.2, Criterion 1 (repeated below). (c) The response should also address how the results of functional requirements analysis are verified and how the results are updated as the design process proceeds.

*Evaluation:* The review focused on the three subitems of Criterion 2 (a, b, and c), which are discussed separately.

(a) A description should be provided of the AP600 functions, processes and systems and a comparison to the reference plants/systems so that one can identify areas of difference that exist.

Information addressing this criterion has been provided in Section 2 of WCAP-14644, Revision 0. The AP600 CSFs are identified in Table 1 of WCAP-14644, Revision 0, and include subcriticality, core cooling, heat sink, RCS integrity, containment, and RCS inventory. Table 2 provides a comparison of the AP600 CSFs and their success paths with those of the reference plant. The reference plant for the AP600 is the generic PWR design for currently licensed Westinghouse nuclear power plants. Section 2.1.3 and Table 3 provide a comparison of the design of the SSCs and their function allocation between the AP600 and the reference plant. The table indicates whether each of the success paths for each CSF are unchanged, modified, or new.

The CSFs for the AP600 are the same as those for the reference plants, but the success paths and SSCs are different. The major differences in the AP600 are (1) the use of safety-related, passive systems for safety injection and decay heat removal, (2) the use of advanced digital I&C, (3) automation of certain SSC actuation and control functions that help reduce operator workload, and (4) design changes that were identified through a review of operating experience.

WCAP-14644, Revision 0, provides a detailed and acceptable description of the AP600 functions, processes, and systems as well as a comparison to the reference plants/systems so that one can identify areas of difference that exist.

(b) The response should address the staff's specific concerns identified in the evaluation section of DSER Section 18.4.3.2, Criterion 1. The DSER stated "Safety functions (e.g., reactivity control) should be defined. These include functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant processes (plant system configurations or success paths) should be clearly defined that are responsible for or capable of carrying out the function."

The DSER Evaluation of this criterion stated: High-level safety functions have been defined and are displayed in Figures 18.6-9 and 18.6-10 of the SSAR (Revision 0). These include the functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. Figures 18.6-9 and 18.6-10 of the SSAR (Revision 0) show the top four levels in the functional decomposition. For example, Level 1, containing "Prevention of Radiation Release," is decomposed in Level 2 into "Fuel Integrity," "RCS Boundary Integrity," etc. In Level 3, "Fuel Integrity" is decomposed into "Reactivity Balance" and "Fuel Clad Heat Balance." In Level 4, "Reactivity Balance" is decomposed into "Control Gross Reactivity" and "Control RCS Boron Concentration." The following examples demonstrate the staff's concern with completeness:

- Level 1 of these figures only includes "Prevention of Radiation Release," and not other safety functions such as site personnel protection (e.g., from exposure to high radiation sources) or protection of the environment from various releases such as toxic chemicals. It is not clear whether these safety functions are covered in the decision sets in Figures 18.6-1 through 18.6-8 of the SSAR (Revision 0).

- At Level 2, the box for radioactive waste management is not developed, and it is not clear if this will include monitoring routine radioactive releases. These items should be considered because they also contribute to the specification of requirements for controls, displays, and alarms.

- At Level 4 in Figure 18.6-10 of the SSAR (Revision 0), it is not clear why there are no functions identified for "steam generator (SG) water inventory" and "control containment temperature."

It is not clear, based on the methodology presented, how the results are verified for completeness and accuracy.

As the focus of WCAP-14644, Revision 0, was not on the decision sets model or the goal-means decomposition, these issues were not addressed. However, these are related functional requirements activities that are conducted by the HSI design group to support the Westinghouse function-based task analyses and display design. As such, the details of this item have been transferred to Element 4, "Task Analysis," and are addressed there. It is important to note that while Element 3 is being reviewed at a complete element level, Element 4 is being reviewed at the implementation plan level.

(c) The response should also address how the results of functional requirements analysis are verified and how the results are updated as the design process proceeds.

WCAP-14644, Revision 0, Section 2.3 discusses the verification and updating of functional requirements analyses. Several different analyses contribute to the evaluation of functional requirements including SSAR Chapter 15 safety analyses, PRA analyses, and function-based task analyses. SSAR safety analyses address the ability of the plant functions, systems, and processes to cope with design-basis events. PRA analyses address the acceptability of plant functions, systems, and processes for coping with beyond-design-basis accidents. The function-based task analyses performed by the HSI design team provides verification of the detailed sensor and control specifications for CSF-related requirements.

WCAP-14644, Revision 0, Section 2.3 also describes the mechanisms for modifying functional requirements if the analyses described above identify a need to do so. Modifications would be accomplished through the formal procedures described in the AP600 design configuration change control process (discussed in the Element 1 review). The procedures assure that the change is properly implemented, documented, and verified.

This information provides an acceptable explanation of the process by which functional requirements will be verified and the requirements can be changed, if required. Based on this information, Open Items 18.4.3.2-1 through 18.4.3.2-7 are closed and the criteria are satisfied.

New Open Item/Criterion 3

*Criterion:* (a) A description should be provided of the human role in AP600 functions, processes and systems (as defined in New Criterion 2 above) in terms of personnel responsibility and level of automation. Because it is our understanding that the technical basis for allocation was largely based on operating experience (e.g., successful allocations were not changed and problematic allocations were changed), a comparison to the reference plants/systems should be documented so that differences in allocation can be identified. Where allocations have changed, the basis for the change should be identified. Passive systems should be considered a special form of automation because initiation and control of these functions often do not require personnel actions. (b) A description should be provided as to how the functional allocation process for the AP600 will accommodate the need for thorough HFE input early in the design process. This is particularly important for those areas identified above that are "different" from the predecessor plants/systems.

*Evaluation:* The review focused on the two subitems of Criterion 3 (a and b), which are discussed separately.

(a) A description should be provided of the human role in AP600 functions, processes and systems (as defined in New Item 2 above) in terms of personnel responsibility and level of automation. Because it is our understanding that the technical basis for allocation was largely based on operating experience (e.g., successful allocations were not changed and problematic allocations were changed), a comparison to the reference plants/systems should be documented so that differences in allocation can be identified.

Where allocations have changed, the basis for the change should be identified. Passive systems should be considered a special form of automation because initiation and control of these functions often do not require personnel actions.

WCAP-14644 (Revision 0), Section 1.3, provides an overview of the role of the operator. Section 3 describes the specific role of the operator with respect to CSF success paths (the details are presented in Table 4) and documents the basis for the allocation (the details are presented in Table 5). Table 3 provides comparisons between the AP600 and the reference plant with respect to allocation of functions.

The role of the AP600 operator is described at a high level as including the monitoring of plant states and automatic operations, controlling the operation of non-safety systems, and terminating the safety systems when plant conditions have been stabilized. The overall difference between this role and that of operators in current plants is not significant. The specific detailed differences relate to the specific actions performed by operators due to differences in safety-related systems and the increased automation of the AP600. For example, while the AP600 uses passive safety systems, from the perspective of the operator these function like automatic systems. At a high level, the operator's role with respect to these systems is essentially the same as with other automatic systems (e.g., to verify their operation and terminate them when EOP criteria are met). Table 3 provides a detailed comparison between the AP600 and the reference plant of the function allocation for actions within the CSF success paths. The table indicates whether the allocation is unchanged, modified, or new (for new actions). Explanatory notes are provided for each action. For example, Startup Feedwater under Core Cooling is identified as a modified allocation because steam generator level control has been automated, while its control was manual in the reference plant. Thus operators do not have to throttle back feedwater flow to prevent steam generator overfill or RCS overcooling in the AP600.

Table 4 in WCAP-14644, Revision 0, breaks down each CSF success path into actuation and control actions. Each is classified as to the level of automation provided, including passive, automatic (only), parallel (actuation and control can always be accomplished manually or automatically), selectable (the operator selects whether actuation and control are accomplished manually or automatically), complementary (actuation and control responsibilities are shared), and manual.

The technical bases for the allocations identified in Table 4 are documented in Table 5. The bases provided stem from the function allocation methodology discussed in New Open Item 1 above and illustrated in Figure 1 of the WCAP.

WCAP-14644, Revision 0, provides a detailed audit trail from function allocations in the reference plant to how those allocations were represented in the AP600. The technical basis for each allocation is documented based on the methodology developed from NUREG/CR-3331, "A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automated Control." The staff finds this approach acceptable.

(b) A description should be provided as to how the functional allocation process for the AP600 will accommodate the need for thorough HFE input early in the design process. This is particularly important for those areas identified above that are "different" from the predecessor plants/systems.

WCAP-14644, Revision 0, Section 4.1, describes the HFE input provided early in the design process. When making initial allocations, "explicit considerations of limitations in human capabilities" were provided on the basis of knowledge of operating experience and HRA analyses. For example, tasks were not allocated to human resources when personnel could not preform a task quickly enough to accomplish critical safety actions within required time, when the tasks were complex or not routinely performed, or when the combination of tasks would lead to high workload. Based on this information, Open Items 18.4.3.3-1 through 18.4.3.3-3, 18.4.3.3-5, and 18.4.3.3-6 are closed and the criteria are satisfied.

New Open Item/Criterion 4

*Criterion:* A description should be provided of how the integrated role of the operator across all systems is confirmed for acceptability. If function allocation was performed by individual system designers, will the IAEA process described in the RAI responses be used at all, and if so how?

The process should be described by which functions are reallocated in an iterative manner, in response to developing design specifics, operating experience, and the outcomes of ongoing analyses and trade studies.

*Evaluation:* WCAP-14644, Revision 0, Section 4.2, describes the evaluation of the integrated role of the operator and Section 4.3 describes the mechanisms for modifying function allocations.

In WCAP-14644, Revision 0, Section 4.2, Westinghouse describes the evaluation of the integrated role of the operator using task and workload analysis, HSI design and evaluation, and verification and validation. In WCAP-14644 (Revision 0), Westinghouse indicates that because of the dynamic and interactive aspects of human performance, the allocations are evaluated through subsequent HFE analyses throughout the design process. Following the initial allocations by system designers, the integrated role of operators is assessed during task analyses when workload evaluations are conducted. Because the task analyses will address a full range of operating modes, they provide an opportunity to identify operational phases in which workload can be expected to be high. The HSI will be specifically designed to support the operator's functional role in the plant (through the support of the functional decomposition analyses), which will be evaluated in verification activities. The final allocation will be evaluated as part of integrated system validation. Because validation will use dynamic simulation, the tests will provide an opportunity to adjust allocations should problems be identified.

In WCAP-14644, Revision 0, Section 4.3, Westinghouse describes the mechanisms for modifying function allocations. If problems with respect to allocation are identified, a process is in place to address the problem. Options include modifications to the HSI to better support the operators tasks, modifications to system design to change the level of automation, or modifications to the staffing assumptions. Once the problem has been addressed, modifications would be accomplished through the formal procedures described in the AP600 design configuration change control process (discussed in the Element 1 review). The procedures assure that the change is properly implemented, documented, and verified.

Westinghouse described an acceptable approach to evaluating the functional role of the operator and to developing design changes to modify the function allocations should it become necessary as the design develops. Based on this information, Open Items 18.4.3.3-4 and 18.4.3.3-7 are resolved and the criteria are satisfied.

18.4.4 Conclusions

The objective of this review is to ensure that the applicant has defined the plant's safety functional requirements, and that the functional allocations take advantage of human strengths and avoid allocating functions that would be negatively influenced by human limitations. Functional requirements analysis and function allocation analysis were reviewed at a complete element review level. Westinghouse discussed a detailed analysis of functional requirements and allocation, and has identified a process to further evaluate allocation if necessary. Westinghouse has acceptably completed this NUREG-0711 element.

18.5 Element 4: Task Analysis

18.5.1 Objectives

The objective of this review is to ensure that the applicant's task analysis identifies the requirements of the tasks that plant personnel are required to perform, as follows:

- provide one of the bases for making design decisions (e.g., determining before hardware fabrication, to the extent practicable, whether system performance requirements can be met by combinations of anticipated equipment, software, and personnel)
- ensure that human performance requirements do not exceed human capabilities
- be used as basic input for developing procedures
- be used as basic information for developing staffing, training, and communication requirements of the plant
- form the basis for specifying the requirements for the displays, data processing, and controls needed to carry out tasks

18.5.2 Methodology

18.5.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-14651 (Revision 2) dated May 8, 1997
- WCAP-14690 (Revision 1) dated June, 1997
- WCAP-14655 (Revision 1) dated August 8, 1996
- WCAP-14695 (Revision 0) dated July 23, 1996
- WCAP-13958 (Revision 0) dated January 13, 1994
- the AP600 PRA

18.5.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 4, "Task Analysis," of NUREG-0711. The staff reviewed Westinghouse's task analysis at an implementation plan review level because the work will not be completed in this area until after design certification.

18.5.2.3 DSER Item Resolution

To address task analysis open items, Westinghouse submitted a document describing their task analysis process, entitled "AP600 Task Analysis Activities" (transmitted to the staff on May 24, 1995). The staff submitted their review of this document in a letter dated September 5, 1995, from the NRC to Westinghouse. Numerous telephone conversations were conducted to discuss and clarify NRC comments and Westinghouse technical information.

Following the review and subsequent open item discussions, Westinghouse submitted SSAR (Revision 23) Section 18.5, "AP600 Task Analysis Implementation Plan." In addition, Westinghouse submitted WCAP-14695, (Revision 0) "Description of the Westinghouse Operator Decision-Making Model and Function-Based Task Analysis Methodology."

18.5.3 Results

Criterion 1: Scope

*Criterion:* The scope of the task analysis should include selected representative and important tasks from the areas of operations, maintenance, test, inspection, and surveillance. The analyses should be directed to the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, low power, and shutdown conditions.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.29, Westinghouse indicated that the scope of the task analysis will include all operations tasks for the full range of plant operating modes for the MCR. The analysis will cover operations that are critical to plant safety, both inside and outside the MCR, related to any facilities where these actions need to be performed. Maintenance, test, and inspection task analyses will be performed for those tasks determined by the PRA to be potential areas of high safety risk. While this scope is acceptable, the response indicated that the threshold for defining critical or high-risk tasks had not been determined. Because this threshold determines whether or not maintenance, test, and inspection tasks will be included in the analysis, the threshold definition is needed for the staff to accept the task analysis scope. Also, further discussion is necessary to clarify how the PRA will be used to identify the tasks and the PRA levels to be included (e.g., Level 1 regarding core damage, and Level 2 regarding the release of fission products into and from the containment).

Westinghouse should identify the threshold for defining critical or high-risk tasks, how the PRA will be used to identify the tasks, and the PRA levels to be included (e.g., Levels 1 and 2). This was Open Item 18.5.3-1.

FSER Evaluation

To address the issue of task analysis scope and the other task analysis open issues, Westinghouse submitted a document describing their task analysis process, entitled "AP600 Task Analysis Activities (transmitted to the staff on May 24, 1995), hereafter referred to as the "TA Plan."

The Westinghouse approach to task analysis is to evaluate tasks from two perspectives (1) function-based task analysis (FBTA) and (2) operational sequence analysis (OSA). FBTA is described in SSAR (Revision 23) Section 18.5.2.1, "Function-Based Task Analyses," and in WCAP-14695 (Revision 0), "Description of the Westinghouse Operator Decision-Making Model and Function-Based Task Analysis Methodology." The scope of the FBTA is on decomposition of the higher level functions (as described in Level 4 in SSAR Figure 18.5-1). As indicated in the DSER, this approach is an appropriate and acceptable means of assuring that function-based requirements are identified that are not dependent on specific operator tasks.

The scope of the OSA was identified on page 1 of the TA Plan. The scope is identified as including the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, low power and shutdown conditions. These will include tasks representing the full range of activities in the AP600 ERGs, and tasks identified as critical or risk-significant. While this information clarifies part of the task analysis scope issue, the TA Plan did not address whether task analyses will be performed on representative maintenance, test, inspection, and surveillance tasks.

This issue was clarified in SSAR (Revision 23) Section 18.5, "AP600 Task Analysis Implementation Plan." SSAR (Revision 23) Section 18.5.1, "Task Analysis Scope," indicated that the traditional task analyses will include tasks that involve maintenance, test, inspection, and surveillance. The tasks selected will involve activities involving "risk-significant" systems,

structures, and components (SSCs). This information acceptably addressed the staff's concern involving the scope of the task analysis.

SSAR (Revision 23) appropriately incorporated the information included in the TA Plan that contributed to the resolution of this issue. Based on the information provided, Open Item 18.5.3-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 2: Task Linking

*Criterion:* Tasks should be linked using a technique such as using operational sequence diagrams. Review of the descriptions and operational sequence diagrams should identify which tasks can be considered "critical" in terms of importance for function achievement, potential for human error, and impact of task failure. Human actions that are found to affect plant risk via PRA importance and sensitivity analyses should also be considered "critical." Specific task analyses should be performed for all critical tasks. The determination of the PRA/HRA critical human actions should consider internal and external initiating events, and actions affecting the Level I and II analyses of the PRA. (See the discussion of Element 6 in Section 18.7 of this report for an explanation of PRA/HRA analyses.) Where critical functions are automated, the analyses should consider all human tasks, including monitoring the automated system and execution of backup actions if the system fails.

*Evaluation:*

DSER Evaluation

There are three aspects of this criterion to be addressed, as follows:

(1) identification of critical tasks in the task analyses and the PRA

As discussed in the evaluation of Criterion 3, "Description of Task Analysis," later in this section, the Westinghouse approach to task analysis focuses on the cognitive requirements of tasks that are organized in a decomposition of plant functions. It is unclear whether Westinghouse considered operational sequences, which tend to be event- or scenario-based. Therefore, the role of the task analysis in specifying tasks as critical needs to be clarified.

With respect to the PRA, Westinghouse's response to RAI 720.133 indicates that the identification of critical human actions is not completed pending the completion of sensitivity analyses.

(2) analysis of critical tasks

The SSAR does not indicate how critical tasks were evaluated in the task analysis. During a meeting on June 14, 1994, Westinghouse indicated that specific task analyses were performed for those tasks that were identified as critical, but these have not been provided to the staff for review.

(3) analysis of human tasks associated with automatic actions

In its response to RAI 620.72, Westinghouse indicated that its approach explicitly identifies human tasks associated with automated systems in order to identify monitoring and control requirements. Therefore, this aspect of the criterion is acceptable.

Westinghouse should identify all critical human actions as discussed in their response to RAI 720.133, and describe how task analysis will be used in the evaluation of the critical tasks in operational sequences. This was Open Item 18.5.3-2.

FSER Evaluation

While the scope of the task analysis includes critical or risk-significant tasks, the TA Plan indicated that, at present, PRA results indicate that "there are no AP600 tasks that meet the criteria for critical or high-risk tasks" (p. 1). SSAR (Revision 23) Section 18.5.1, "Task Analysis Scope," states that the analyses will involve actions identified as "critical human actions or risk-important tasks." While, at present, no tasks meet the Westinghouse criteria, the SSAR clearly indicates they will be included if future analyses identify such tasks. The staff finds the Westinghouse criteria for risk-significant tasks acceptable (see WCAP-14651, Revision 2, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," which discusses the definition of critical human actions and risk-important tasks). Additional discussion of the staff's assessment of the Westinghouse criteria for determining risk significant tasks derived from the PRA can be found Section 18.7.3 of this report under "Criterion 1: Critical Human Actions." Based on this information, Open Item 18.5.3-2 is closed and this NUREG-0711 criterion is satisfied.

Criterion 3: Description of Task Analysis

*Criterion:* Task analysis should begin on a gross level and involve the development of detailed narrative descriptions of what personnel must do. Task analyses should define the nature of the input, process, and output required by and of personnel. Detailed task descriptions should address (as appropriate) the following aspects of each task:

- information gathering
- decision-making requirements
- response requirements
- feedback requirements
- workload
- task support requirements
- workplace factors
- staffing and communication requirements
- hazard identification

NUREG-0711 contains a more detailed description of the types of information contained in each area identified above.

*Evaluation:*

DSER Evaluation

The Westinghouse functional task analysis methodology begins with the high-level functional goals and decomposes them. A goal-means structure will be used to map the cognitive and physical tasks that define the operational space of the plant to each plant function. The goal-means structure representation is based on the concept of describing the plant's functional processes in terms of the goals to be achieved and the means or mechanisms available for achieving them.

Cognitive task analysis methodology is used to identify the monitoring and feedback, planning, and control requirements. For each node in the functional decomposition model, Section 18.6.7 and RAI 620.47 of the SSAR (Revision 0) identified a set of 11 questions that are organized into these categories. (See also Table 1 in WCAP-13957.) The answers to the questions become the database that is used to write task descriptions that are used to support HSI design. Samples of the task descriptions are contained in Westinghouse's response to RAI 620.71.

Because the emphasis of the task analysis is on cognitive requirements, the methodology described will acceptably provide the necessary information to support the definition of requirements for information gathering, decision making, response, and feedback.

It is not clear how the methodology will address the other categories of information identified in the criterion above. For example, it is not clear how the methodology will address the time flow and workload effects of performing crew tasks, such as following a procedure. These considerations are typically addressed in what Westinghouse refers to as "traditional" task analysis. RAI 620.70 gives the task analysis approach described in NUREG-0700 as an example. In its response to RAI 620.28, Westinghouse states that "the cognitive task analysis deals only with the decision-making tasks that are to be performed by the operations staff. The complete function-based task analysis includes both the results of cognitive task analysis and the traditional task analysis that includes the control actions required and the steps needed to get to the appropriate control actions." The function-based task analysis methodology described in the SSAR (Revision 0) does not appear to include such methods. In fact, Section 18.6.7 of the SSAR (Revision 0) indicates that traditional task analysis approaches "are of little or no use in those areas where effective decision making is the essence of the task."

Section 18.6.4 of the SSAR (Revision 0) does indicate that "traditional" task analyses will be used for personnel tasks such as field equipment operation, but a methodology is not described beyond a reference to Drury, et al. (1987), which does not in itself adequately describe the methodology as it will be applied to AP600 tasks. It also seems appropriate to address the same cognitive questions in these task analyses as well.

The staff agrees that the functional decomposition approach and cognitive task analysis methods are appropriate to the design of an effective HSI (as NUREG-0711 criteria indicate). However, the temporal, workload, staffing, and other aspects of performing tasks in a control room are important considerations at the task analysis stage, and are important contributors to HSI design. Therefore, while the staff supports the emphasis on cognitive factors, these other factors should be considered. Clarification of the application of task analysis methods is needed

to satisfy this criterion. Specifically, how are the cognitive task analyses and "traditional" methods integrated to analyze crew tasks, what decision criteria are used to judge whether tasks need the cognitive task analysis, and what is the total set of task analysis data that will result from the completion of all task analysis methods?

Westinghouse should indicate how time factors, workload, task support requirements, workplace factors, staffing, and communication will be addressed in the task analysis. Westinghouse should also describe how the cognitive task analyses and "traditional" methods will be integrated to analyze crew tasks, what decision criteria will be used to judge whether tasks need the cognitive task analysis, and the total set of task analysis data that will result from the completion of all task analysis methods. This was Open Item 18.5.3-3.

FSER Evaluation

Westinghouse provides information regarding task analysis in the section entitled "Task Analysis Implementation Plan" of the TA Plan. The section includes a discussion and clarification of the integration of both FBTA and OSA approaches to the task analysis in the AP600 design process. While the focus of FBTA is on decomposition of the higher level AP600 functions as described in detail in the SSAR, the focus of the OSA will be the analysis of the operational tasks as defined within the scope of task analysis activities.

The OSA will be performed in two phases. First, (OSA-1) tasks will be developed to include plant state data, data source, actions, criteria/reference values, feedback, time, sequencing requirements, support requirements, and work environment considerations. These results will provide the operational requirements for task performance. These requirements and constraints provide input into HSI design development.

The resulting designs will be tested in concept tests, which will enable further refinement of the analysis results. To accomplish this, a second OSA (OSA-2) will be performed on a representative subset of the tasks analyzed in the first phase of OSA, which include those which are risk important and those where there are performance concerns. These analyses will address the completeness of available information, time to perform tasks, operator workload, and staffing.

This information addresses the staff's concerns regarding the use of traditional analysis methods, their integration with FBTA, the information to be derived from task analysis activities, and its input and use in the detailed HSI design. In summary, the combination of FBTA and OSA provides a particularly strong technical basis for identifying operational requirements to be addressed in the detailed HSI design.

In a telephone conference (September 13, 1996) among NRC, BNL, and Westinghouse, Westinghouse indicated that the task analysis section of the SSAR will include a "bottom-up" description (which addressed concerns regarding completeness and accuracy of the FBTA, discussed in NRC Letter August 8, 1996). SSAR (Revision 23), Sections 18.5.2.2, (OSA-1), and 18.5.2.3, (OSA-2), as discussed above, acceptably address the staff's concern about completeness.

SSAR (Revision 23) Section 18.5.2, "Task Analysis Implementation Plan," appropriately incorporated the information included in the draft task analysis plan that contributed to the

resolution of this issue. Based on this information, Open Item 18.5.3-3 is closed and this NUREG-0711 criterion is satisfied.

Criterion 4: Task Analysis Iterations

*Criterion:* The task analysis should be iterative and become progressively more detailed over the design cycle.

*Evaluation:*

DSER Evaluation

Section 18.6.7 of the SSAR (Revision 0) indicates that the task analysis will be iterative. The analysis will be completed when a database is developed containing the answers to the questions posed in the cognitive analysis of each node in the functional decomposition model. The iteration will include task assignments to humans or machines. This criterion is satisfied.

FSER Evaluation

SSAR Revision 23 and WCAP-14695 (Revision 0) describe a task analysis process that is iterative, the contents of which are developed and refined as it is performed over the design cycle. Westinghouse's task analysis process is based on functional decomposition and combines traditional task analysis with cognitive task analysis methods. The use of these two task analytic techniques attempts to (1) ensure that a complete set of operator tasks is selected for evaluation, (2) determine the process plant data needed to support operator decisions, and (3) to make the plant equipment achieve their designed purposes. Based on this information, this NUREG-0711 criterion is satisfied.

Criterion 5: Job Design Issues

*Criterion:* The task analysis should incorporate job design issues such as the following:

- the number of crew members
- crew member skills
- allocation of monitoring and control tasks to the formation of a meaningful job and management of a crew member's physical and cognitive workload

*Evaluation:*

DSER Evaluation

This is not addressed as part of task analysis in the SSAR (Revision 0), as discussed in this section under Criterion 3, "Description of Task Analysis." Westinghouse should identify the relevant job design factors (such as the number of crew members and crew member skills), and indicate how they will be addressed in the task analysis. This was Open Item 18.5.3-4.

FSER Evaluation

As indicated in the discussion of Open Item 18.5.3-3 above, the second set of OSA evaluations will incorporate crew staffing considerations, as described in SSAR (Revision 9) Section 18.5.2.3. The workload assessment as part of these analyses will provide "an indication of the adequacy of staffing assumptions" (p. 18.5-4). Where high workload or time limits occur, alternative staffing assumptions, task allocations, or design changes will be evaluated. With respect to skills, Westinghouse indicated that skill requirements addressed by NRC requirements for training are assumed (i.e., no special skills are assumed for AP600 operators). This is an acceptable approach.

Westinghouse further addressed this issue in the section entitled "Job Design Factors" of the TA Plan (SSAR (Revision 9) Section 18.5.3). The section indicated that job design considerations such as staffing and crew skills are the responsibility of the COL. A COL action item was identified in the TA Plan that indicates "Combined License applicants referencing the AP600 certified design will develop a job design document that specifies the full scope and responsibilities of each control room position" (p. 4). The staff found this acceptable provided the document considered the assumptions and results of the task analyses described in the SSAR and the TA Plan.

SSAR (Revision 9) Section 18.5.2, "Task Analysis Implementation Plan," appropriately incorporated the information included in the draft task analysis plan that contributed to the resolution of this issue with the following exception. In SSAR (Revision 9), Section 18.5.4, "Combined License Information Item," the COL item description was changed to delete the reference to the development of a job design document. The staff considered the provision for a rationale of job design considerations to be an important aspect of the AP600 review to be performed after certification. Therefore, deletion of this documentation was not acceptable. Further, the staff's concerns regarding assumptions and results of the task analyses were not included.

In SSAR Revision 19, Westinghouse addressed the staff's concern by stating that a COL applicant referencing the AP600 certified design will document the scope and responsibilities of each main control room position, considering the assumptions and results of the task analysis. This is COL Action Item 18.5-1. Based on this information, Open Item 18.5.3-4 is closed and this NUREG-0711 criterion is satisfied.

Criterion 6: Minimum Inventory

*Criterion:* The task analysis results should be used to define a minimum inventory of alarms, displays, and controls necessary to perform crew tasks based upon both task and I&C requirements.

*Evaluation:*

DSER Evaluation

This item is addressed under Criterion 1, "Minimum Inventory," in Section 18.12 of this report. Westinghouse should describe how the task analysis will define a minimum inventory of alarms, displays, and controls necessary to perform crew tasks. This is addressed under Open Item 18.12.3-1.

FSER Evaluation

SSAR (Revision 23) Section 18.5, "Task Analysis Implementation Plan," indicates that the FBTA is used as a completeness check on the availability of needed indications, parameters, and controls (p.18.5-3). The SSAR also indicates that the OSAs will provide information on the inventory of alarms, controls, and parameters needed to perform sequences selected for analysis, which include those addressed in the discussion of Task Analysis Criterion 1, Scope above. Westinghouse described a minimum inventory of alarms, displays, and controls for the AP600 (see FSER Section 18.12 for the staff's review of the inventory). Based on this information, this NUREG-0711 criterion is satisfied.

Criterion 7: Input to HSI Design, Procedures, and Training

*Criterion:* The task analysis results should provide input to the HSI design, procedure development, and personnel training programs.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.75, Westinghouse indicated that task analysis "is the foundation of the design of the information and control system." The task analysis results are translated into task descriptions that serve as the basis for HSI design. Section 18.6.5 of the SSAR (Revision 0) indicates that

> "... the impact of cognitive task analysis is for the AP600 human engineering design team to realize that the responsibility of the operators to continually evaluate the operational success or failure of executing the current procedure. It is a fundamental assumption in the design of the computerized support system of the AP600 that the human operators have a thorough understanding of the functional purpose or objective of each procedure... Providing the operators with a thorough understanding of purposes and objectives is a requirement of the AP600 Operator Training Program."

Section 18.8.9.4.1 of the SSAR (Revision 0) specifically identifies the results of task analysis as providing a basis for developing the AP600 training program. Section 18.6.7 of the SSAR (Revision 0) identified task analysis as being used to derive procedures; however, Section 18.9.8 of the SSAR (Revision 0) (on procedure design) did not indicate the use of the task analysis results.

Although task analysis is specifically identified as providing a basis for HSI and training program design, its status with respect to procedure development is unclear. This has been identified as Open Item 18.9.3-2, which is discussed under Criterion 2, "Basis for Procedure Development," in Section 18.9.3 of this report because the issue is limited to procedures. Resolution of this criterion is, therefore, linked to that open item, and a separate issue is not warranted. This is addressed under Open Item 18.9.3-2.

FSER Evaluation

SSAR (Revision 23) Sections 18.9, "Procedure Development," and 18.5.2, "Task Analysis Implementation Plan," do not identify the relationship between task analysis and procedure or training development. Further, SSAR (Revision 23) Figure 18.2-3, "Overview of the AP600 Human Factors Engineering Process," did not show a task analysis as an input to either procedure or training development. However, because both are COL items, this is acceptable.

The relationship between procedure development and task analysis is addressed in WCAP-14690 (Revision 1), "Designer's Input to Procedure Development for the AP600." The WCAP states that the "plant operating procedures' technical bases... shall be consistent with ... task analyses" (p 2-1) and that the EOP technical content should be developed from the ERGs with additional input from the task analysis, among other things. The staff considers these statements to be appropriate and acceptable.

The relationship between training program development and task analysis is addressed in WCAP-14655 (Revision 1), "Designer's Input for the Training of HFE V&V Personnel." The WCAP indicates that the results of the task analysis will serve as input to the training of V&V personnel. Following V&V, a "Training Insights Report" will be developed and provided to the COL applicant. The report will provide, among other things, the task analysis that is completed for the HFE V&V, as well as the knowledge, skills, and abilities (KSA) analysis associated with those tasks (p. 4-1).

Thus, while procedure and training program development are COL activities, Westinghouse will provide the COL with the input from task analyses. The staff understands this to mean that the COL will utilize the AP600-specific task analysis information in the development of procedures and training programs. This is COL Action Item 18.5-2. Further, the staff expects the COL will utilize task analysis information for all training and procedure efforts that involve tasks for which task analyses were performed, even if those go beyond the scope of the V&V activities. Based on the staff's understanding of the information provided, this NUREG-0711 criterion is satisfied.

Criterion 8: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's task analysis should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

The cognitive task analysis methodology is based largely on the work of Rasmussen (1986) and Westinghouse (Woods, et al.), and is consistent with the recommendations of IEC-964 in accordance with NUREG-0711. However, this criterion cannot be found acceptable until the issues discussed in this section under Criterion 3, "Description of Task Analysis," are resolved. Westinghouse should identify source documents to serve as the basis for determining the types of information previously identified in Criterion 3. This was Open Item 18.5.3-5.

FSER Evaluation

In the TA Plan, Westinghouse identified the documents that served as the basis for the development of their task analysis methodology. These documents included NUREG/CR-3371, IEC-964, MIL-STD 1478, and a NATO document entitled "Applications of human performance models to system design." These documents, in conjunction with the basis documents for the FBTA, provide a solid and acceptable technical foundation for a comprehensive task analysis. SSAR (Revision 23) appropriately incorporated the information included in the TA Plan that contributed to the resolution of this issue. Based on this information, Open Item 18.5.3-5 is closed and this NUREG-0711 criterion is satisfied.

18.5.4 Conclusions

The objective of the task analysis review is to ensure that Westinghouse's task analysis identifies the requirements of the tasks that plant personnel are required to perform. Task analysis was reviewed at an implementation plan level of detail; that is, finished products from the element were not available for review but the methodology for conducting a complete task analysis was evaluated. The methodology will be used by the COL to conduct a complete task analysis, after design certification. This is COL Action Item 18.5-3. Westinghouse has acceptably developed a task analysis implementation plan and has satisfied this NUREG-0711 element.

18.6 Element 5: Staffing

18.6.1 Objectives

The objective of this review is to ensure that the applicant has analyzed the requirements for the number and qualifications of personnel in a systematic manner that includes a thorough understanding of task requirements and applicable regulatory requirements.

18.6.2 Methodology

18.6.2.1 Material Reviewed

The following Westinghouse documents were used in this review:

- SSAR (through Revision 23)

- WCAP-14075 dated May 20, 1994
- WCAP-13559 (Revision 0) dated December 10, 1992
- WCAP-14694 (Revision 0) dated July 1996

18.6.2.2 Technical Basis

The staff focused its DSER review on an evaluation of the Westinghouse documents with respect to the general criteria and topics of NUREG-0711, Element 5, "Staffing." 10 CFR 50.54, "Conditions of Licenses," was also used to develop the DSER.

18.6.2.3 DSER Item Resolution

Following the DSER, staffing was identified as a COL action item in SSAR (Revision 23) Section 18.6, "Staffing." Thus, the staff did not pursue resolution of the specific concerns identified in the DSER related to staffing. Instead the focus of the review was changed to determining the acceptability of the COL action item description.

18.6.3 Results

Criterion 1: Number and Qualifications of Personnel

*Criterion:* The staffing analysis should determine the number and background (qualifications) of personnel required during the full range of plant conditions and tasks, including operational tasks (normal, abnormal, and emergency), plant maintenance, and plant surveillance/testing. The scope of personnel that should be considered is identified in Element 1 of NUREG-0711.

*Evaluation:*

DSER Evaluation

Sections 18.7 and 18.9 of the SSAR (Revision 0) only discuss staffing levels with respect to operational personnel. No discussion is provided regarding other plant personnel (e.g., maintenance or I&C) staffing levels. Section 18.9.13 of the SSAR (Revision 0) lists the full range of plant modes for which staffing levels need to be considered, but states that staffing recommendations are based on the human engineering design and implementation process that is described in Section 18.8 of the SSAR (Revision 0). It is not clear how that process will be used to address staffing level issues.

In its response to RAI 620.45, Westinghouse stated that the staffing of the MCR will be verified during various plant operating modes through task analysis and testing; however, the actual process that will be used for this verification is not specifically defined. Additionally, there is no discussion devoted to how staffing requirement determinations will be made for nonoperational personnel during the full range of plant conditions.

Also, Westinghouse provided limited discussion on staff qualifications, and the discussion that is provided (in Section 18.9.2 of the SSAR, Revision 0) is only relevant to operations staff. This section states that the descriptions of the operator functions and qualifications are based on the human engineering design and implementation process described in Section 18.8 of the SSAR

(Revision 0). It is not clear how this process will be used to address necessary personnel background requirements.

Westinghouse should provide additional information on how the HFE design and implementation process will address the number and qualifications of personnel required during the full range of plant conditions and tasks, including operational tasks, plant maintenance, and plant surveillance and testing. This was Open Item 18.6.3-1.

FSER Evaluation

Following the DSER, Westinghouse identified staffing as a COL action item. Therefore, the staff did not require resolution of the concerns identified in the DSER and Open Item 18.6.3-1 and the rest of the open items are considered closed.

SSAR (Revision 23) Section 18.6.1, "Combined License Information Item," states that the COL applicant will address staffing levels and qualifications of plant personnel, including operations, maintenance, engineering, I&C, radiological protection, security and chemistry. The description states that the staffing requirements of 10 CFR 50.54(m) will be addressed.

While this description is acceptable, the staff determined that it is necessary for the COL applicant to (1) address the staffing considerations in NUREG-0711, (2) address relevant concerns identified in the DSER evaluation, and (3) to identify the minimum documentation that the COL applicant will provide to the staff to complete its review. This is COL Action Item 18.6-1. Based on this evaluation, the staffing-related DSER items are post-design certification issues that will be addressed by the COL applicant.

Criterion 2: Staffing Levels

*Criterion:* Staffing levels should be based on an analysis of the following factors:

(a) initial HSI staffing goals and their bases, including staffing levels of predecessor systems and a description of significant similarities and differences between predecessor and current systems

(b) required actions determined from the task analysis

(c) availability of operators, considering other activities that may be ongoing and for which operators may take on responsibilities outside the control room (e.g., fire brigade)

(d) the physical configuration of the control room and control consoles

(e) the availability of plant information from individual operator workstations from individual and group view HSI interfaces

(f) required interaction between operators for diagnosis, planning, and control activities

(g) required interaction between personnel for administrative, communications, and reporting activities

(h) actions required by 10 CFR 50.47 (and NUREG-0654) to meet an initial accident response in key functional areas as required by the emergency plan

(i) staffing requirements described in Section 13.1.2-13.1.3, "Operating Organization," of NUREG-0800 and 10 CFR 50.54

*Evaluation:*

DSER Evaluation

Section 18.7.1 of the SSAR (Revision 0) lists the following three factors that contribute to the determination of staffing requirements for successful operation of the AP600:

(1) regulatory requirements for presence of licensed and nonlicensed individuals to perform specific duties

(2) capabilities of humans to perform the tasks required for safe and efficient plant operations

(3) economic incentives to limit operations staff to a practical minimum

The SSAR (Revision 0) states that these three factors are examined to determine the requirements for each operations and control center. It is not clear, in many instances, how these factors were examined to determine the stated requirements.

Sections 18.7.2.1 and 18.7.2.2 of the SSAR (Revision 0) discuss the number of personnel needed to staff for operations. In its response to RAI 620.46, Westinghouse stated that initial staffing requirements were derived from Chapter 10 of the EPRI ALWR URD and from assessing the capabilities of a compact control room configuration. Section 18.9.1.1 of the SSAR (Revision 0) states that two main control area operators are required for plant startup and shutdown, but once steady-state conditions are achieved, only one is required for plant operations. 10 CFR 50.54(m) requires that two reactor operators and two senior reactor operators be on shift at all times, but only one reactor operator and one senior reactor operator are required to be in the control room at any specified time. Therefore, the staffing design for an AP600 facility may not meet the requirements of 10 CFR 50.54(m) under all plant conditions. It is not clear what analyses were conducted to determine that these requirements were appropriate for the AP600. In addition, the PRA provides credit for shift technical advisor (STA) activities in the MCR. Information is needed on how the STA is integrated into the MCR staffing configuration. This finding relates to item (l) of Criterion 2, and partially relates to item (a) of Criterion 2. It does not, however, completely satisfy this element because no discussion is provided on the examination of typical staffing levels in predecessor systems, and no correlations are made with the differences and similarities between current and predecessor systems as described in WCAP-14075.

Section 18.7.2 of the SSAR (Revision 0) states that staffing requirements are validated against the task analysis (item (b) of Criterion 2), but does not discuss how this is done.

The SSAR (Revision 0) sections related to staffing (specifically, Section 18.7) do not take into consideration the availability of operators with regard to other activities that may be ongoing and for which operators may be required to take responsibility (item c of Criterion 2).

Section 18.7.2 of the SSAR (Revision 0) states that staffing requirements are validated against the physical design of the AP600 operations and control centers. Additionally, Section 18.9.1.2 of the SSAR (Revision 0) states that a high degree of coordination among the data displays, procedures, process controls, operating crew training, and job descriptions is provided, and that coordinating the control room resources with the crew's mental and physical tasks is achieved. These statements relate to item (d) of Criterion 2, but do not discuss how this will occur.

Section 18.9.1.1.2 of the SSAR (Revision 0) discusses how any operator workstation screen can display any graphic; however, in order to maintain the concept of spatial dedication to the operator, specific functions are assigned to specific screens. Additionally, operators do not need to physically change positions to access control devices. Finally, Section 18.9.1.1.1 of the SSAR (Revision 0) states that the wall panel information station is located at one end of the main control area at a height so that both operators and the shift supervisor can view it while sitting at their respective workstations. These statements partially address item (e) of Criterion 2, but do not specifically tie into how this information will be used to address staffing requirements.

Section 18.9.1.2 of the SSAR (Revision 0) states that interaction between operators is possible, but again, it is not clear how this information was taken into account in the analysis of required staffing levels (item (f) of Criterion 2). Interactions between personnel required for administrative, communications, and reporting activities (item (g) of Criterion 2) are not discussed.

There is no specific discussion regarding actions required by 10 CFR 50.45 (and NUREG-0654) or the staffing requirements described in 10 CFR 50.54 and NUREG-0800 (items (h) and (i) of Criterion 2). Section 18.7.1 of the SSAR (Revision 0) states, however, that NRC regulatory guidance defines minimum staffing for the AP600. (See Criterion 5, "Industry Standards, Guidelines, and Practices," in this section for additional discussion of this issue.)

In summary, the documentation in the SSAR (Revision 0) related to staffing addresses some, but not all, of the elements listed under Criterion 2, "Staffing Levels." For those elements that are addressed, it is not clear how the information was or will be used to make staffing decisions.

Westinghouse should discuss how the staffing design meets the requirements of 10 CFR 50.54(m), and describe the analyses conducted to determine whether these requirements were appropriate for the AP600. Westinghouse should also describe the process that will be used to validate staffing requirements against the task analysis and against the physical design of the AP600 operations and control centers, as well as how the availability of plant information from individual operator workstations will be used in the analysis of staffing levels. Westinghouse should also discuss the availability of operators considering other ongoing activities, and how that relates to staffing. In addition, Westinghouse should provide more information on the required interaction between operators for diagnosis, planning, and control activities, and interaction between personnel for administrative, communications, and reporting activities. Finally, Westinghouse should discuss how the actions required in 10 CFR 50.47 (and

NUREG-0654) and staffing requirements in Sections 13.1.2 and 13.1.3 of NUREG-0800 and 10 CFR 50.54 will be taken into account in the staffing level decisions made for the AP600. This was Open Item 18.6.3-2.

FSER Evaluation

See discussion under staffing Criterion 1, "Number and Qualifications of Personnel," above. The staffing-related DSER item is a post-design certification issue and will be addressed by the COL applicant. Open Item 18.6.3-2 is closed.

Criterion 3: Staffing Analysis Iteration

*Criterion:* The staffing analysis should be iterative; that is, the initial staffing goals should be reviewed and modified as the analyses associated with other NUREG-0711 elements are completed.

*Evaluation:*

DSER Evaluation

Section 18.7.2.1.1 of the SSAR (Revision 0) defines the staffing for plant operations but states that the M-MIS designer must evaluate the adequacy of the specified staffing level. If a determination is made that the staffing level is not adequate or, if meeting this requirement adds substantial specialized automatic control or equipment so that a change in the number of reactor operators is required, the function-based task analysis will be modified and these changes input to the M-MIS design process. It is not clear, however, how this will be done, given that the task analysis does not seem to be crew member-based.

The information provided in the SSAR (Revision 0) does not provide any further detail on the iterative nature of the staffing level analysis. Westinghouse should describe in more detail the iterative nature of the staffing level analysis. In addition, Westinghouse should discuss how the task analysis will be modified if a determination is made that the staffing level is inadequate or if meeting the staffing level requirement adds substantial specialized automatic control of equipment, given that it is not clear that the task analysis is crew member-based. This was Open Item 18.6.3-3.

FSER Evaluation

See discussion under staffing Criterion 1, "Number and Qualifications of Personnel," above. The staffing-related DSER item is a post-design certification issue and will be addressed by the COL applicant. Open Item 18.6.3-3 is closed.

Criterion 4: Basis for Staffing

*Criterion:* The staffing analysis should consider the issues associated with the following NUREG-0711 elements and then compare these issues to staffing assumptions regarding the

number and qualifications of operations personnel. The basis for staffing should be modified to address these elements:

- operating experience review
  - operational problems and strengths that resulted from staffing levels in predecessor systems
- function analysis and allocation
  - mismatches between functions allocated to the operator and the qualifications of anticipated operators
- task analysis
  - the knowledge, skills, and abilities required for operator tasks addressed by the task analysis
  - requirements for operator response time and workload
  - requirements for operator communication and coordination
  - the job requirements that result from the sum of all tasks allocated to each individual operator both inside and outside the control room
- human reliability assessment
  - the effect of overall staffing levels on plant safety and reliability
  - the effect of overall staffing levels and the coordination of individual operator roles on critical human actions
  - the effect of overall staffing levels and the coordination of individual operator roles on human errors associated with the use of advanced technology
- HSI design
  - staffing demands resulting from the locations and use (especially concurrent use) of controls and displays
  - the requirements for coordinated actions between individual operators
- procedures
  - staffing demands resulting from requirements for concurrent use of multiple procedures
  - skills, knowledge, abilities, and authority required of operators by the procedures

- training
  - crew coordination concerns that are identified during the development of training
- verification and validation
  - ability of minimum size operating crew to control plant during validation scenarios
  - ability of operators to effectively communicate and coordinate actions during all validation scenarios
  - ability of operators to maintain awareness of plant conditions and operator actions throughout all validation scenarios

*Evaluation:*

DSER Evaluation

Of the NUREG-0711 elements listed above, only Operational Experience, Task Analysis, HSI Design, and Verification and Validation are specifically addressed, and only as they relate to staffing of operations personnel. In its response to RAI 620.45, Westinghouse referred back to the response to RAI 620.9, which summarizes the applicant's review of operating experience described in WCAP-13559. It is unclear to the staff how this information was used in developing appropriate staffing levels for the AP600. Section 18.7.2 of the SSAR (Revision 0) states that staffing requirements are validated against both the physical design of the AP600 operation and control centers, and the task analysis. Section 18.7.2.1.1 of the SSAR (Revision 0) defines the staffing for plant operations, but states that the M-MIS designer must evaluate the adequacy of the specified staffing level. Section 18.7.2.2 of the SSAR (Revision 0) states that the staffing requirements for the remote shutdown room are validated against the physical design and function-based task analysis for the AP600.

Westinghouse should provide additional information, particularly for those elements of Criterion 4, "Basis for Staffing," of this section, that are not specifically addressed for operations personnel, and for all the elements of Criterion 4, "Basis for Staffing," of this section as they relate to nonoperations personnel. This was Open Item 18.6.3-4.

FSER Evaluation

See discussion under staffing Criterion 1, "Number and Qualifications of Personnel," above. The staffing-related DSER item is a post-design certification issue and will be addressed by the COL applicant. Open Item 18.6.3-4 is closed.

Criterion 5: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's staffing implementation plan should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

This criterion is partially met by Westinghouse's indication in Section 18.7.1 of the SSAR (Revision 0) that one of the factors used in determining staffing requirements was existing regulatory requirements. However, no specific references are provided in Section 18.7 of the SSAR (Revision 0). Westinghouse should identify the industry standards, guidelines, and practices on which the staffing implementation plan is based. This was Open Item 18.6.3-5.

FSER Evaluation

See discussion under staffing Criterion 1, "Number and Qualifications of Personnel," above. The staffing-related DSER item is a post-design certification issue and will be addressed by the COL applicant. Open Item 18.6.3-5 is closed.

18.6.4 Conclusions

The objective of this review is to ensure that the applicant has analyzed the requirements for the number and qualifications of personnel in a systematic manner that includes a thorough understanding of task requirements and applicable regulatory requirements.

Following the DSER, Westinghouse identified staffing as a COL action item. Therefore, the staff did not require resolution of the concerns identified in the DSER for design certification. DSER staffing open items will be addressed by the COL applicants part of post-design certification issues.

18.7 Element 6: Human Reliability Analysis

18.7.1 Objectives

The objectives of the Human Reliability Analysis (HRA) review are to ensure that:

- the HRA activity effectively integrates the HFE program activities, as well as the PRA and risk analysis activities
- the applicant has addressed human error mechanisms in the design of the plant HFE (i.e., the HSIs, procedures, shift staffing, and training in order to minimize the likelihood of personnel error and to provide for error detection and recovery capability).

18.7.2 Methodology

18.7.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-14651, Draft dated May 14, 1996

- WCAP-14651, (Revision 1) dated October 9, 1996
- WCAP-14651, (Revision 2) dated May 8, 1997
- Chapter 5 of the AP600 PRA (Revision 0) dated June 26, 1992
- ET-SOAR-PRRA-91-407, "Human Reliability Analysis Guidebook for AP600 Probabilistic Safety Study," dated February 1992 (Section 5 of WCAP-12699, Revision 2)

18.7.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 6, "Human Reliability Analysis," of NUREG-0711. Section 7.4.1, "Human Reliability Analysis Methodology," of NUREG-0711 addresses the technical review of HRA methodology. These criteria were not applied by the staff as part of the HFE review, because this part of the HRA review is being conducted as part of the staff's PRA review addressed in Section 19 of this report. Instead, the HFE review focused on the integration of the HRA with HFE design.

In its response to RAI 620.51, Westinghouse indicated that the HRA implementation plan, the PRA, and HRA are within the scope of design certification. However, the analysis results report for this HRA element of the NUREG-0711 requires a completed function-based task analysis report and is not within the scope of design certification. Therefore, the staff reviewed Westinghouse's HRA at an implementation plan review level, because Westinghouse will not complete work in this area until after design certification.

18.7.2.3 DSER Item Resolution

To address Element 6 open items, Westinghouse first submitted a document entitled "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan" (Westinghouse Implementation Plan) transmitted by fax on May 24, 1995. The NRC staff reviewed this in the summer of 1995, and their results were transmitted to Westinghouse in September 1995. In May 1996, Westinghouse submitted draft WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan." The staff reviewed this new document and reevaluated the open items based upon its contents. The staff described the results of this review in a letter from the NRC to Westinghouse dated June 20, 1996. On July 3, 1996, a follow-up conference call was held between the NRC and Westinghouse to clarify several open issues. By letter dated October 9, 1996, Westinghouse submitted WCAP-14651 (Revision 1), and then Revision 2 on May 8, 1997.

18.7.3 Results

General Criterion: Implementation Plan

*Criterion:* While NUREG-0711 criterion for this element does not explicitly include an implementation plan, such a plan is needed to address the NUREG-0711 criterion-based review to follow. This criterion addresses the availability of an implementation plan in the SSAR.

*Evaluation:*

DSER Evaluation

Based on the material reviewed, Westinghouse did not have an implementation plan for HRA-HFE integration. Such a plan is needed and should consider the information that follows.

The plan should address how and when the HRA will be requantified as the HFE program completes the design. This is especially important because the current HRA/PRA was finished, even though many aspects of the HFE have not yet been completed (for example, function allocation, task analyses, HSI design, procedures, and operator training programs). The HRA did not take into account the human performance effects of the new advanced HSI design because the AP600 HFE design is not complete. The evaluations of these effects have not been completed for the MCR, remote shutdown panel, and local control stations, which could significantly impact the results of the HRA as well as the PRA. The staff's concern over human error probability (HEP) estimation was discussed during meetings with Westinghouse on February 23, and June 14, 1994. Westinghouse calculated very optimistic human error probabilities, considering that no EOPs and ERGs are available, the control room layout has not been well defined, the functional relationship of the senior reactor operator (SRO) and STA has not been well defined, and many significant operator actions require a response in a short timeframe. These concerns were described in RAI 720.276 through RAI 720.278.

Although Westinghouse responded to some of these RAIs, the responses were not submitted to the staff in time to support this stage of the review. An accurate HRA and PRA is important to the HFE process because of their use in determining the critical operator actions. Further, for the newly designed passive plants, such as the AP600, the HRA and PRA are being used for other significant determinations, including resolution of the concerns regarding the regulatory treatment of non-safety systems. Therefore, once the HFE design is complete, it is important to requantify the HRA and PRA, and to reverify decisions made based upon the results of the HRA and PRA. Westinghouse should provide an HRA-HFE integration implementation plan. This was Open Item 18.7.3-1.

FSER Evaluation

In WCAP-14651 (Revision 2), dated May 1997, the various items associated with proper integration of the PRA/HRA and the HFE process are discussed in detail, including use of HRA/PRA insights to guide HFE design, identification of critical human actions and risk important tasks, task analyses for critical human actions and risk important tasks, reexamination of critical human actions and risk important tasks, and validation of HRA performance assumptions. Thus, Westinghouse developed an implementation plan with an appropriate scope. Further, Section 18.7 of the SSAR (Revision 23) references this implementation plan. The acceptability of the individual items is discussed under the evaluations of the following individual criteria.

In Sections 3.2 and 5.0 of the WCAP-14651 (Revision 2), Westinghouse addressed the issue of whether there is a need to reevaluate and possibly requantify the HRA/PRA after the HFE design is complete. Westinghouse stated that performance assumptions will be confirmed as part of both the task analyses and the control room validation. Westinghouse will perform an

evaluation as to whether any of the assumptions of the HRA must be changed. If necessary, the HRA will be modified and the impact on the PRA will be assessed. Reports will be generated documenting the results, which will be submitted to the NRC for review. Based on this information, Open Item 18.7.3-1 is closed and this NUREG-0711 criterion is satisfied.

Criterion 1: Critical Human Actions

*Criterion:* Critical human actions should be identified from the HRA and PRA, and used as input to the HFE design effort. These critical actions should be developed from the Level 1 (core damage) and Level 2 (release from containment) portions of the PRA, including both internal and external events. They should be developed using selected (more than one) importance measures and HRA sensitivity analyses to ensure that an important action is not overlooked because of the selection of the measure or the use of a particular assumption in the analysis.

*Evaluation:*

DSER Evaluation

In its response to RAI 720.133, Westinghouse indicated that the identification of critical human actions is not complete pending the completion of sensitivity analyses. Westinghouse should describe the process that will identify critical human actions for the Level 1 and Level 2 PRA, including both internal and external events, following the completion of sensitivity analyses. This was Open Item 18.7.3-2.

FSER Evaluation

This issue, associated with the identification of critical human actions, was raised in the AP600 review as Open Item 18.7.3-2. It was also raised in the context of the HFE review for DSER Open Items 18.5.3-1 and -2. Westinghouse initially provided responses to these open items in faxes dated April 19, 1995, and May 24, 1995. NRC provided a faxed set of comments on these responses to Westinghouse on June 20, 1995. The Westinghouse responses and NRC comments were discussed in a conference call on June 22, 1995, and the Westinghouse position was further documented in a faxed memo from Westinghouse to NRC dated June 30, 1995. The NRC concerns related directly to the above criterion, were eventually resolved as discussed below. Westinghouse submitted draft WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation," (May 1996), which addressed some, but not all, of the NRC comments and questions on the June 20, 1995 NRC fax to Westinghouse. The main remaining issue was the quantitative threshold for the identification of the critical human actions. On July 3, 1996, a follow-up conference call between the NRC and Westinghouse was held to clarify questions related to critical human actions.

By letter dated October 9, 1996, Westinghouse submitted Revision 1 of WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," and Revision 2 on May 8, 1997.

The critical human actions of the NUREG-0711 are defined to be "tasks that must be accomplished in order for personnel to perform their functions. In the context of PRA, critical tasks are those that are determined to be significant contributors to plant risk." In its Integration

Plan, Westinghouse chose to subdivide the NUREG-0711 critical human actions into two categories, critical human actions and risk-important tasks. However, Westinghouse indicated that they will address both of these types of actions through their HFE design program.

The threshold for defining a Westinghouse critical human action is high. It is any action that, if failed, would result in total core damage frequency (CDF) greater than or equal to 1E-4 events/Rx-year or a severe release frequency greater than or equal to 1E-5 events/Rx-year. With these thresholds, the AP600 has no critical human actions. This is because of the low overall CDF of AP600, the passive nature of the AP600, and the high value of the threshold selected. The staff has accepted Westinghouse's high threshold for defining critical human actions because Westinghouse also defines risk-important tasks in the paragraphs that follow (in a manner acceptable to the staff) and uses them appropriately for other portions of the control room design where critical actions were intended. Also, as indicated in Section 18.2 of this report, because of the high threshold for defining critical human actions, the staff considered an additional task (manual actuation of the ADS) as critical and, as such, a necessary task to be included in the Minimum Inventory of Control Room Controls, Displays, and Alarms. Westinghouse agreed and added this action to the Inventory. It is also the staff's understanding that, although Westinghouse has not identified any critical human actions based on preliminary results from the PRA studies completed in 1996, as PRA studies are updated, critical human actions may be identified.

The thresholds for defining a risk-important task are detailed in the Integration Plan and consist of both quantitative and qualitative criteria. For the determination of risk important tasks, Westinghouse will use the following PRA studies:

- the internal events at-power PRA
- the shutdown events PRA
- the focused PRA for regulatory treatment of non-safety-related systems (RTNSS) analysis
- the external events PRA (for fire and flood events)
- the seismic margins PRA

For the quantitative criteria, Westinghouse will use two importance measures, risk achievement (or risk-increase) worth and risk reduction (or risk-decrease) worth. The threshold for risk-increase importance, for at-power internal events and shutdown events, is 200 percent or a risk achievement worth of 3.0. This will be applied to both the Level 1 (core damage frequency) and the Level 2 (severe release from containment) PRAs. This risk increase threshold was initially proposed by Westinghouse in their draft integration plan and lacking additional details, was not accepted by the staff. Some of the reasons for staff hesitation in accepting this value were as follows. If an applicant sets their risk criteria too high, then there will be very few task analyses that are based on risk. That is, essentially all actions that receive the detailed task analyses prior to HFE design will have been selected based upon engineering judgement. This could defeat the intent of both NUREG-0711 and the PRA. Additionally, a criterion that is based on increasing total CDF by a factor three times for one human action failure could result in a potentially large increase in risk (depending on the original baseline value of risk). These staff concerns were addressed in Revision 2 of the integration plan as described below.

WCAP-14651 (Revision 2) specifies all of the PRAs that will be used in the determination of risk important tasks, defines the quantitative thresholds, adds five well-specified qualitative criteria, and provides example results of risk-important tasks in Appendix A. The latest baseline values of the various PRA studies, as referenced in the integration plan, were determined to range from 6.5E-7 events/Rx-year down to about 2E-10 events/Rx-year. These are low values compared to the PRAs for current day plants. Thus, the AP600 can accept a somewhat higher percentage increase than would be acceptable for current plants. Further, using only the quantitative criteria, the integration plan in Appendix A provides examples of risk-important tasks. Depending on how one converts human action basic events to tasks, there are about 13 to 15 risk-important tasks. This appears to be a reasonable number of risk-defined operator tasks to address in the task analysis portion of the HSI design.

Thus, Westinghouse developed an acceptable approach to define critical human actions and risk-important tasks from the PRA/HRA to be used as input to the HFE design effort. They are developed from Level 1 and Level 2 PRAs and include consideration of both internal and external events. They will be selected using multiple measures and criteria to ensure that important actions are not overlooked.

On the basis of the above information, Open Item 18.7.3-2 is closed and the NUREG-0711 criterion is satisfied.

Criterion 2: Critical Human Actions and Task Analysis

*Criterion:* The details of human performance of critical human actions and their associated tasks and scenarios identified through the initial PRA/HRA should be specifically addressed by Westinghouse in Element 4, "Task Analysis." This will help ensure that these tasks are within acceptable human performance capabilities (e.g., within time and workload requirements).

*Evaluation:*

DSER Evaluation

The methodology for task analysis with respect to treatment of time and workload considerations was identified as part of Open Item 18.5.3-3. Westinghouse should describe the process they will use to address the task analyses for critical human actions. This was Open Item 18.7.3-3.

FSER Evaluation

Section 3.0 of WCAP-14651 (Revision 2) provides a commitment that the Westinghouse AP600 HRA/PRA group will specify human actions and task sequences to be used as input to the task analyses. This will include critical human actions (if any) and risk-important tasks. The human actions and tasks identified by HRA activities will be included in the set of tasks examined using operational sequence task analyses. The analyses will include performance requirements, such as time windows, within which an action needs to be completed. Workload of the operators will also be addressed as discussed in Section 3.2 of the WCAP-14651 (Revision 2). By using this process, the HSI design and procedures will be developed in a manner that can adequately support the critical human actions and risk important tasks.

On the basis of the above information, Open Item 18.7.3-3 is closed and the NUREG-0711 criterion is satisfied.

Criterion 3: Detailed Examination of Critical Actions

*Criterion:* Critical human actions that are identified in the HRA/PRA as posing serious challenges to plant safety and reliability should be *re-examined* by function analysis, task analysis, HSI design, or procedure development to either change the operator task or the control and display environment to reduce or eliminate undesirable sources of error.

*Evaluation:*

DSER Evaluation

The relationship between the HFE function allocation and the modeling of manual human actions should be clarified. For example, in its response to RAI 720.177, Westinghouse discussed manual and automatic valve actuation during reduced inventory operations. Additional information is needed on the impact of HFE function allocations yet to be performed on the HRA.

In its response to RAI 720.118, Westinghouse indicated that the HEPs were not evaluated to account for "the use of advanced digital technology or to account for the role of the operator as a monitor and decision maker rather than performing actions directed by procedures." This approach is inconsistent with the role of the operator that is described in Section 18.6.6 of the SSAR (Revision 0) and operator training in Section 18.9.9.3 of the SSAR (Revision 0). The M-MIS is being designed to support an operator trained as a decision maker, and one who does not accept procedures in an unquestioning manner. It is expected that such an operator might spend additional time following procedures (for information validation and confirmation of procedure appropriateness and adequacy). This should be reflected in the evaluation of critical actions for HEP estimation.

Westinghouse should describe the process that will (1) provide additional information on the impact of HFE function allocations yet to be performed on the HRA, (2) provide detailed evaluations of critical actions to reduce or eliminate sources of error, and (3) clarify the possible inconsistency between the operator role assumptions in the HFE design and the HRA. This was Open Item 18.7.3-4.

FSER Evaluation

Section 4.0 of WCAP-14651 (Revision 2) states that any critical human action or risk important task, that is determined to be a potentially significant contributor to risk, will be re-examined by task analysis, HSI design, and procedure development. These evaluations will be used to identify changes to the operator task or the HSI to reduce the likelihood of operator error and provide for error detection and recovery capability.

Section 3.2 of the WCAP (Revision 2) discusses how the task analyses will be used to address the assumptions used in the HRA by developing more accurate estimates of workload and task completion times. This information will be provided to the Westinghouse HRA/PRA group.

Based on the above information, Open Item 18.7.3-4 is closed and the NUREG-0711 criterion is satisfied.

Criterion 4: Using HRA/PRA Insights

*Criterion:* The use of the HRA/PRA results by the HFE design team should be specifically addressed (i.e., how the HFE program addressed critical personnel tasks through HSI design, procedural development, and training to minimize the likelihood of operator error and provide for error detection and recovery capability).

*Evaluation:*

DSER Evaluation

In its response to RAI 720.117, Westinghouse indicated that "HRA analysts worked together with system designers to perform the individual system analyses used to develop fault trees for the various systems modeled in the PRA, complete the HRA, and finalize the system design." Westinghouse further indicated that specific insights from the HRA were incorporated in the system design, and that the individual system designs were modified to support performance of the modeled operator actions. Dominant cutsets were reviewed to identify sequences where human reliability was a significant contributor to failure. For limiting sequences, changes were made to provide necessary operator-related improvements (design and operation) to eliminate the limiting human failures. HRA was integrated with the development of high-level operator action strategies. However, no examples of the process were provided.

Westinghouse should provide examples of how the HRA/PRA insights were used to improve design and limit risk to human actions and errors and describe the process whereby this effort will continue as part of the HFE design. This was Open Item 18.7.3-5.

FSER Evaluation

As noted in the DSER and in Section 1.2 of WCAP-14651 (Revision 2), Westinghouse has designed the AP600 taking into account lessons learned from existing plant experience, and the results of past HRAs and PRAs. This allowed Westinghouse to reduce the potential for human error. Westinghouse states that this simplifies the plant and reduces the number of human actions required. For example, no human actions are required to maintain core cooling following design-basis events.

Further, Section 1.2 of WCAP-14651 (Revision 2) provides a discussion of how the HRA/PRA results will be used in task analysis, HSI design, procedure development, and V&V to identify changes to operator tasks, procedures, or the HSI to minimize the likelihood of operator error and provide for error detection and recovery capability.

Regarding training, Westinghouse stated that training program development is a COL responsibility. Section 1.2 of the Westinghouse implementation plan discusses how Westinghouse will provide the COL with documentation that includes a description of HRA assumptions, PRA results relevant to training, and insights relevant to training based upon the V&V. This will include a list of critical human actions (if any), risk important tasks, performance requirements for those actions (e.g., response time).

Based on the above information, Open Item 18.7.3-5 is closed and the NUREG-0711 criterion is satisfied.

Criterion 5: HRA Validation

*Criterion:* HRA assumptions such as decision-making and diagnosis strategies for dominant sequences should be validated via walk-through analyses with personnel with operational experience using a plant-specific control room mockup, prototype, or simulator. Reviews should be conducted before the final quantification stage of the PRA.

*Evaluation:*

DSER Evaluation

This issue is not addressed in the methodology described in Chapter 5, "HRA," of the AP600 PRA or the Human Reliability Analysis Guidebook for the AP600 Probabilistic Safety Study (ET-SOAR-PRA-91-407). Westinghouse should describe the process for validation of HRA assumptions and possible revision of the HRA if necessary. This was Open Item 18.7.3-6.

FSER Evaluation

Section 5.0 of WCAP-14651 (Revision 2) discusses the validation of HRA performance assumptions. It states that validation of the HRA operator performance assumptions will be performed as part of the Integrated HFE system validation. This will include scenarios that include critical or risk-important human actions, as well as specific performance assumptions that the HRA/PRA group identifies for confirmation. Westinghouse will not validate the quantitative HRA probabilities. The qualifications of personnel involved in the analyses are identified in WCAP-14651 (pp 5-1, members of the PRA/HRA group with experience acceptable to the staff). Although walk-throughs are not specifically identified in the WCAP, exercises using scenarios are mentioned as part of the validation effort which is conducted as part of the overall Integrated HFE System Validation which incorporates control room walk-throughs and extensive simulator exercises. After review of the results of the validation, the HRA/PRA group will determine whether any changes need to be made to the HRA assumptions or HRA quantification. If changes are needed, the HRA will be modified and the impact on the PRA will be assessed. A report will be generated, documenting the results of the exercises intended to validate the HRA performance assumptions, and submitted to the NRC for review as part of the COL application information provided in COL Action Item 18.7-1.

Based on the above information, Open Item 18.7.3-6 is closed and the NUREG-0711 criterion is satisfied.

18.7.4 Conclusions

The objectives of this review are to ensure that (a) the HRA activity effectively integrates the HFE program activities and PRA/risk analysis activities, and (b) the applicant has addressed human error mechanisms in the design of the plant HFE (i.e., the HSIs, procedures, shift staffing, and training in order to minimize the likelihood of personnel error and to provide for error detection and recovery capability). HRA was reviewed at an implementation plan level of detail.

The staff identified several open items. These items were acceptably addressed and the staff has completed its review of Element 6, "Human Reliability Analysis," of NUREG-0711.

Westinghouse developed an acceptable implementation plan for integrating HRA with HFE for the AP600 design. The COL applicant referencing the AP600 certified design is responsible for the execution and documentation of the human reliability analysis/human factors engineering integration implementation plan. This is COL Action Item 18.7-1.

## 18.8 Element 7: Human-System Interface Design

This section discusses the results of the staff's review of Westinghouse's process for HSI design. A detailed review of the specific features of the HSI (such as the alarms, displays, and controls of the control room and the remote shutdown station) was beyond the scope of this review because the HSI design features will not be completely developed by Westinghouse by the time of design certification. Therefore, the staff's review addressed the HSI design process methodology and was conducted at an implementation plan review level. Included in the HSI review was the safety parameter display system (SPDS). Although the MCR is not fully designed, the staff evaluated Westinghouse's approach to meeting the functional requirements for the SPDS (see Section 18.8.2 of this report).

### 18.8.1 HSI Design Process

#### 18.8.1.1 Objectives

The objective of this review is to evaluate the process by which HSI design requirements are developed, and HSI designs are selected and refined. The review should ensure that the applicant has appropriately translated function and task requirements to the controls, displays, and alarms that are available to the crew. The applicant should have systematically applied HFE principles and criteria (along with all other function, system, and task design requirements) to identify HSI requirements, select and design HSIs, and resolve HFE/HSI design problems and issues. The process and rationale for the HSI design (including the results of trade-off studies, other types of analyses and evaluations, and the rationale for selection of design and evaluation tools) should be documented for review.

#### 18.8.1.2 Methodology

##### 18.8.1.2.1 Material Reviewed

The used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-9817, (Revision 2) dated June, 1991
- WCAP-12601, (Revision 15) dated April 1, 1995
- WCAP-14396, (Revision 1) dated August 12, 1996
- WCAP-14396, (Revision 2) dated January 27, 1997

- WCAP-14401, (Revision 2) dated August 8, 1996
- WCAP-14401, (Revision 3) dated May 8, 1997
- WCAP-14822, (Revision 0) dated February 25, 1997
- WCAP-14695, (Revision 0) dated July 23, 1996
- Procedure AP-3.1, AP600 System Specification Documents (SSDs), (Revision 1), February 28, 1991
- Procedure AP-3.2, Design Configuration Change Control, (Revision 3), March 11, 1994
- Procedure AP-3.6, (Revision 2), March 11, 1994
- Sample design documents

18.8.1.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 7, "Human-System Interface Design," of NUREG-0711. The staff reviewed Westinghouse's HSI design at an implementation plan review level, because Westinghouse will not complete work in this area until after design certification.

18.8.1.2.3 DSER Item Resolution

Element 7 is being reviewed at an Implementation Plan Review level. Therefore, Westinghouse's submittals should describe the proposed methodology in sufficient detail for the staff to determine whether implementing the methodology will lead to products that meet NUREG-0711 acceptance criteria for the element. The actual completion of the plan will then take place after design certification. While some implementation plans can be reviewed on their own merits, the staff may request a sample analysis that demonstrates the application of the methodology and its results. ITAAC are needed for completing the implementation plan and providing the results to the staff for review.

A meeting was held in Pittsburgh, PA, on March 8 through 10, 1995, to discuss Element 7 open items. As part of the discussions, Westinghouse agreed to make design process documentation and sample design process products, such as HFE guidelines documents, available for staff review. A review of this documentation was conducted on April 5 and 6, 1995, at the Westinghouse office in Rockville, MD. On the basis of this review and using information obtained in the meeting in Pittsburgh, the status of the open items was reviewed. Insights and clarifications based on the review and meeting also led to a reevaluation of specific material contained in the SSAR. All three sources of information contributed to the review of the Element 7 open items. As a result of the review, several open items were closed. The results of the review were sent to Westinghouse in a letter dated July 25, 1995.

To address the remaining open items, Westinghouse submitted SSAR (Revision 23) Section 18.8, "Human-System Interface Design." They also submitted WCAP-14396 (Revision 2), "Man-in-the-Loop Test Plan Description," to address the AP600 HFE test program.

18.8.1.3 Results

Criterion 1: HSI Design Process Guidance

*Criterion:* The HSI design process should be organized and documented to support its standardized and consistent use by the members of the design team and their contractors. Guidance should be provided to the team for accomplishing the following tasks (each of which is defined in the criteria that follow):

- task-related HSI requirements
- general HSI design
- detailed HSI design
- HSI evaluation
- final HSI design documentation

*Evaluation:*

DSER Evaluation

The M-MIS design implementation process is described in Section 18.8.2.1.3 of the SSAR (Revision 0). According to Westinghouse, "specific implementation guidance is provided to the M-MIS subsystem designers so that each designer implements the function-based task analysis outputs consistently and according to human engineering principles established for the design." A subsystems integration document is also provided because "each of these subsystems provides only a portion of the support required from the complete interface." The process by which the design will be evaluated is described in Section 18.8.2.3.2 of the SSAR (Revision 0). According to Section 18.8.2.3.4 of the SSAR (Revision 0), the results of these evaluations will allow conclusions to be drawn regarding "the effectiveness of particular M-MIS features in supporting human performance; the factors that contribute to human performance difficulty; and enhancement to the M-MIS required to improve human performance." The specific means are not discussed by which the conclusions will provide feedback to the design process (e.g., the process by which the conclusions are communicated to the designers and the method for establishing that any design changes address the conclusions). The process is not described for reflecting the results of the evaluations in the design guidance and incorporating changes into the final design documentation.

In its response to RAI 620.40, Westinghouse stated that implementation guideline documents, subsystems integration documents, and design-basis guideline documents will not be completed until after design certification. Similarly, in its response to RAI 620.34, Westinghouse stated that the documentation that will guide the COL applicant in making changes to the M-MIS will be available at the time of COL application. Westinghouse did not describe the process by which these documents will be developed.

Westinghouse should describe how evaluation results will be communicated to designers, incorporated into design guidance, and reflected in final design documentation. The process by

which implementation guidance will be developed must also be described. This was Open Item 18.8.1.3-1.

FSER Evaluation

SSAR (Revision 23) Section 18.8, "Human System Interface Design," addresses the design of the HSI based on task analysis and other design inputs. It provides a general description of the translation of task requirements to HSI resource requirements, the procedures for development and documentation of the detailed design, and design tests and evaluations. To support a more in depth examination of the design process, the staff reviewed the following Westinghouse documents describing the AP600 design process on April 5 and 6, 1995, at the Westinghouse office in Rockville, MD:

- WCAP-12601, "AP600 Program Operating Procedures," (Revision 15, dated April 1, 1995)
- WCAP-9817, "Design Review Manual," (Revision 2, dated June, 1991)
- a sample document illustrating a design review

Westinghouse addressed Criterion 3 with a revision to WCAP-14396 (Revision 2) and Revision 22 to SSAR Section 18.8.1.9, "Human System Interface Characteristics: Identification of High Workload Situations," (see discussion under Open Item 18.8.1.3-3: Human System Interface Characteristics below).

In addition, Westinghouse submitted WCAP-14822, "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8" (see discussion of WCAP-14822 in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures, in Section 18.2.3.3 of this report).

The staff has reviewed WCAP-14822 and found that it incorporates the design review procedures noted in the evaluation of Criterion 5 (HFE Documentation), Section 18.2.3.3 of this report (HFE Process and Procedures), and contributes to the resolution of this issue.

Based on this information, Open Item 18.8.1.3-1 is closed and the NUREG-0711 criterion is satisfied.

Criterion 2: HSI Design Scope

*Criterion:* The scope of the HSI design should include the following factors:

- the overall work environment
- work space layout (e.g., control room and remote shutdown facility layouts)
- control panel and console design
- control and display device layout

- information and control interface design details, such as graphic display formats, symbols, dialogue design, input methods, and so forth.

*Evaluation:*

DSER Evaluation

The design process described in Section 18.8.2 of the SSAR (Revision 0) indicates that the HSI design will include the alarm system, display system, controls, procedures, workstation layout, and control room. This scope is consistent with the criterion. This SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23), Section 18.8, "Human System Interface Design," indicates that an implementation plan for the design of the non-HSI portion of the plant is provided. The scope of the HSI design includes the operation and control centers (main control room, remote shutdown room, local control stations, technical support center, and all associated workstations for each area) and each of the HSI resources covering, for example, the alarm system, wall panel information system, and soft/dedicated controls.

The staff noted in its review of Revision 22 of the SSAR that the definition of the AP600 operations and control centers (OCS) in SSAR Section 7.1.1 was inconsistent with the definition of OCS in SSAR Section 18.8. Westinghouse stated that the definition of OCS in SSAR Section 18.8 was the correct definition and that SSAR Section 7.1.1 would be revised to be consistent with SSAR Section 18.8. This was FSER Confirmatory Item 18.8-1. Revision 24 of the SSAR provided a corrected definition of the OCS in SSAR Section 7.1.1 and, therefore, Confirmatory Item 18.8-1 is closed.

Although the SSAR reviewed by the staff in its FSER evaluation was changed from the SSAR reviewed for the DSER, the staff's evaluation and conclusions were not altered. Based on this information the NUREG-0711 criterion is satisfied.

Criterion 3: Task-Related HSI Requirements

*Criterion:* This criterion addresses the identification of the HSI requirements to support human functions and tasks using the results of earlier NUREG-0711 elements as a basis. The requirements should address alarms, displays, controls, and operator aids. For example, the range and accuracy of displayed information should be consistent with operator information requirements for making decisions regarding the plant state. Precision requirements for the display of plant information (e.g., the number of demarcations on a scale) should be defined to a level that is consistent with task requirements without burdening the operator with unnecessary detail (e.g., an excessive number of decimal places). Units of measurement should be defined to be consistent across related operator tasks (e.g., operators should not have to convert values from one measurement system to another). The technical basis for task-related HSI requirements should be documented.

*Evaluation:*

DSER Evaluation

Westinghouse described the function-based task analysis as a method for identifying control and displays needed for operator tasks. In its response to RAI 620.81, Westinghouse indicated that design reviews will identify omissions. Additional opportunities for verifying the completeness of the design (e.g., cross-checks against emergency procedure guidelines) should be identified. The process by which the correction of omissions is ensured in the final design should be described.

The function-based task analysis presented in Sections 18.8.2.1.2 and 18.9.1.3 of the SSAR (Revision 0) provides a structured approach for identifying information and controls that are required for performing specific functions. While the example provided in Section 18.9.1.3 of the SSAR (Revision 0) describes how parameters and specific values are defined, it is not clear how the range, accuracy, precision, and measurement units for individual displays and controls will be defined. The means by which these items are defined in the initial stages of the design process should be described.

Westinghouse should describe the process by which possible omissions in controls and displays are eliminated from the final design. The means by which features of controls and displays are initially defined must also be described. This was Open Item 18.8.1.3-2.

FSER Evaluation

SSAR (Revision 23) Section 18.8.1.7, "Task-Related Human System Interface Requirements," addresses the derivation of HSI requirements from task requirements. The task analyses to be performed in support of AP600 HSI design include "traditional" task analyses using an OSA methodology in addition to the FBTAs, as discussed previously. The staff reviewed the methodology for OSA and found that the OSA is developed for a representative set of operational and maintenance tasks and addresses the intent of NUREG-0711 criteria for task analysis. Therefore, the staff finds it acceptable.

Included in the information obtained from these task analyses is the identification of operational information requirements (e.g., the alarm, parameters, and controls needed to perform the task sequences). This information is used to develop descriptions of the HSIs. For example, a description may include detailed information of what the display needs to provide the operator to complete a task. The description includes the necessary calculated values and supporting algorithms to support the operators' task requirements.

Based on this information, Open Item 18.8.1.3-2 is closed and the NUREG-0711 criterion is satisfied.

Criterion 4: HSI Characteristics

*Criterion:* The HSI should provide the task-required alarms, displays, controls, and operator aids (as defined in this section in Criterion 3, "Task-Related HSI Requirements") for process

monitoring, decision making, and control. The HSI design should support human performance and usability through the following characteristics:

- compatibility with the cognitive and physiological capabilities of plant personnel
- minimization of the demands of secondary tasks (i.e., those activities performed when interfacing with the system, but not directed to the primary task of process monitoring, decision-making, and control). Examples, include activities that the operators must engage in to manage the interface, such as navigating through displays, managing windows, and accessing data (Although sometimes necessary, performing secondary tasks detracts from the crew's performance of primary tasks.)
- support for the use of the HSI, such as providing flexibility (e.g., multiple means to carry out actions or verify automatic actions), guidance on HSI use, and error tolerance and mitigation
- accommodation of human performance under the range of conditions encompassing normal as well as credible extreme conditions. (The design process should take into account the use of the HSI over the duration of a shift and in plausible scenarios that may result in reduced visibility and ventilation or CR evacuation. The design of non-CR HSIs, such as local control stations, should address constraints imposed by the environment (e.g., noise, temperature, contamination) and by protective clothing.)

*Evaluation:*

DSER Evaluation

The staff concludes that provisions have been made to assess the effects of interface management on operator performance based on examining the description of evaluation issues in Section 18.8.2.3.5 of the SSAR (Revision 0). For each of the major classes of operator activity, there are evaluation issues in which the dependent measures include indicators of the accuracy and efficiency of the use of displays, controls, or procedures. The workload associated with secondary tasks is not discussed in the context of the evaluation issues. In its response to RAI 620.84, Westinghouse stated that "measures of workload (including mental workload) will play a role in the integrated validation study" because these measures are most meaningful "when realistic and complete operator tasks are being studied." Either the subjective workload assessment technique (SWAT) or the NASA task load index (TLX) technique will be used to assess workload in the integrated validation study. However, high workload may also be imposed in the course of "part-task" evaluations, and provisions are not described for detecting workload-related problems early in the design process.

The SSAR (Revision 0) did not describe specific features of the HSI designed to enhance usability. The guidance to be provided to designers for correcting usability problems identified in the course of HSI evaluations should be described.

The description of the control room in Section 18.9.1 and Figure 18.9.1-1 of the SSAR (Revision 0) indicated that the operators will be sitting at individual workstations for extended periods of time. This contrasts with conventional control rooms in which operators often stand or walk about the control room to access information and perform control actions. Possible

negative effects of such an arrangement (e.g., postural or visual fatigue, or loss of alertness) should be considered in comparison with other design alternatives. Evaluations of similar workstations in other work environments should be consulted or performed. Design rationales should be documented, and features of the design intended to mitigate negative aspects should be described.

Section 18.8.2.1.3.4 of the SSAR (Revision 0) stated that guidance documents will direct the layout of workstations, the arrangement of the control room, and the area environmental requirements. These documents are not among those available for review. The description of these documents indicates that they will provide guidance in the context of activities and requirements of the operating crew as determined by the operations tasks model, and will contain references to source material. The content description did not mention degraded control room conditions or environments outside the control room. The design-basis environmental conditions in which the plant would still be operated from the control room should be specified, and the likely effects on operator performance should be considered. Westinghouse should also demonstrate that the design will support the required performance under such conditions. In the event of an evacuation of the control room, monitoring and control is performed from the remote shutdown room, as discussed in Section 18.8.2.1.1.2.4 of the SSAR (Revision 0). Section 18.11 of the SSAR (Revision 0) indicated that the environmental conditions of the remote shutdown room are specified such that human and machine performance will not be degraded. Design information and criteria for some aspects of the environment (illumination; heating, ventilating, and air conditioning (HVAC); and shielding) are addressed elsewhere in the SSAR (Revision 0). This section also stated that proper acoustic criteria will be used, but did not cite any specific standards. References to appropriate standards should be provided.

Local control stations are described in Section 18.8.2.1.1.2.8 of the SSAR (Revision 0), which states that the use of local control stations during normal and emergency operations "is consistent with the overall operator staffing and performance considerations developed from the task analysis." In its response to RAI 620.82, Westinghouse indicated that critical local actions will be identified during the design process. These actions will be included in the verification and validation plan. Local control stations are described as "habitable areas" and the same term is used to describe the MCR. There is no further discussion of the environmental conditions at local control stations, nor of how the design will accommodate these conditions. A process should be established whereby the worst credible conditions at each local control station are identified, and the effects on operator performance considered. The means should be specified by which the negative effects of environmental factors (e.g., noise, heat, and radiation sources) and protective clothing (e.g., noise protectors, respirators, and gloves) are addressed in the design of these local control stations.

Westinghouse should describe how potential problems associated with high workload will be identified early in the design process, and how the concerns noted in the evaluation above will be addressed. Westinghouse should also describe how the design of workstations (inside and outside the MCR) ensures support of optimal operator performance under a range of conditions. This was Open Item 18.8.1.3-3.

FSER Evaluation

On June 7, 1995, Westinghouse provided a draft response to this open item. Westinghouse described how situations of high workload would be identified early in the design process through the use of analytic techniques and part-task simulations, as referenced in OCS-T5-001, "Man-in-the Loop Test Plan." The test plan will specifically address the impact on operator performance of secondary tasks associated with display navigation and management. Westinghouse committed to provide design guidance for correcting usability problems encountered in the course of HSI evaluations and referenced accepted industry guidance documents and a Westinghouse-specific document (OCS-J7-001) to direct the layout of workstations, the control room, remote shutdown room, local control stations, and the areas' environmental requirements.

The response to RAI 620.84 was incorporated into SSAR (Revision 9), Section 18.8.1.9, "HSI Characteristics: Identification of High Workload Situations." OCS-T5-001 was submitted in final form as WCAP-14396 (Revision 1), "Man-in-the-Loop Test Plan Description." Two problems were noted. First, the information in the RAI response was not included in the SSAR in detail but was summarized. In the summary, the description of approaches to subjective workload measurement were not included. Thus, the revised description does not suggest an approach to workload assessment beyond indicating that subjective techniques will be used.

Second, the SSAR indicated that the concept tests will include assessments of workload for the impact of secondary tasks such as display system navigation. The staff considers this important because of concerns over the potential for such tasks to impose high workload and to be distracting from operators' primary tasks of monitoring and controlling the plant. However, the associated test described in WCAP-14396 (Revision 1) did not include workload as performance measure. Section 4.2 of the WCAP addresses the tests to be performed for workstation displays. Concept Test 4: "Ability to navigate displays, finding information" addresses the staff's concern, but workload is not identified as a performance measure. In fact, workload was only mentioned in conjunction with one of the concept tests (Test 3) defined in WCAP-14396 (Revision 1).

The staff asked Westinghouse to clarify the measurement of workload and its use in the concept tests to resolve this open item. Westinghouse provided clarification in WCAP-14396 (Revision 2) and SSAR (Rev 23) Section 18.8.1.9, "HSI Characteristics: Identification of High Workload Situations." Westinghouse revised WCAP-14396 to include the assessment of workload to the list of performance measures in Concept Test 4. The SSAR revision identified that a workload assessment method such as SWAT, NASA-TLX, or equivalent would be used.

Based on this information, Open Item 18.8.1.3-3 is closed and the NUREG-0711 criterion is satisfied.

Criterion 5: General HSI Design Feature Selection

*Criterion:* This criterion addresses the selection of general HSI design features, such as the selection of a large screen MCR display panel (compared to workstation displays only) or use of touch screen controls (compared to hard controls or trackballs). The selection of general features should be based on a consideration of alternative approaches for addressing the HSI design characteristics, as identified in this section in Criterion 4, "HSI Characteristics."

Evaluation methods can include operating experience and literature analyses, trade-off studies, engineering evaluations and experiments, and benchmark evaluations. Such evaluations should consider the strengths and limitations of design options. The process for evaluating alternatives should be documented and include the justification for their final selection.

*Evaluation:*

DSER Evaluation

Section 18.8.2.3.2.1 of the SSAR (Revision 0) describes the following M-MIS features as "central" to the AP600 design:

- wall panel information station
- functionally organized alarm system
- compact workstations
- functionally and physically organized workstation displays
- computer-based procedures
- plant communication system

These features "are used as a starting point to define how the M-MIS is intended to support operator performance..." In its response to RAI 620.41, Westinghouse indicated that the central elements of the HSI design were established based on a "comprehensive model of operator performance" that incorporates information from a variety of sources (e.g., reports of problems with current control technology, studies of human performance, Westinghouse expertise, and industry experience as discussed in the EPRI ALWR URD).

Section 18.8.2.3.2.4 of the SSAR (Revision 0) reviews the "rationale for each M-MIS feature" (that is, the wall panel information station, functionally organized alarm system, compact workstations, functionally and physically organized workstation displays, computer-based procedures, and plant communication system). For each operator activity identified by Westinghouse (detection and monitoring, interpretation and planning, and controlling plant state), the SSAR (Revision 0) describes the ways in which the relevant features support the activity. However, there is no explicit consideration of possible limitations of the design features, and the reason(s) for choosing these features over other potential alternatives is not specified.

Additional information is needed on the process Westinghouse will use to evaluate design alternatives (e.g., documentation of decisions based on studies of human engineering trade-offs, tests of alternatives, and evaluations of previous applications).

Westinghouse should describe the process used to evaluate design alternatives identified in the staff's evaluation. This was Open Item 18.8.1.3-4.

FSER Evaluation

SSAR (Revision 23) Section 18.8.1.8 addressed this item. The SSAR states that the HSI resources identified were selected as a starting point for meeting the information and control needs for general human activities (such as detection, planning, and control) identified in the operator decision making model (described in WCAP-14695). The relationship between the

human activities and the control room resources are described in SSAR (Revision 23) Figure 18.8-3. For example, detection and monitoring are supported by the alarm system, the wall panel information system, the Qualified Data Processing System (QDPS) and the plant information system. The principal source for the initial selection was utility requirements and operating experience review. The acceptability of each resource and the evaluation of design alternatives for the detailed implementation of each resource is accomplished through the test and evaluations that are performed during concept testing and final V&V. The results of testing will be used to refine the design. The basis of all resource design decisions will be documented in the functional design documentation.

Based on this information, Open Item 18.8.1.3-4 is closed and the NUREG-0711 criterion is satisfied.

Criterion 6: Guidelines for Detailed HSI Design

*Criterion:* The applicant should use HFE guidelines for the detailed design of the selected general HSI features, layout, and environment. This will facilitate the standard and consistent application of HFE principles to the detailed design. Generic HFE guidance documents should be tailored to the applicant's specific HSI design and documented in a guidance or specification document. HFE guidance documents should contain statements of their intended scope, references to source materials, instructions for their proper use, and procedures to be followed when discrepancies are found.

*Evaluation:*

DSER Evaluation

Section 18.8.2.1.3 of the SSAR (Revision 0) stated that guidance documents are provided to designers of the alarm system; the information display system; the controls interface; and the workstation and control room layout, arrangement, and environment. In Figure 18.8.2-1 of the SSAR (Revision 0) (as well as Westinghouse's response to RAI 620.59), the following six guideline documents are identified:

(1) alarm guidelines
(2) display guidelines
(3) controls guidelines
(4) training guidelines
(5) anthropometric guidelines
(6) guidelines for integration of subsystems

In its response to RAI 620.59, Westinghouse stated that the guidance will be developed from existing guidelines documents, supplemented as necessary "to address issues that are not covered sufficiently." Section 18.8.2.3.5.4.1 and Sheet 25 of Table 18.8.2-2 of the SSAR (Revision 0) cite as sources NUREG-0700, MIL-STD-1472, ASHRAE 55-1981, ANSI/HFS-100, and EPRI NP-3659, although limited applicability of NUREG-0700 is noted. In its response to RAI 620.20, Westinghouse indicated that supplementary material can be drawn from a variety of sources (e.g., research on the psychology of graphic displays and ecological interfaces, lessons learned from the experience of the aerospace industry with automation, research on navigation of computer displays, experience in the design of expert systems, and techniques for cognitive

modeling of operator performance). The response indicated that Westinghouse has developed a display design handbook and alarm design guidelines based on such sources (see also Westinghouse's response to RAI 620.49). In its response to RAI 620.59, Westinghouse stated that guidance will be "tailored to the AP600 interface" and "may include guidance and principles developed from Westinghouse human factors research." Westinghouse's response to RAI 620.83 suggested that the results of early concept tests may also contribute to the tailored guidance.

In its response to RAI 620.90, Westinghouse stated that a plant labeling guideline will be developed that will be based on EPRI NP-6209.

Although Westinghouse's responses to RAI 620.43 and RAI 620.76 indicated that some AP600 human factors design documentation is currently complete, the documents referenced by the applicant were not available to the staff in time for review and integration into this evaluation. A copy of the display design handbook was requested in RAI 620.59, but was not made available to support this stage of the review.

Westinghouse should provide the requested handbook and guidelines as samples of the results of the process. This was Open Item 18.8.1.3-5.

FSER Evaluation

To address this open item, Westinghouse made examples of their design guidance available for staff review. The staff reviewed these detailed guideline products as samples of the products of the Westinghouse design process. Because they were not AP600-specific documents, the detailed contents, (e.g., the actual guidelines themselves) were not reviewed. These documents were reviewed in terms of statements of their intended scope, references to source materials, instructions for their proper use, and procedures to be followed. Development and implementation of the AP600 design specific guidelines are subject to ITAAC.

One document provided guidance on display design. It identified an approach to display design that goes beyond a presentation of guidelines. The guidance is fairly general and does not represent an AP600-specific application. The staff reviewed a plant-specific document (not AP600) which provided an example of how the general display features are implemented (discussed in the next paragraph below). The general principles document provides a clear statement of its application and identifies many of the inadequacies of other guidance documents. It addresses the general aspects of display design and provides comprehensive treatment, for example general principles; display "atoms" (such as font size and coding); display elements (such as labels, icons, and units); formats (such as text, tables, trend plots, and mimics); and the integration of formats into higher-level displays. The organization of the total set of displays is addressed as well. The document provides a clear rationale as to the basis for the guidance. This is a positive feature that should facilitate its use by designers in evaluating tradeoffs. The document also contains numerous graphics and illustrations providing examples of the design principles that will further support its use by the design team. References to numerous appropriate source documents are included such as the Boff Human Engineering Compendium; Smith and Mosier; Tufte, 1983; Helendar, 1988; and NUREG-0700.

The staff also examined more detailed design-specific display guidance document which identified and presented display types in a hierarchal manner. The goal of each display was identified along with what information was presented (e.g., status, values, reliability), and pokefields (fields on the displays that access additional displays). The way the information is to be displayed was also specified. Numerous displays designed in accordance with the design standard were provided.

The staff also reviewed an alarm system design guideline which was a very comprehensive document that addresses alarms from the perspective of their role in plant operations and not simply the end-point design. For example, the document addresses the historical problems with alarm system design (e.g., identifying alarms in bottom-up fashion by the designers of individual components and systems). This method provides a different perspective of the plant from viewing it as an integrated whole or complete with an integrated alarm system. Further, individual system designers are inclined to create alarms without thinking about the operator actions with which the alarm should be associated. To address this problem, a combination of top-down and bottom-up provides a merger. Top-down refers to a definition of alarms to support operator functional and tasks.

The alarm system document contained guidelines on alarm identification for use by HSI designers (top-down alarms) and plant system designers (bottom-up alarms). The information that should be included in each proposed alarm was identified. The technical basis for the alarm guidance included references to numerous appropriate sources such as EPRI 3448, ALWR URD (1989); Van Cott and Kinkade; IEEE 1023-1988; NUREGs-0737, -0696, -0800, -1342; and RG 1.97.

In conclusion, the Westinghouse design process provides for the development of comprehensive detailed design guidance and provides sufficient information to support its standard and consistent application. The application of the process to AP600 guidance is addressed in SSAR (Revision 23) Section 18.8.1.2, Design Guidelines. The specific commitment to develop HSI design guidance for each HSI resource is identified. A general description of the content of the guidance documents is provided and includes: intended scope, references to sources, instructions for use, design conventions and guidelines, and provisions for guideline deviations based on a documented rationale.

Based on this information, Open Item 18.8.1.3-5 is closed and the NUREG-0711 criterion is satisfied.

Criterion 7: Analysis for Detailed HSI Design

*Criterion:* Design details, problems, and issues that are not well defined by guidelines, or where guidelines conflict, should be analyzed. Analysis methods can include operating experience and literature analyses, trade-off studies, engineering evaluations and experiments, and benchmark evaluations. For example:

- Mockups and models may be used to resolve access, workspace, and related HFE problems, and incorporate these solutions into system design.

- Dynamic simulation and HSI prototypes should be considered for use to evaluate design details of equipment requiring critical human performance or equipment not adequately addressed by guidelines.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.20, Westinghouse acknowledged that "no formally documented guidance exists to address many of the advanced control room design issues," because, in large part, most guidance documents maintain a conservative standard with respect to the basis for the guidance. In its response to RAI 620.59, Westinghouse stated that elements of the design may be based on "guidance and principles developed from Westinghouse human factors research." As indicated in Westinghouse's response to RAI 620.83, the results of evaluations (especially early concept tests) will be important in resolving issues not well defined by available guidance.

Westinghouse should describe in more detail the analysis methods by which design issues not covered by available guidance are identified and resolved. In particular, Westinghouse should describe the means by which evaluation results are translated into design guidance (see Criterion 1, "HSI Design Process Guidance," in this section). This was Open Item 18.8.1.3-6.

FSER Evaluation

Westinghouse clarified, in discussions, that the evaluation issues discussed in SSAR (Revision 0) Section 18.8.2.3.5, "Evaluation Issues and Descriptions," represented design details, problems, and issues that are not well defined by guidelines and which are being addressed through the evaluation test program. A total of 17 issues were identified. The last two of these are part of V&V and, therefore, are addressed in the staff's V&V review (see the Element 10 review). The remaining 15 issues address significant HFE topics. They are organized into three groups based on the type of operator activity being analyzed: detection and monitoring; interpretation and planning controlling the plant state. Issues such as use of wall panel and workstation displays to support situation assessment and use of alarm information during multi-fault events will be evaluated. Based upon the staff's understanding of the human performance issues and guideline limitations as discussed in NUREG/CR-5908, "Advanced Human-System Interface Design Review Guideline," this list appears to be comprehensive in scope.

Each issue was discussed with respect to conceptual and performance testing phases. For each, the information generally provided: the hypotheses, experimental manipulations, subject characteristics, minimum tested requirements, measurements and performance criteria, timing (when in the design process the test should be conducted), and use of the results. The comprehensive approach to analyzing human performance issues not addressed by guidance should appropriately address these issues.

The feedback provided to the design process for each of the evaluations was described. For example, the results from Evaluation 1 will be used to contribute to the development of functional

requirements for the design of overview displays for the wall panel information station and workstation.

The material used to address the DSER issue has been incorporated into SSAR (Revision 23) Section 18.11, "Human System Interface Design Test Program," and in WCAP-14396 (Revision 2), "Man-in-the-Loop Test Plan Description." The presentation is slightly changed from the earlier material reviewed. For example, the tests are not described in terms of conceptual and performance phases and the information provided for each is slightly changed. However, the changes do not negatively impact the quality of the material.

Based on this information, Open Item 18.8.1.3-6 is closed and the NUREG-0711 criterion is satisfied.

Criterion 8: HSI Evaluation

*Criterion:* The HSI should be evaluated in an ongoing effort to ensure its acceptability for task performance and conformance to HFE criteria, standards, and guidelines. Special attention should be given to those HSIs that are unique or safety-related. This should be done to ensure that poor design solutions do not remain undetected until Element 10, "Human Factors Verification and Validation," is implemented, at which time design changes become more difficult.

Aspects of the HSI that are at variance with design guidance or for which HFE guidance is lacking should be analyzed. The applicant may use many means to resolve these issues, including operating experience and literature analyses, trade-off studies, engineering evaluations and experiments, and benchmark evaluations.

Evaluations should be conducted to ensure that the HSI includes all information and controls required to perform operator tasks, and that extraneous controls and displays not required for the accomplishment of any tasks are excluded. The outcomes of these evaluations and rationale for resulting design decisions should be documented and available for review.

*Evaluation:*

DSER Evaluation

According to the SSAR (Revision 0), evaluation of the conformance to standards and guidelines is conducted "throughout the functional requirements phase of the M-MIS design process." The SSAR (Revision 0) did not mention evaluations against tailored "guidelines" (see Criterion 6, "Guidelines for Detailed HSI Design," in this section) provided to the designers of each subsystem (see Section 18.8.2.1.3 of the SSAR, Revision 0). In RAI 620.59, the staff questioned whether the general design guidelines cited by Westinghouse, taken together, were sufficiently comprehensive; and recommended using tailored guidance in the evaluations. In its response to RAI 620.59, Westinghouse indicated that tailored guidance will be used in the evaluations. The adequacy of such guidance for these evaluations will depend on the degree to which their development meets Criterion 6.

Section 18.8.2.3.5.4 of the SSAR (Revision 0) indicated that the experimental evaluations discussed above will be performed in two stages, namely concept testing and acceptance

testing. The evaluation of the M-MIS concepts against human engineering guidelines is said to occur at "various stages" in the development process. In its response to RAI 620.20, Westinghouse referred to design reviews for each of the interfaces "at major milestones in their development." Criteria should be established for identifying unique or safety-related HSIs, and for planning the stages at which HSI design elements are evaluated against human engineering guidelines.

In its response to RAI 620.59, Westinghouse further stated that the design guidance will specify some design decisions, but will be "written at a fairly high level" to allow a knowledgeable designer to consider trade-offs when necessary. No formal process for identifying or documenting the resolution of design issues was mentioned.

In its response to RAI 620.81, Westinghouse stated that the availability of controls and displays defined by the task analysis is ensured by the design review of the displays and controls, which will "identify if any information determined necessary by the task analysis has been left out." The response also indicated that the proposed indications and controls that might be recommended by the system designers for any given location are "filtered through the task analysis and, if found unnecessary to support specific tasks identified for that given location, they are deleted."

The approach to defining major issues on which to evaluate the M-MIS design is described in Section 18.8.2.3.2.5 of the SSAR (Revision 0), which organizes the issues according to the three major classes of operator activity, and centers on the aspects of the M-MIS designed to support the activity. Within each activity group, the issues consider either single or multiple features in either straightforward or complex situations. Because of the scarcity of guidance for the design of advanced control rooms, these evaluations are an important part of the design process. This is reflected in the detailed specification of the test plans (e.g., hypotheses, test bed and subject requirements, manipulations, dependent measures) for each issue. To the extent the evaluations are not exhaustive (i.e., every display, procedure, or control is not exercised under all conditions), the rationale for selecting those that are included in the evaluation plans should be discussed, and a plan for taking into account the implications of the evaluations in the overall design should be described.

Westinghouse should describe the rationale for the HSIs, design elements, and procedures selected for evaluation, and for the points in the design process at which the evaluations are to occur. Westinghouse should also describe the process for identifying and resolving conflicts in guidance, as well as the rationale for design decisions that conflict with guidance. This was Open Item 18.8.1.3-7.

FSER Evaluation

As indicated in the review of criterion 6 above, Westinghouse made examples of their design guidance available for staff review. It was concluded that the Westinghouse design process provides for the development of comprehensive detailed design guidance and provides sufficient information to support its standard and consistent application. As was identified in SSAR Section 18.8.2.3.5.4.1, "Evaluation Issue 16," this guidance will be used to evaluate the design against HFE guidelines at various stages of design development. Thus, the aspect of the criterion addressing use of HFE guidelines in the evaluation was acceptably addressed.

A second part of the criterion is the use of analysis for aspects of the HSI that are at variance with design guidance or for which HFE guidance was lacking. As was discussed with respect to Criterion 7 above, and based upon discussions held with Westinghouse, the role of the evaluation issues discussed in SSAR Section 18.8.2.3.5, "Evaluation Issues and Descriptions," was clarified. These evaluations will address aspects of the design that cannot be resolved using available HFE guidance. These evaluations will also take place at various points in the design process. Thus, the part of the criterion addressing use of analyses in the evaluation is acceptably addressed.

The third part of the criterion is to evaluate the design to ensure that the HSI includes all information and controls required to perform operator tasks and that extraneous controls and displays not required for the accomplishment of any tasks are excluded. This type of evaluation did not appear to be discussed by Westinghouse as part of the HSI design process. A methodology to perform this analysis was included in WCAP-14401 (Revision 3), "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan." While this is good practice and acceptably meets the criterion, the staff recommends that such analyses also be conducted at various points in the design process, as are the HFE guidelines evaluations.

The fourth part of the criterion is to document the results of these evaluations. As per the Westinghouse design process described in WCAP-14822, Revision 0, the results of design evaluations are documented as part of the design files. Thus, the part of the criterion addressing documentation of analyses was acceptably addressed.

The information from earlier SSAR revisions was acceptably included in SSAR Revision 19. Evaluation Issue 16; is discussed in SSAR (Revision 23), Section 18.11, "HSI Design Test Program;" and a more detailed description is included in WCAP-14401 (Revision 3), "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan." This SSAR section also included the above discussion of SSAR Section 18.8.2.3.5, "Evaluation Issues and Descriptions."

In conclusion, the Westinghouse design process provides for the acceptable evaluation of HSIs.

The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822, Revision 0, "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8." (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures). The staff has reviewed WCAP-14822 (Revision 0) and found that it acceptably incorporates the design review procedures noted above as leading to the resolution of this issue.

Based on this information, Open Item 18.8.1.3-7 is closed and the NUREG-0711 criterion is satisfied.

Criterion 9: HSI Design Documentation

*Criterion:* The HSI design should be documented to include the following features:

- the detailed HSI description, including the format and performance characteristics

- the basis for the HSI design characteristics with respect to operating experience and literature analyses, trade-off studies, engineering evaluations and experiments, and benchmark evaluations

*Evaluation:*

DSER Evaluation

The results of the design process for the main control area are described in Section 18.9 of the SSAR (Revision 0). General descriptions of major equipment (wall panel information station, operator and supervisor workstations, and safety panel) are provided in Section 18.9.1 of the SSAR (Revision 0). The alarm system and computer-based procedures are described in greater detail in Sections 18.9.2 and 18.9.8 of the SSAR (Revision 0), respectively. Design process results for other areas within the main control room and for control centers outside the control room are described in Sections 18.9 and 18.10 of the SSAR (Revision 0), respectively.

As indicated in this section's evaluation of Criterion 5, "General HSI Design Feature Selection," the SSAR (Revision 0) did not specifically describe the basis for the central elements of the control room design.

Westinghouse should describe how the final HSI design will be documented, incorporating the bases given in the criterion. This was Open Item 18.8.1.3-8.

FSER Evaluation

A full documentation of the AP600 HSI is not currently available because the design is not yet completed. SSAR (Revision 23) Section 18.8, "Human System Interface Design," and 18.12, "Inventory," documents the current status of the MCR resources, including HSI requirements, description, and technical basis.

The complete documentation process for the final design is described and controlled under WCAP-12601, "AP600 Program Operating Procedures" (Revision 15, dated April 1, 1995), which provides a description of the HSI documentation process. Procedure AP-3.1, "AP600 System Specification Documents (SSDs)," Revision 1, dated February 28, 1991, establishes requirements for SSDs. SSDs identify specific system design requirements and show how the design satisfies the requirements. They provide a vehicle for documenting the design and its basis. General Step C states that the SSDs provide for the control room HSI design. Step E and Appendix C provide a list of the AP600 systems for which SSDs are required, which includes the operation and control centers (OCS). Appendix A provides a top level Table of Contents by section for each SSD and Appendix B provides a summary description of what should go into sections of the SSD.

WCAP-12601, Procedure AP-3.2, "Design Configuration Change Control," Revision 3, March 11, 1994, provides the required process and actions to implement a design change in a document that is under configuration control. The scope of the procedure includes SSDs, drawings, and so forth It has considerable information on responsibilities, procedures, documentation, and approvals.

WCAP-12601, Procedure AP-3.6, "AP600 Design Criteria Documents," Revision 2, March 11, 1994, specifies requirements for the preparation, review, approval, and revision of design criteria documents, which define the requirements for specific aspects of the AP600 design, typically in a single discipline or subdiscipline.

In conclusion, the Westinghouse design process defined in WCAP-12601 and illustrated in the SSAR for the current state of the AP600 HSI design completion will provide an acceptable documentation of the detailed HSI design.

The staff requested that the relevant procedures be docketed in a Westinghouse report. In response to this request, Westinghouse submitted WCAP-14822, Revision 0, "AP600 Quality Assurance Procedures Supporting NRC Reviews of AP600 SSAR Sections 18.2 and 18.8." (See discussion of the WCAP in discussion of Open Item 18.2.3.3-1: HFE Process and Procedures). The staff reviewed the WCAP and found that it acceptably incorporates the DR procedures noted above as leading to the resolution of this issue.

Based on this information, Open Item 18.8.1.3-8 is closed and the NUREG-0711 criterion is satisfied.

Criterion 10: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's effort should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

According to Westinghouse's response to RAI 620.39, the "human factors guidelines and systems engineering procedures to implement the task analysis" will be prepared using the references in Section 18.8.3 of the SSAR (Revision 0). The documents cited include both general and nuclear power plant-specific human engineering guidelines, treatments of human performance and human error, and descriptions of cognitive engineering and operator performance modeling. Therefore, while specific concerns were raised previously in this review element concerning the adequacy of the available guidance for advanced control rooms, the overall design process is adequately supported by current information. The SSAR (Revision 0) acceptably addressed this NUREG-0711 criterion.

FSER Evaluation

SSAR (Revision 23), Section 18.8.1.2, "Design Guidelines," provides a commitment from Westinghouse that the HFE program will be developed using accepted industry standards, guidelines, and practices. Section 18.8.6, "References," provides numerous citations of applicable standards, guidelines, and practices used to develop the AP600 HSI design. Additional references are cited in supporting WCAP reports also referenced in SSAR (Revision 23).

Based on this information, the NUREG-0711 criterion is satisfied.

18.8.1.4 Conclusions

The objective of this review is to evaluate the process by which HSI design requirements will be developed and HSI designs will be selected and refined. The staff reviewed HSI development at an implementation plan level of detail. The review addressed the process by which function and task requirements will be translated to the displays and controls that will be available to the crew. Westinghouse should have a process for systematically applying HFE principles and criteria (along with all other function, system, and task design requirements) to the identification of HSI requirements, the selection and design of HSIs, and the resolution of HFE/HSI design problems and issues. The process and rationale for the HSI design (including the results of trade-off studies, other types of analyses and evaluations, and the rationale for selection of design and evaluation tools) should be documented for review.

The HSI design process presented in the SSAR has many positive features, including a systematic identification of information and control requirements, and the systematic testing of concepts and designs. This process includes developing functional requirements and functional specifications for key components of the HSI design. This is followed by the development of physical implementation documents that guide the detailed design of software and hardware.

The review of the AP600 HSI focuses strongly on the process by which the final design will be developed. Details of the guidance documents and the process by which they will be completed are important considerations in this review because the full details of the actual HSI design were not available before design certification.

Westinghouse has provided an acceptable Human-System Interface Design implementation plan for the AP600 design.

18.8.2 Safety Parameter Display System

18.8.2.1 Objectives

The objective of this review is to evaluate the way in which SPDS functions will be provided in the AP600 control room. The review will ensure that the applicant has appropriately translated SPDS functional requirements to the displays that are available to the crew.

18.8.2.2 Methodology

18.8.2.2.1 Material Reviewed

The review focused on an evaluation of Westinghouse material pertinent to the SPDS. The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-14396 (Revision 2) dated January 27, 1997

18.8.2.2.2 Technical Basis

The staff focused its review on an evaluation of information provided by Westinghouse pertaining to the SPDS with respect to the criteria contained in 10 CFR 50.34 (f)(2)(iv), Supplement 1 of NUREG-0737, and NUREG-1342. This review considered the extent to which Westinghouse's design will support the functions required for the SPDS, because Westinghouse has not completed the detailed design of the control room displays.

18.8.2.2.3 DSER Item Resolution

To address Element 7 SPDS open items, Westinghouse submitted a response (June 7, 1995) to RAI 620.48. The open item contains several subcomponents. As a result of the review of the Westinghouse response several open items were resolved. The results of the review were sent to Westinghouse in a letter dated September 28, 1995.

Westinghouse addressed these concerns in SSAR (Revision 9) Section 18.8.2, "Safety Parameter Display System." Additional comments were provided to Westinghouse in a letter dated December 1996. Discussion on the comments and the SSAR were held on January 7, 1997, and January 14, 1997.

Final resolution to SPDS issues were accomplished through Revision 23 to the SSAR and by incorporating several SPDS issues in the design issues tracking system, as described below.

18.8.2.3 Results

Criterion 1: General SPDS Requirements

*Criterion:* The top-level requirements for SPDS are contained in 10 CFR 50.34 (f)(2)(iv). The detailed NRC criteria that follow were derived from Supplement 1 of NUREG-0737.

*Evaluation:*

DSER Evaluation

In Section 18.9.2.2.6 of the SSAR (Revision 0), Westinghouse stated that "the alarm system meets the requirements of the safety parameter display system (SPDS)." In its response to RAI 620.48, Westinghouse stated that, in the AP600 control room, alarms will be better organized, have cause-effect relationships more clearly presented, and be fewer in number than is typical in current control rooms. Westinghouse concluded that this presentation, in combination with the analog information regarding plant processes provided by other control board CRT displays, satisfies the intent of the SPDS requirement.

In Item (2)(iv) of Section 1.9.3 of the SSAR (Revision 0), Westinghouse stated that alarms are grouped "by plant process or purpose, as directly related to the critical safety functions," and that the requirement for analog display of plant parameters is met by similarly grouped information available on graphic CRT displays.

The staff acknowledges that the implementation of the SPDS in a new advanced plant will and should be different than that which was backfitted into existing nuclear power plants.

Implementation as proposed by Westinghouse may satisfy the SPDS requirements. However, the high-level concepts and criteria still should be addressed in such a new implementation. Given the current state of the MCR HSI design, it is not possible to determine whether the SPDS will meet the requirements. Therefore, implementation of the design of the SPDS is considered an open item.

Westinghouse should provide assurance that the SPDS design will meet all of the pertinent criteria as part of the HSI. This was Open Item 18.8.2.3-1. This is also discussed under Criteria 2 through 9, which follow.

FSER Evaluation

10 CFR 50.34 (f)(2)(iv) indicates that the design should provide a plant safety parameter display console that will (a) display to operators a minimum set of parameters defining the safety status of the plant, (b) capable of displaying a full range of important parameters and data trends on demand, and, (c) be capable of indicating when process limits are being approached or exceeded. A discussion of these requirements follows.

(a) A plant safety parameter display console will be provided that will display to operators a minimum set of parameters defining the safety status of the plant.

As described in SSAR (Revision 23) Section 18.8.2, "Safety Parameter Display System," Westinghouse addresses the SPDS concerns and criteria via an integrated design rather than a stand-alone, add-on system, as is used at most current operating plants. The regulatory requirements will be met by integrating the SPDS requirements into the design requirements for the alarm and display systems. In NUREG-0800, the staff indicated that, for applicants who are in the early stages of the control room design, the "function of a separate SPDS may be integrated into the overall control room design" (p. 18.0-1). Therefore, the Commission has determined that the special circumstances described in 10 CFR 50.12(a)(2)(ii) exist in that the requirement for an SPDS console need not be applied in this particular circumstance to achieve the underlying purpose because Westinghouse has provided an acceptable alternative that accomplishes the intent of the regulation. On this basis, the Commission concludes that an exemption from the requirements of 10 CFR 50.34(f)(2)(iv) is authorized by law, will not present an undue risk to public health and safety, and is consistent with the common defense and security. However, for the implementation of an integrated SPDS to be acceptable, it must meet the detailed SPDS requirements reflected in this item.

(b) The SPDS will be capable of displaying a full range of important parameters and data trends on demand.

The minimum set of parameters defining safety status is reviewed in Criterion 8. With respect to other "important parameters," Westinghouse's integrated HSI design provides parameter display to operators via the wall panel information display and the workstation displays. A complete specification of the individual parameters to be displayed will be developed as the MCR design and its supporting analyses, such as FBTA and HRA, continue. The status of the functions of reactivity control, reactor core cooling and heat removal, reactor coolant system integrity, radioactivity control and containment will be

provided. Most of the parameters used to monitor these functions are continuously displayed. Those that are not will be available in one navigation step. SSAR (Revision 23), Chapter 7, identifies parameters for postaccident monitoring (PAM) which includes those needed to monitor the critical safety functions (CSFs).

The ability of operators to call up data trends on demand is addressed in Section 18.9.5.

(c) *The SPDS will be capable of indicating when process limits are being approached or* exceeded.

This SPDS function will be satisfied by the AP600 alarm management system.

Another set of top-level requirements for the SPDS is contained in NUREG-0737-Supplement Number 1, 3.8.a, Items (1), (2), and (3). These are expressed in terms of one acceptable way of implementation, with other proposals to be reviewed as necessary.

Item (1) states that the licensee/applicant should review the functions of the nuclear power plant operating staff that are necessary to recognize and cope with rare events that pose significant contributions to risk, could cause operators to make cognitive errors in diagnosing them, and are not included in routine operator training programs.

Item (2) states that the licensee/applicant should combine the results of this review with accepted human factors principles to select parameters, data display, and functions to be incorporated into the SPDS.

Item (3) states they should then design, build, and install the SPDS in the control room and train its users.

Westinghouse's selection of rare events that present significant contributions to risk for use in control room (and hence SPDS) design was discussed in their June 30, 1995, response to DSER Open Items 18.5.3-1 and -2. Following considerable discussion between the staff and Westinghouse on the risk criteria for selecting those activities to design the control room (and hence the SPDS), an approach that was acceptable to the staff was developed concerning risk-significant actions. Thus, Item (1) of Criterion 1 related to SPDS was acceptably addressed.

Westinghouse committed to design, build, and install the SPDS in accordance with accepted human factors principles as discussed in SSAR (Revision 23) Section 18.8.2.5, "Human Factors Engineering." This commitment addressed Item 2.

Westinghouse discussed the training of users in SSAR (Revision 23) Section 18.8.2.7, "Procedures and Training." However, training has been defined as a COL item (see SSAR (Revision 23) Section 18.10, "Training Program Development"). Thus, the SPDS training issue will not be addressed as part of the design certification review.

Based on this information, Open Item 18.8.2.3-1 is closed and the SPDS criterion is satisfied.

Criterion 2: Rapid and Concise Display of Safety Parameters

*Criterion:* The SPDS should provide a rapid and concise display of critical plant variables to control room operators.

*Evaluation:*

DSER Evaluation

In Section 18.9.2.4.9 of the SSAR (Revision 0), Westinghouse described the processing time, update rate, and display access time requirements for the alarm system as a whole; however, the rapidity with which SPDS-related alarms and displays will be presented is not explicitly discussed. The maximum processing time permitted from data input to alarm display is given as 2 to 3 seconds. The refresh rate for the display of a process variable is no less frequently than once every 2 seconds. The time permitted for the system to create and show a requested display (or to acknowledge the request for a complex display) is 2 seconds.

Evaluation of the conciseness of the presentation of SPDS-related information depends on implementation details that are not available at this time. Westinghouse should describe how the SPDS will provide a rapid and concise display of critical plant variables to control room operators. This was part of Open Item 18.8.2.3-1 which is now closed.

FSER Evaluation

The basis for the requirement for a concise display stems from the lack of centralized display capability in the TMI-2 control room. TMI-2 control room personnel could not easily develop an overview of plant conditions, which contributed to the severity of the accident. In their response to RAI 620.48 (Revision 2) checklist items 3.1, 3.2, and 3.3, Westinghouse stated that their alarm management system is organized around the concept of plant process functions, which include the five safety functions defined by the NRC for the SPDS. The layout of these functions ensures that they are always visible. For the AP600, a similar design will be used for the wall panel information system. Westinghouse also committed to group the individual parameters that support the safety functions by those safety functions in both the AP600 alarm system and the plant information system displays. Westinghouse stated that the status of all five safety functions will always be displayed via the alarm system overviews that will be displayed to the operators through the wall panel information system. Thus, a concise display will be available which acceptably addresses this aspect of the SPDS criterion.

Regarding the criterion of a rapid display, judgement of a rapid display is dependent on sample rate, update rate, system response times, and a display format that is easy to understand and rapidly comprehended.

In SSAR (Revision 9) Section 18.8.2.2, "Display of Safety Parameters," Westinghouse stated that the design goal for the graphical display response time is two seconds; the design goal for AP600 HSI is to update the displays every one to two sec; and, the process data sampling is one sec or less. Westinghouse also committed to develop appropriate human-factored display formats. These commitments met the criterion with the exception of response time, as explained below.

The acceptability of a display response time of two seconds (and as stated in SSAR Section 18.8.2.2, as long as 10 seconds) for operator support during transient operations may be problematic for operators. The staff recognizes that this value is within the response time originally developed for SPDS. However, such SPDS consoles were supplemental to the available indications and controls. It is also recognized that a two second response time is within the time range recommended by most current HFE guidelines. However, this value is based on general literature and, therefore, may not be fully adequate for emergency operations in a process control environment such as a nuclear power plant. Delays have the potential to create frustration in operators who are used to having information instantly available through continuously displayed analog instruments. The staff, therefore, recommended that Westinghouse commit to verify the acceptability of the two second criterion and if found unacceptable, to determine the appropriate display response time.

In SSAR (Revision 9), Section 18.8.2.2, "Display of Safety Parameters," Westinghouse indicated that the acceptability of the display response time of two seconds would be evaluated during man-in-the-loop concept testing. If found unacceptable, a revised time would be determined. Further, Westinghouse included this design issue in the HFE issues tracking system. This approach is acceptable to the staff. However, WCAP-14396 (Revision 2), "Man-in-the-Loop Test Plan," did not include this issue as one to be tested. The staff requested Westinghouse to clarify where this issue will be addressed.

Westinghouse addressed this issue in SSAR Section 18.8.2.2 (Revision 23), which was revised to indicate that most of the safety parameters used to monitor SPDS functions will be continuously displayed on the wall panel information system. Those that are not continuously displayed will be accessible from the operator's workstation with one navigation action. In addition, Westinghouse agreed to include the issue of response time as a Design Issues Tracking System item (item 3465) and examine it in their man-in-the-loop test program (WCAP-14396). The tracking system item references the NRC letter dated September 28, 1995, in which the staff's concerns are documented. The item indicates that "The acceptability of a display response time of 2 seconds for operator support during transient operations is determined during Man-in-the-Loop testing. If 2 seconds is determined to be unacceptable, then a revised display response time is determined." This acceptably addresses the staff's concerns.

Based on this information, the SPDS criterion is satisfied.

Criterion 3: Convenient Display of Safety Parameters

*Criterion:* The location of the SPDS should be convenient to the control room operators.

*Evaluation:*

DSER Evaluation

In Item (2)(iv) of Section 1.9.3 of the SSAR (Revision 0), Westinghouse stated that "displays are available at the operator workstations, the supervisor workstation, the remote shutdown workstation, and the technical support center." Westinghouse should describe how the SPDS implementation will be convenient to control room personnel. This was also part of Open Item 18.8.2.3-1 which is closed.

FSER Evaluation

To meet this criterion, the SPDS should be convenient to all operators/users of the SPDS. In SSAR (Revision 23) Section 18.8.2, "Safety Parameter Display System," Westinghouse indicated that the SPDS would utilize the main control alarm system and display system in order to fully integrate the SPDS into the AP600 HSI. All process displays and controls (including the SPDS) will be available at each of the redundant operator workstations. The control room supervisor has another console that contains all of the same displays. The STA also has a console with all displays. Finally, the wall panel information system is a parallel display device that also contains the SPDS information, and is available and viewable by all in the control room.

Thus, the status of critical safety functions is conveniently located where it can be monitored from anywhere in the control room and is continuously displayed by the overview alarms presented on the wall panel information system and, in addition, in the computerized emergency operating procedures system when in use.

Based on this information, the SPDS criterion is satisfied.

Criterion 4: Continuous Display of Safety Parameters

*Criterion:* The SPDS should continuously display plant safety status information.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.50, Westinghouse stated that "the AP600 control room design concept is that few or no displays will be fixed or continuously displayed." The response notes that the advantages of spatial dedication are employed in the alarm overview displays and the wall panel information system, but that the displays have operator-selectable elements and are dynamic (i.e., change with plant state). Westinghouse should describe how the SPDS function will continuously display plant safety information. This was also part of Open Item 18.8.2.3-1, which is closed.

FSER Evaluation

In SSAR (Revision 23) Section 18.8.2, Westinghouse indicated that the status of all five safety functions is always displayed via the alarm management system. The alarm system is organized on the dark board concept for all plant modes. Thus, when no alarms are displayed, it indicates that the status of all safety functions is acceptable. The alarm system also will have failure indicators to ensure the operability of the alarm system itself. Further, the AP600 computerized procedures for EOPs will provide a continuous display of the overall state of each of the safety functions as part of the EOP requirement to monitor the status of the Critical Safety Function Status Trees. The computerized procedures system proposed by Westinghouse was not reviewed for design certification.

Thus, the status of critical safety functions is conveniently located where it can be monitored from anywhere in the control room and is continuously displayed by the overview alarms presented on the wall panel information system.

Based on this information, the SPDS criterion is satisfied.

Criterion 5: High reliability

*Criterion:* The SPDS should have a high degree of reliability.

*Evaluation:*

DSER Evaluation

A response to this criterion was not received by the staff in time to be evaluated for inclusion in this report. Westinghouse should describe how the SPDS will achieve a high degree of reliability. This was also part of Open Item 18.8.2.3-1, which is now closed.

FSER Evaluation

The SPDS is to be incorporated into the AP600 control room; however, the control room is not yet designed. In SSAR (Revision 23) Section 18.8.2, Westinghouse indicated that availability and reliability criteria will be included in the design process as is standard for Westinghouse I&C systems. The Westinghouse response to this criterion (i.e., a commitment by Westinghouse to provide a description of how a high degree of reliability will be achieved for all I&C systems including the SPDS) has been determined acceptable by the staff.

Based on this information, the SPDS criterion is satisfied.

Criterion 6: Isolation

*Criterion:* The SPDS should be suitably isolated from electrical or electronic interference with safety systems.

*Evaluation:*

DSER Evaluation

A response to this criterion was not received by the staff in time to be evaluated for inclusion in this report. Westinghouse should describe how the SPDS will be suitably isolated from electrical or electronic interference with safety systems. This was also part of Open Item 18.8.2.3-1 which is closed.

FSER Evaluation

In SSAR (Revision 23) Section 18.8.2.4, "Isolation," Westinghouse stated that a discussion of the electrical isolation for the control room is in SSAR (Revision 23), Chapter 7. The staff review

the Westinghouse response to this criterion (i.e., that data links are fiber-optic isolated, transmit only, to the monitor bus) and determined that it acceptably addresses suitable isolation of the SPDS.

Based on this information, the SPDS criterion is satisfied.

Criterion 7: Human Factors Engineering

*Criterion:* The SPDS should be designed incorporating accepted human factors principles.

*Evaluation:*

DSER Evaluation

While the human factors engineering of the alarm system and graphic displays that serve the SPDS function, as described in Sections 18.8 and 18.9 of the SSAR (Revision 0), is addressed as part of the overall control room human factors engineering design process review, specific commitment to SPDS HFE, per NRC requirements, should be provided. Westinghouse should describe how human factors principles will be incorporated into the SPDS. This was also part of Open Item 18.8.2.3-1, which is now closed.

FSER Evaluation

In SSAR (Revision 23) Section 18.8.2.5, "Human Factors Engineering," Westinghouse stated that the SPDS will be incorporated in the control room alarm and display systems. In accordance with the NUREG-0711 element on HSI design (evaluated herein), the staff considered the HSI design acceptable at the program plan level. The detailed implementation of SPDS displays, controls, and interface management (e.g., navigation) characteristics will not be complete until after design certification.

Based on this information, the SPDS criterion is satisfied.

Criterion 8: Minimum Information

*Criterion:* The SPDS should display sufficient information to determine plant safety status with respect to safety functions as described in Table 2 of NUREG-1342.

The safety functions and parameters of Table 2 were developed for conventional PWRs. They are still generally applicable for the AP600, but will need to be revised slightly to address the passive plant differences.

*Evaluation:*

DSER Evaluation

This criterion was not sufficiently addressed in the SSAR (Revision 0). Therefore, this criterion will remain open. Westinghouse should describe how the SPDS will display sufficient information

to determine plant safety status with respect to safety functions. This was also part of Open Item 18.8.2.3-1, which is now closed.

FSER Evaluation

In discussing the minimum parameters for display, NUREG-1342 states that the minimum information to be provided shall be sufficient to provide information about the following five safety functions:

(1) reactivity control
(2) reactor core cooling and heat removal from the primary system
(3) RCS integrity
(4) radioactivity control
(5) containment conditions

The specific parameters to be displayed are to be determined by licensees and applicants. Sample acceptable parameters for BWRs and PWRs are contained in Tables 2 and 3 of NUREG-1342.

In response to RAI 620.48 (Revision 2) checklist item 2.1, Westinghouse indicated that the presentation of process data through the abnormality (alarm) messages on the wall panel information system and through the video display unit (VDU) graphical displays is organized around these five safety functions. However, Westinghouse took exception to the reactor core cooling and heat removal function. Specifically, Westinghouse indicated that the function would be defined at the level of individual parameters such as RCS temperature, RCS water mass inventory, RCS pressure, RCS circulation, steam generator water level, RHR flow, and RHR heat exchanger delta-temperature. Westinghouse stated that integrating these parameters into a single function would increase operator workload because if a problem occurred, the operator must mentally determine which of the sensed variables (parameters) must be addressed. Further, Westinghouse indicated that the AP600 HSI will support the operator activity of situation assessment at the same level of abstraction as the control devices that operators must use to take corrective actions.

In the staff's opinion, decomposing the reactor core cooling and heat removal function into several parameters would potentially detract from the operator's ability to monitor that CSF (i.e., rapid determination that the status of each CSF is acceptable.) Westinghouse's proposed approach appeared to create additional workload associated with the operator having to check each individual parameter status to determine that the function is satisfactory. This was one of the problems that led to the staff's requirement for an SPDS. Presenting both levels of display (function and individual parameter) however, is an approach consistent with a levels-of-abstraction view. When a problem occurs, operators will not have to "mentally determine which of the sensed variables must be addressed" with the more detailed information being presented (e.g., automatically), and will also be able to monitor the status of the CSF. The Westinghouse approach seemed to imply that information should only be presented at one level of abstraction, (i.e., the level at which the operator controls the process.) However, the design philosophy generally seems to be that various levels of abstraction are desirable because, depending on the task, different levels are necessary. The task of monitoring CSFs is supported by a display at a higher level. As an example for the function in question (reactor core cooling and heat removal from the primary system), potential function level displays could address

subcooling margin, heat transfer rate from the reactor, and heat transfer rate from the primary to the secondary.

In Westinghouse's response to RAI 620.48 (Revision 2) checklist item 2.2, they indicated that the variables depicting each of the five safety functions are in SSAR (Revision 8) Section 7.5.3.2, Table 7.5-5 (Type B Variables and parameters). Individual parameters for the safety functions identified as acceptable by the staff for PWRs are listed in Table 2 of NUREG-1342 and were used as the starting point for the staff's review.

(1) For reactivity control, the SPDS should display power range, intermediate range and source range reactor power. SSAR (Revision 8) Table 7.5-5 indicated that for AP600 this function will include neutron flux, control rod position, and boric acid concentration. Various ranges of neutron flux are not described.

(2) For reactor core cooling and heat removal, the SPDS should monitor RCS level, subcooling margin, temperatures (Th, Tc, core exit), steam generator (SG) pressure, and RHR flow. SSAR (Revision 8) Table 7.5-5 contained all of these except RCS level, subcooling margin, and SG pressure.

(3) For RCS integrity, the SPDS should monitor RCS pressure, Tc, containment sump level, and for the SG - pressure, level, and blowdown radiation. SSAR (Revision 8) Table 7.5-5 indicates that this function will include RCS pressure, WR Th, WR Tc. Sump levels (except perhaps as containment water level) and SG parameters were not addressed.

(4) For radioactivity control, the SPDS should monitor effluent stack monitors, steamline radiation, and containment radiation. Of these, only containment area high range radiation were included in SSAR Table 7.5-5 (Revision 8).

(5) For containment conditions, the SPDS should monitor containment pressure, containment isolation status, and hydrogen concentration. SSAR Table 7.5-5 (Revision 8) indicates that this function will include containment pressure, containment area high range radiation, containment water level, and hydrogen concentration. Containment isolation status did not appear to be addressed.

In a letter dated September 28, 1995, from NRC to Westinghouse, the staff requested further explanation as to why Westinghouse's proposed approach to monitoring the core cooling and heat removal function would not result in an increased operator workload and an explanation as to why the parameters noted above were not identified. Westinghouse addressed this information in SSAR (Revision 23) Section 18.8.2.6, "Minimum Information." In SSAR (Revision 23) Section 18.8.2.2, the five critical safety functions are listed but no reference is made to the parameters used. In Section 18.8.2.6, individual parameters are addressed only through a reference to Table 2 of NUREG-1342 which, as noted above, provides acceptable parameters for monitoring safety functions. However, these are noted as a starting point and not the actual parameters. The staff considers Westinghouse's description presented in Revision 23 of the SSAR to reflect a movement away from the approach to SPDS which gave rise to the concerns identified. The current approach places SPDS design clearly within the HFE plan, defers detailed design to be a post-certification activity, and includes minimum information for

safety monitoring as an HFE issue tracking system item. The staff agrees in principle with this decision because Element 7 is being reviewed at an implementation plan level only.

The SSAR (Revision 23) indicates that, using the NUREG information as a start, the AP600 HSI design process will define the integration of safety function monitoring into AP600 displays. Westinghouse identified the issue of what constitutes the minimum information as an HFE issue to be tracked in the tracking system. While this may be a reasonable approach, the SSAR does not provide sufficient information to resolve the open item. Specifically, the staff's detailed concerns regarding the provision of the overall status for all safety functions at the functional level and the identification of specific parameters were not addressed. Because no description of the issue tracking system was provided, it is unclear whether Westinghouse intended to address the staff's concerns. Westinghouse should address these issues and commit in the SSAR to provide, as part of the HSI design process, a justification for each parameter from Table 2 of NUREG-1342 that is not included as part of safety status monitoring.

Westinghouse addressed the staff's comment by including the issue of minimum information as a Design Issues Tracking System item (item 3466). The tracking system item references the NRC letter dated September 28, 1995, "Status of AP600 Draft Safety Evaluation Report Open Items Related to Requirements for the SPDS" in which the staff's concerns are documented. The item indicates that "The safety functions and respective parameters presented in Table 2 of NUREG-1342 are used as a starting point or specifying the AP600 functions and perspective parameters. The list needs to be evaluated and revised to address the AP600 passive plant design." This acceptably addresses the staff's concerns.

Based on this information, the SPDS criterion is satisfied.

Criterion 9: Procedures and Training

*Criterion:* Procedures and operator training, addressing actions with and without the SPDS, should be implemented.

*Evaluation:*

DSER Evaluation

Procedures addressing actions related to SPDS are not discussed in the SSAR (Revision 0) because the SPDS is not treated as a separate entity. Because of the integrated nature of the proposed SPDS implementation for the AP600 design, this approach could be acceptable, but more supporting information is required. Westinghouse should describe how procedures and operator training, addressing actions both with and without the SPDS, will be implemented. This was also part of Open Item 18.8.2.3-1, which is now closed.

FSER Evaluation

SSAR (Revision 23) addresses procedures and training in Section 18.8.2.7, "Procedures and Training." This section indicates that procedures and training are the responsibility of the COL applicant. Thus, review of this SPDS criterion is a post-design certification activity.

Based on this information, the SPDS criterion is satisfied.

18.8.2.4 Conclusions

The objective of this review is to evaluate the way in which the functions of the SPDS will be provided in the AP600 control room. The staff has completed its review of Element 7 of NUREG-0711, "Human Systems Interface Design," and Westinghouse has acceptably addressed all open items. The COL applicant referencing the AP600 certified design is responsible for the execution and documentation of the human system interface design implementation plan. This is COL Action Item 18.8-1.

18.9 Element 8: Procedure Development

18.9.1 Objectives

The objective of this review is to ensure that the applicant's procedure development program will result in procedures that support and guide human interaction with plant systems and control plant-related events and activities. Human engineering principles and criteria should be applied along with all other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated.

18.9.2 Methodology

18.9.2.1 Material Reviewed

The review focused on an evaluation of the Westinghouse documents with respect to the topics and general criteria of the NUREG-0711. The following Westinghouse documents were used in this review:

- SSAR (through Revision 23)
- WCAP-14690 (Revision 1) dated June 27, 1997
- WCAP-14477 (Revision 1) dated November 7, 1997
- WCAP-14075 dated May 20, 1994

The staff reviewed another pertinent document, the "Westinghouse AP600 Emergency Response Guidelines (ERGs)," and evaluated under Criteria 2 and 5.

18.9.2.2 Technical Basis

The staff focused its DSER review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 8, "Procedure Development," of NUREG-0711.

18.9.2.3 DSER Item Resolution

Following the DSER, "procedure development" was identified as a COL action item in SSAR (Revision 23) Section 18.9, Procedure Development. Thus, resolution of specific staff concerns raised in the DSER was not sought. Instead the focus of the review was changed to determining the acceptability of the COL action item description and evaluation of the AP600 ERGs.

18.9.3 Results

Criterion 1: Technical Guidance

*Criterion:* This element covers the following procedures

- generic technical guidelines (GTGs) or ERGs
- plant and system operations (including startup, power, and shutdown operations)
- abnormal and emergency operations
- preoperational, startup, and surveillance tests
- alarm response

*Evaluation:*

DSER Evaluation

The plant-specific technical guidance on which the EOPs are based will be developed from the Westinghouse Owners Group (WOG) generic ERGs. These generic ERGs will be "modified and adapted to the specific plant configuration of the AP600" by a process described in Section 18.9.8.1.1 of the SSAR (Revision 0).

Section 18.9.8 of the SSAR (Revision 0) states that the following types of procedures will be developed for the AP600:

- normal operating procedures
- abnormal operating procedures
- emergency procedures
- alarm response procedures
- maintenance procedures

Normal operating procedures describe the actions to be taken to "start up the plant, operate the plant at power, shut down the plant, operate individual plant systems, perform surveillance testing and remove equipment from service for maintenance activities." Sections 13.5.1 and 13.5.2 of the SSAR (Revision 0), addressing administrative, operating, and maintenance procedures, state that these procedures are "Combined License applicant specific" and "outside the AP600 design certification scope." Westinghouse should clarify the scope of the procedure development program. This was Open Item 18.9.3-1.

FSER Evaluation

Following the DSER, procedures were identified as a COL action item. Thus, resolution of specific staff concerns raised in the DSER was not sought and all of the open items are considered closed.

SSAR (Revision 23) Section 18.9.1, "Combined License Information," refers to SSAR (Revision 23) Section 13.5, "Plant Procedures," for a description of the item. The item states that procedure development is the responsibility of the COL applicant. Westinghouse will provide the applicant with WCAP-14690 (Revision 1), "Designer's Input to Procedure Development for the AP600." It should be noted that, although Westinghouse submitted this

document in support of the COL's procedure development program, the staff has not evaluated the computerized procedure system identified by Westinghouse as the interface to plant procedures. The NRC neither endorses nor rejects using the computer as a platform for presenting procedures. In the NRC's review of the EPRI URD guidance on computer-based procedures (CBPs), questions were raised concerning the basis for the computerized procedure requirement (NRC, 1991; see RAI 620.13, p. 6-7). EPRI (1991) indicated that CBP guidance is lacking and that it will have to be developed by the designer using simulation. The response noted that "Since both the 'soft' and 'hard' procedures are subject to the test of active simulation, there will inherently be a direct comparison between the 'soft' and the 'hard' procedures as part of the design process. Differences in operator performance with the computer-presented procedures compared to the conventional printed procedures should be evident from these evaluations" (p. 31). Further, EPRI indicated that "If the soft procedures are not concluded to represent an improvement when active simulation is attempted, there is a clear fall-back to hardcopy procedures" (p. 30).

In consideration of the EPRI URD and the subsequent response to the RAI, the staff noted that:

> "...the development of electronically displayed procedures is a desirable goal for the overall integration of operator information needs. The staff position is that the M-MIS designer should consider the use of electronically displayed procedures early in the design process to resolve any issues concerning their development, operability, maintainability, and reliability. If electronically displayed procedures are determined to be an improvement over hard-copy procedures and the M-MIS designer has integrated electronically displayed procedures into the overall M-MIS design, they should be provided as part of the design." (NRC, 1994, p. 10.B-17)

The staff position reflected in the URD review is applicable to the AP600 use of computerized procedures. That is, the acceptance of them will be based, in part, on the type of evaluations described above.

Evaluation of the Westinghouse computerized procedure system was not included in design certification for the AP600. The WCAP provides information on the computer-based procedure system which will serve as the interface to the plant procedures.

While this description is acceptable, the staff has determined that it is necessary for the COL applicant to (1) address the procedure development considerations in NUREG-0711, (2) address relevant concerns identified in the DSER review, and (3) to identify the minimum documentation that the COL applicant will provide to the staff to complete its review. This is COL Action Item 18.9-1.

Based on this interpretation of the COL Information, the procedure-related DSER items are considered satisfied.

Criterion 2: Basis for Procedure Development

*Criterion:* The basis for procedure development should include the following:

- plant design bases
- system-based technical requirements and specifications
- task analyses results
- critical human actions identified in the HRA/PRA
- initiating events to be considered in the EOPs, including those events present in the design bases
- GTGs (ERGs)

*Evaluation:*

DSER Evaluation

According to Section 18.9.8.1 of the SSAR (Revision 0), the AP600 EOPs will be based on the WOG generic ERGs. The development of EOPs will use "the same accepted and established process used by utilities with Westinghouse pressurized water reactors." The process used to develop plant-specific EOPs is described in detail in Section 18.9.8.1 of the SSAR (Revision 0) (and summarized in Westinghouse's response to RAI 620.87). Development will begin with the ERGs for a low-pressure reference plant that has "major functional similarities" (Section 18.9.8.1.1 of the SSAR, Revision 0) to the AP600; details are provided in Westinghouse's response to RAI 620.89. A comparison was made between the low pressure (LP) reference plant and the AP600 design to determine the applicability of the LP ERGs for developing the AP600 high-level operator action strategies. These strategies are listed in Section 18.9.8.1.1.2 of the SSAR (Revision 0) (and in Tables 18.9.8-1 through 18.9.8-37 of the SSAR, Revision 0). Other than applying the LP ERGs, the means by which methods specified in the criterion will be used for procedure development are not described.

The evaluation of this criterion is related to Westinghouse's response to RAI 440.32 and the staff's August 25, 1994, letter, which requested the submittal of a complete version of the AP600 ERGs. Also, the staff requested that Westinghouse describe how (or whether) methods, in addition to low-pressure reference plant/ ERG comparison, will be used for procedure development. This was Open Item 18.9.3-2.

At the time of the DSER development, Westinghouse had not provided the staff with copies of the ERG for staff review. In the DSER, the staff states that Westinghouse should submit the AP600-specific ERGs so that the staff can verify that the EOPs will be symptom-based. This was Open Item 18.9.3-5.

FSER Evaluation

Westinghouse submitted Revision 2 of the AP600 ERGs and supporting background documents by letter dated January 10, 1997, and submitted Revision 3 of the AP600 ERGs and background documents by letter dated June 19, 1997 (AP600 Document Number GW-GJR-100). The staff reviewed these submittals and sent three letters, dated February 6, March 13, and April 9, 1997 to Westinghouse requesting additional information. Several telephone conferences were held to discuss these questions and Westinghouse's proposed resolution to the staff's comments. Westinghouse provided written responses to the staff's comments by letters dated

September 19, 1997, November 6, 1997, and January 29, 1998 and implemented changes through Revision 6 of the ERGs.

The staff reviewed the ERGs for the AP600 and the responses to the RAIs. The ERGs retain the structure and event mitigation strategies of Westinghouse operating PWRs. They provide symptom-based as opposed to event-based guidance to the operator, and include optimal recovery guidelines and function restoration guidelines. The optimal recovery guidelines include the procedural guidance for reactor trip response, loss of reactor or secondary coolant, passive systems termination, loss-of-coolant accident (LOCA) outside containment, steam generator tube rupture, and so forth. The function restoration guidelines address safety functions such as reactivity control, core cooling, heat sink, RCS integrity, containment and pressurizer inventory. The ERGs also use critical safety function (CSF) status trees.

The staff, with the help of Brookhaven National Laboratory (BNL), performed the review to determine whether there is sufficient information in the AP600 ERGs and the ERG background document so that the COL can use them to develop an effective set of EOPs, which will then provide guidance for the operators during emergency and accident situations. The following criteria were used by the staff for the review:

1. ERGs are in proper post-TMI symptom-oriented format.

2. ERGs appropriately cover transients and accidents analyzed in SSAR Chapter 15. Also, the EPGs address transients and accidents beyond design-basis with multiple failures and operator errors.

3. ERG actions are technically supported as documented in the ERG background document.

4. The minimum inventory of controls, displays, and alarms appropriately addresses the actions specified in the ERGs and the risk-important operator actions of the PRA.

5. The ERGs provide sufficiently clear guidance that allows operators to terminate passive systems.

6. The ERGs properly address adverse systems interactions (ASI) identified in the Westinghouse ASI report, WCAP-14477.

7. The ERGs also make use of non-safety equipment for mitigating transients and accidents.

The staff reviewed the AP600 Emergency Response Guidelines and Background Document (through Revision 5) and the AP600 Adverse System Interactions Evaluation Report (Revision 1), (WCAP-14477), against the above criteria.

BNL reviewed the ERGs and the ERG background documentation to identify steps in the guidelines that could result in adverse systems interactions. BNL cross-checked the adverse interaction resolutions of WCAP-14477 to ensure that the recommended resolutions are

appropriately addressed in the ERGs. In addition, the ERGs reflect the fact that the operators will make use of non-safety equipment for mitigating transients and accidents.

The ERGs are presented in a function or symptom-oriented format, which is designed to maintain the critical safety functions of AP600. They are divided into optimal recovery guidelines, CSF status trees, function restoration guidelines, shutdown safety status trees, and shutdown guidelines. There is a section in the Background Document for each of these items. They are written in a clear and concise fashion; they use an accepted two column format; the warnings, cautions, and notes are set off from the text; steps use proper action verbs; and the decision points and values are specifically noted.

The transients and accidents described in Chapter 15 are covered by various portions of the ERGs. Also, the ERGs address transients and accidents beyond the design-basis, with multiple failures and operator errors. The ERG Background Document provides the bases for the steps in the ERGs and also provides analyses and justifications that demonstrate that the ERGs adequately address these transients and accidents. In certain cases during the review, the staff identified areas of the ERGs (e.g., identification of continuously applicable steps) that would need to be further addressed by the COL, but this fact was not clearly specified. Westinghouse identified these general areas in the ERG Background Document, so that the COL applicant would be aware of this need.

The minimum inventory of controls, displays, and alarms defined by Westinghouse in the SSAR appropriately addresses the actions specified in the ERGs and the risk-important operator actions of the PRA.

The staff also reviewed the ERGs to determine whether Westinghouse has provided guidance concerning the termination of the passive safety systems by the operators. The ERGs were found to provide information and guidance of sufficient detail for termination of passive safety systems. The ERG background document provided additional detail and contained the basis for the ERG steps as well as information that will be useful to procedure writers developing the final EOPs.

For the AP600, Westinghouse developed shutdown ERGs used during Modes 5 (cold shutdown) and Mode 6 (refueling). The shutdown ERGs are also symptom based. The AP600 shutdown ERGs were developed using the same philosophy and methodology that was used for developing the at-power ERGs. Since there is no generic guidance for shutdown ERGs in operating plants, the shutdown guidelines for AP600 are first of a kind guidance and focus on monitoring and maintaining the same plant critical safety functions (CSFs) and barriers (fuel cladding, reactor coolant system, and containment building) which protect the public whether the plant is at power or is shutdown. The CSFs (subcriticality, core cooling, heat sink, RCS integrity, containment and inventory), which are used to monitor plant conditions for safety challenges during operating modes 1, 2, 3 and 4, were also used as the basis for developing a monitoring tool to detect challenges to the plant safety state for the remaining shutdown conditions (modes 5 and 6). The symptoms for the conventional CSF status trees and the underlying intent of the safety function was evaluated with respect to modes 5 and 6 shutdown conditions. The result was a single status tree for shutdown operations during modes 5 and 6 that represents all six of the CSFs.

The shutdown safety status tree SDF-0.1 addresses the entry conditions for entering the Shutdown Procedures. The following parameters are used as entry conditions:

- Pressurizer level
- RCS hot leg level
- operation of normal RNS
- containment radiation
- nuclear flux
- RCS temperature and pressure
- controlled heat up or cooldown in progress
- CMT actuation signal

The following Shutdown Guidelines were provided:

- SDG-1, Response to loss of RCS inventory during shutdown
- SDG-2, Response to loss of RNS during shutdown
- SDG-3, Response to high containment radiation during shutdown
- SDG-4, Response to increasing nuclear flux during shutdown
- SDG-5, Response to RCS cold overpressure during shutdown
- SDG-6, Response to unexpected RCS temperature changes during shutdown

The shutdown guidelines address the CSF as they relate to shutdown modes 5 and 6. Core cooling is addressed by monitoring both the RCS level (either pressurizer or hot leg) and operation of RNS. Heat sink during shutdown is addressed by monitoring operation of the RNS; containment is addressed by monitoring containment radiation; subcriticality is addressed by monitoring nuclear flux; RCS integrity is addressed by monitoring the RCS pressure and temperature; and inventory is addressed by monitoring RCS level.

Based on the accepted importance of CSFs in monitoring plant safety challenges in modes 1 through 4, the staff has reviewed the AP600 shutdown ERGs (including the shutdown safety status tree, response guidelines, and associated background documents) to ensure that the AP600 shutdown ERGs encompass the CSFs. A summary of this assessment and the staff's conclusions is provided below:

Subcriticality

Obtaining subcriticality is not a significant concern applicable to modes 5 and 6 since the reactor is already shutdown and only decay heat is being generated in the core. The critical safety function concern for modes 5 and 6 is maintaining subcriticality by preventing conditions leading to inadvertent criticality. Therefore, the importance of this CSF is somewhat less than for at-power conditions. The CSF is monitored by a flux doubling alarm to identify a loss of shutdown margin that precedes an inadvertent criticality. By alerting the operator of the need for prompt action to re-establish shutdown margin, inadvertent criticality and any associated addition of heat into the system should be easily avoidable. Based on the above considerations, the staff finds the AP600 ERG treatment of this CSF acceptable for shutdown conditions.

Core Cooling

The core cooling safety function is applicable in shutdown, but due to the initial low energy levels and RCS temperatures, elevated core exit temperatures would not be expected for a relatively long period of time following a loss of core cooling (when compared to at-power conditions). As long as water level is maintained above the reactor core, heat can be removed to prevent core heatup to damaging temperatures. The presence of adequate water level to maintain the core cooling can be determined by either pressurizer level or hot leg level (when the RCS boundary is opened and in a reduced inventory condition). Both levels are monitored in the shutdown status tree. To prevent heat up and possible high saturation pressures (which could inhibit operation of the passive injection systems), the core cooling safety function was prioritized first on the status tree. The staff agrees with the assessment that this is the highest priority CSF for shutdown conditions and finds its treatment in the Westinghouse shutdown ERGs acceptable.

Heat Sink

The primary heat sink during shutdown conditions is the RNS. If the RNS is lost, prompt mitigating actions must be taken by the operator to re-establish RNS cooling or provide alternate ways of removing core decay heat using passive safety features of the AP600 design. The heat sink status (i.e., RNS operability) is checked after the shutdown core cooling status check because operation of the RNS in the shutdown cooling mode cannot take place if adequate core cooling has not been established. Loss of heat sink is prioritized ahead of containment since the primary system heat up on the loss of RNS will be slow and time is available to the plant operator (via technical specification controls) for addressing containment closure. Corrective actions upon loss of RNS are adequately addressed in the shutdown ERG response guidelines. Based on the above discussion, the staff finds the shutdown ERG treatment of the heat sink CSF acceptable.

Integrity

The only challenge to primary system integrity during shutdown is system overpressurization. Because the primary system is already at a low temperature, significant rapid cooldown cannot occur. For the integrity CSF, the cold overpressure limits are checked, and if exceeded, will alert the operator to the proper shutdown guidelines. This treatment of the integrity CSF in the AP600 shutdown ERGs is acceptable to the staff.

Containment

The primary purpose of containment during shutdown is to maintain cooling water inventory inside containment following loss of RNS. The loss of residual heat removal results in steam being released to the containment. If the containment is closed and sufficient cooling is provided through the containment shell to condense the steam, the condensate will eventually drain back to the reactor coolant system, providing a long-term decay heat removal path. If this is unsuccessful then core damage is possible and the primary purpose of containment then becomes the retention of fission products. SDG-4 provides assurance that the containment will be closed given a high radiation signal inside containment. The containment will most likely be closed prior to a high radiation signal because SDG-1, 2, and 3 initiate actions to establish containment closure. Containment closure as discussed in these guidelines includes establishing the desired position of available containment isolation valves to minimize release

outside containment. In WCAP-14837, "Shutdown Evaluation Report," Westinghouse states that the pressure resistant barriers that make up containment, such as the isolation valves, will have a design pressure of 45 psig. Based on the above considerations, the staff finds the treatment of the containment CSF in the AP600 ERGs acceptable.

Inventory

The normal, at-power, primary system inventory can vary considerably during shutdown conditions depending upon the plant condition such as mid-loop operation. Because departure from the normal primary inventory is checked in the shutdown status tree to verify the CSF of adequate core cooling, no additional checks are made to specially address the inventory function. Because the inventory CSF is encompassed in the core cooling CSF, the staff finds the treatment in the AP600 shutdown ERGs acceptable.

In summary, for modes 1 to 4, the critical safety function sequence is as follows:

(1) subcriticality
(2) core cooling
(3) heat sink
(4) integrity
(5) containment
(6) inventory

The above sequence is not followed for the Shutdown conditions (modes 5 and 6). On the basis of the review the staff determined that Westinghouse is following the priority sequence given below during shutdown:

(1) core cooling/inventory
(2) heat sink
(3) containment
(4) subcriticality
(5) integrity
(6) loss of heat sink due to support system failures

The staff concluded that all the CSF are addressed for the different sequences used for the shutdown conditions, and that they are acceptable as described above.

Open item 18.9.3-2 is closed because Westinghouse submitted the required additional information.

As a result of this review, the staff determined that the combination of the ERGs and the ERG background document provide sufficient guidance for the COL applicant to develop EOPs for the operator's use during emergency and accident situations. Development of plant specific EOPs using the guidance provided in the AP600 ERGs is COL Action Item 18.9-2.

The staff concludes that the AP600 ERGs are adequate and acceptable. Therefore, Open Item 18.9.3-5 is closed. See also discussion under procedure development Criterion 1: Technical Guidance above.

Criterion 3: Writer's Guide Development

*Criterion:* A writer's guide should be developed to establish the process for developing technical procedures that are complete, accurate, consistent, and easy to understand and follow. The guide should contain objective criteria so that procedures developed in accordance with the guide will be consistent in organization, style, and content. The guide should be used for all procedures within the scope of this element. The writer's guide should provide instructions for procedure content and format, including the writing of action steps and the specification of acceptable acronyms and terms to be used.

*Evaluation:*

DSER Evaluation

Section 18.9.8.1.2 of the SSAR (Revision 0) states that "the AP600 writer's guide addresses the goals, requirements, and recommendations identified in the writer's guide section of NUREG-0899." A writer's guide that conforms to NUREG-0899 meets this criterion. However, the discussions of procedure content and format in NUREG-0899 do not explicitly address a computer-based presentation of procedures. The writer's guide must reflect both hardcopy and computer-based procedures.

The methods and/or sources used in identifying the unique capabilities and limitations of a computer-based presentation should be specified. The process for reflecting these unique aspects in the writer's guidance for such features as checkoffs, place-keeping, illustrations, verification steps, and support for recurrent or time-dependent steps should be described. Westinghouse should describe how the writer's guide will address the unique features of a paper- and computer-based presentation of procedures. This was Open Item 18.9.3-3.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-3 is closed.

Criterion 4: Content of Procedures

*Criterion:* The content of the procedures should incorporate the following elements:

- title
- statement of applicability
- references
- prerequisites
- precautions (including warnings, cautions, and notes)
- limitations and actions
- required human actions
- acceptance criteria
- checkoff lists

*Evaluation:*

DSER Evaluation

Section 18.9.8.1.2 of the SSAR (Revision 0) states that "the AP600 writer's guide addresses the goals, requirements, and recommendations identified in the writer's guide section of NUREG-0899." The basic organization for procedures provided in NUREG-0899 specifies content similar to those in the criterion. The functional requirements for the computer-based procedures stated in Section 18.9.8.6 of the SSAR (Revision 0) call for the display of many of the elements in the criterion. The contents of paper-based procedures is not explicitly discussed in the SSAR (Revision 0).

Differences in the manner of presentation of the items in this criterion (or in NUREG-0899) for paper-based, compared to computer-based, systems are not discussed. Westinghouse should describe and provide a rationale for the differences, if any, between the paper- and computer-based presentations of the items in this criterion (or in NUREG-0899). This was Open Item 18.9.3-4.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-4 is closed.

Criterion 5: Symptom-Based GTGs

*Criterion:* In addition to the general procedure elements identified in this section in Criterion 4, "Content of Procedures," GTGs should be symptom-based with clearly specified entry conditions.

*Evaluation:*

DSER Evaluation

Insofar as the WOG reference plant ERGs are function-oriented, the AP600 EPGs derived from the WOG ERGs can also be expected to be function-oriented and, therefore, symptom-based rather than event-based. Further, the AP600 EOPs, which are based on the ERGs, are described as symptom-based in Section 18.9.8.1 of the SSAR (Revision 0). A definitive determination will require review of the ERGs themselves. Westinghouse should submit the AP600-specific ERGs so that the staff can verify that the EOPs will be symptom-based. This was Open Item 18.9.3-5.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Also, see FSER Evaluation under Criterion 2, "Basis for Procedure Development." Open Item 18.9.3-5 is closed.

Criterion 6: Procedure V&V

*Criterion:* All procedures should be verified and validated. A review should be conducted to ensure that the procedures are correct and can be performed. Final validation of the procedures should be performed in a simulation of the integrated system as part of the V&V activities.

*Evaluation:*

DSER Evaluation

Section 18.9.8.1.2 of the SSAR (Revision 0) states that EOPs "are subjected to a verification and validation on the AP600 simulator." According to the SSAR (Revision 0), the V&V process addresses the objectives specified in NUREG-0899. It is not clear whether the simulator V&V referred to is a part of the proposed M-MIS evaluations, part of the validation of the integrated M-MIS, or a separate activity.

Section 18.8.2.3.5.5 of the SSAR (Revision 0) states that, during the validation of the integrated M-MIS, "subjects use the simulator to execute operating procedures for design-basis events." Computer- and/or paper-based procedures are among the relevant M-MIS resources associated with many of the evaluation issues that address the M-MIS V&V process. (See Evaluation Issues 7, 8, 9, 10, 11, 13, 14, and 15 described in Section 18.8.2.3.5 of the SSAR (Revision 0).) The coordination of procedures with workstation displays is a specific concern in Evaluation Issues 11 and 14. The design of procedure display interfaces, and the coordination of the procedure display with the physical and functional displays, are specific concerns in Evaluation Issue 13. The results of these evaluations are expected to have implications for the design of the computer-based procedures.

The SSAR (Revision 0) does not describe the circumstances and locations in which hardcopy procedures are expected to be used. Westinghouse should clarify the relationship of the EOP V&V to the M-MIS evaluation issues. The V&V process for hardcopy procedures should also be described. This was Open Item 18.9.3-6.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-6 is closed.

Criterion 7: Computer-Based Procedures

*Criterion:* An analysis should be conducted to determine the impact of providing computer-based procedures (either partial or complete), and to specify where such an approach would improve procedure use and reduce related operating crew errors.

*Evaluation:*

DSER Evaluation

The introductory material to the description of the computer-based plant procedures in Section 18.9.8.6.1 of the SSAR (Revision 0) states that the selection of rule-based responses is

amenable to computerization, and that this may be preferable to conventional presentations (for reasons of reduced likelihood of error, reduced operator workload, and the possibility of independent verification of operator actions). However, Westinghouse does not discuss the possibility that the particular implementation of the computer-based procedures planned for the AP600 might not mitigate those problems associated with hardcopy procedures (e.g., limited space for explanatory material, difficulties associated with the use of multiple procedures, poor integration of procedure use into the ongoing task), and that the computer-based implementation itself could introduce other problems (see Barnes et al., 1994). In addition, the SSAR (Revision 0) does not discuss analyses that address human engineering issues related to computer-based procedures, such as:

- Do computer-based procedures support performance at least as good as that obtained with conventional procedures?
- Can loss or degradation of the computer-based procedures system be adequately mitigated by backup measures?
- Can computer-based procedures foster undue dependence at the expense of situation awareness?

Westinghouse should describe the process by which human engineering issues associated with computer-based procedures will be resolved (e.g., concept testing and other analyses). This was Open Item 18.9.3-7.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-7 is closed.

Criterion 8: Procedure Maintenance

*Criterion:* A plan for procedure maintenance and control of updates should be developed.

*Evaluation:*

DSER Evaluation

The performance requirements for the computerized procedures system discussed in Section 18.9.8.6.4 of the SSAR (Revision 0) include "the capability to modify or edit the procedures in a straightforward manner. This is accomplished by using a relational data base management system." The system is also expected to provide "for the security of the procedural data base so that only authorized personnel make changes." However, it will be necessary to establish a means for applying administrative document control and quality assurance policies to both paper- and computer-based procedures. For example, there is no discussion of the need to ensure that hardcopy procedures (e.g., backups) remain current and consistent with the computer-based procedures. Westinghouse should describe the administrative procedures that will ensure that hardcopy procedures remain current and consistent with the computer-based procedures. This was Open Item 18.9.3-8.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-8 is closed.

Criterion 9: Procedure Use

*Criterion:* The physical means by which operators access and use procedures, especially during operational events, should be evaluated as part of the HFE design process. This criterion generally applies to both hardcopy and computer-based procedures, although the nature of the issues differs somewhat depending on the implementation. For example, the process should address the procedure storage location; easy operator access to the correct procedures; and hardcopy procedure laydown for use in the control room, remote shutdown facility, and local control stations.

*Evaluation:*

DSER Evaluation

Methods by which computerized procedures are accessed are discussed in Section 18.9.8.6.5.1 of the SSAR (Revision 0), which state that computerized procedures can be accessed either manually or automatically. Manual access is by opening "the computerized procedures icon, or equivalent." The particular procedure accessed may be either "a default procedure...selected by the system," or a procedure selected by the user from a menu. Automatic access is initiated "in response to events such as reactor trip, safety injection, or station blackout," and occurs "independently of whether the computerized procedures display is activated." The SSAR (Revision 0) does not discuss precautions taken to prevent automatically accessed procedures from disrupting ongoing operator use of the procedures.

The performance requirements for the computerized procedures system discussed in Section 18.9.8.6.4 of the SSAR (Revision 0) call for redundancy "so as to provide for a backup if one of the user stations fails." Degradation or failure of the computer-based procedures system is not addressed. Physical access to hardcopy procedures that would serve as backup to the computer-based procedures is not explicitly discussed in the SSAR (Revision 0). Westinghouse should describe provisions for access to, and use of, hardcopy procedures, as backups either in the control room or at locations outside the control room. Westinghouse should also describe how disruption of ongoing activity by automatically accessed procedures will be minimized. This was Open Item 18.9.3-9.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-9 is closed.

Criterion 10: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's procedure development effort should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

Section 18.9.8 of the SSAR (Revision 0) states that "the operating and maintenance procedures for the AP600 design implement the recommendations of Regulatory Guide 1.33." The SSAR (Revision 0) further states in Section 18.9.8.1.2 that the development of the AP600 EOPs follows a process that meets the guidelines in NUREG-0899, Supplement 1 to NUREG-0737, and NUREG-1358. Therefore, the procedure development process references most of the documents cited in this criterion. These documents, however, do not adequately support the development of computer-based procedures. Insofar as guidance for the design of computer-based procedures is not readily available and relevant research is very limited (Barnes et al., 1994), additional material will need to be developed. In addition, Figure 18.8.2-1 of the SSAR (Revision 0) lists guidance documents to be developed, but no procedure guideline document is identified. Westinghouse should describe the sources of experience drawn upon in developing guidance for the design of the computer-based procedures. This was Open Item 18.9.3-10.

FSER Evaluation

See discussion under procedure development Criterion 1: Technical Guidance, above. Open Item 18.9.3-10 is closed.

18.9.4 Conclusions

The objective of this review is to ensure that Westinghouse's procedure development program will result in procedures that support and guide human interaction with plant systems, and control plant-related events and activities. Human engineering principles and criteria should be applied along with all of the other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated.

Following the DSER, Westinghouse identified procedures as a combined license action item. Therefore, the staff did not require resolution of the concerns identified in the DSER for design certification. DSER procedure open issues will be addressed by the COL applicant as part of post-design certification issues.

18.10 Element 9: Training Program Development

18.10.1 Objectives

A systems approach to training, as defined in 10 CFR 55.4, is required of plant personnel by 10 CFR 52.78 and 50.120. Training design is to be based on the systematic analysis of job and task requirements. The HFE analyses associated with the HSI design process provide a valuable understanding of the task requirements of operations personnel. Therefore, training program development should be coordinated with the other elements of the HFE design process. The objective of this review is to ensure that the COL applicant establishes an

approach for the development of personnel training that incorporates the elements of a systems approach to training, as well as the following:

- evaluates the knowledge and skill requirements of personnel
- coordinates training program development with the other elements of the HFE design process
- implements the training in an effective manner that is consistent with human factors principles and practices

18.10.2 Methodology

18.10.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-14655 (Revision 1) dated August 8, 1996
- WCAP-14822 (Revision 0) dated February 25, 1997

18.10.2.2 Technical Basis

The staff focused its DSER review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 9, "Training Program Development," of NUREG-0711. The staff reviewed Westinghouse's training at an implementation plan level of detail, because Westinghouse will not complete work in this area until after design certification.

18.10.2.3 DSER Item Resolution

Following the DSER, training was identified as a COL action item in SSAR (Revision 23) Section 18.10, "Training Program Development." Thus, resolution of specific staff concerns raised in the DSER was not sought. Instead the focus of the review was changed to determining the acceptability of the COL action item description.

18.10.3 Results

Criterion 1: Training Mission

*Criterion:* The training program should be developed in accordance with 10 CFR 50.120, 10 CFR Part 55, and other relevant requirements to ensure that personnel have the qualifications commensurate with the performance requirements of their jobs. Training should address the full range of each of the following factors:

- positions of licensed and nonlicensed operational personnel whose actions may affect plant safety
- plant functions and systems, including those that may differ from those in predecessor plants (e.g., passive systems and functions)

- relevant HSI components (e.g., MCR, remote shutdown, panel, local control stations), including characteristics that may differ from those in predecessor plants (e.g., display space navigation and operation of "soft" controls)

- plant conditions

*Evaluation:*

DSER Evaluation

Section 18.9.9.2 of the SSAR (Revision 0) discussed the mission and scope of the AP600 training program. Specifically, this section lists the 10 plant positions for which training programs will be developed, and maintains that these positions are those that directly affect the safe operation of the plant. Section 18.9.9.3 of the SSAR (Revision 0) indicated that the bulk of the discussion related to developing the training program will focus on the control room operators and senior control room operators, with similar processes being used for the other positions.

Based on a review of this material, several issues needed clarification. It is not clear how the 10 indicated plant positions were identified as those that directly affect the safe operation of the plant. The 10 positions listed are currently used by INPO in their training program accreditation process. (See INPO 85-002, Revision 01). However, there is no discussion of the analysis conducted to ensure that these same 10 positions are the positions that directly affect the safe operation of the AP600 plant.

Additionally, Criterion 1 above calls for training to address the full range of plant functions and systems, relevant HSI components, and plant conditions. The material reviewed does not specifically address any of these areas as they relate to training. While the process described should result in a training program that addresses these areas, the relevant documentation does not specifically describe how this will occur. Westinghouse's discussion of the AP600 features that differ from currently operating nuclear power plants in the U.S. primarily relates to a different philosophy that will be implemented in the training of the AP600 operators (e.g., cognitive problem-solving abilities, Section 18.9.9.4 of the SSAR, Revision 0) and changes in the main control area computerized interface (Section 18.9.9.4 of the SSAR, Revision 0). There is little discussion relating to training for the remote shutdown panel and other local control stations, or to training in the area of passive systems and functions.

In summary, Westinghouse should provide further information regarding the areas that training will address. Specifically, the SSAR (Revision 0) defines only the positions for which training will be developed, and no rationale is given for why those positions were chosen. (Have they been determined to be the only positions that directly affect safe plant operations? If so, how was that determination made?) Additionally, the SSAR (Revision 0) does not discuss in detail other areas that should be addressed, as identified in this criterion. Westinghouse should provide additional information regarding the process that will address the rationale behind the selection of the identified positions for developing training programs, as well as information on the other related areas identified in this criterion. This was Open Item 18.10.3-1.

FSER Evaluation

Following the DSER, training was identified as a COL action item. Thus, resolution of specific staff concerns raised in the DSER was not sought and all of the open items are considered closed.

SSAR (Revision 23) Section 18.10.1, "Combined License Information" refers to SSAR (Revision 23) Section 13.2, "Training," for a description of the item. The item states that training program development is the responsibility of the COL applicant. Westinghouse will provide the applicant with WCAP-14655 (Revision 1), "Designer's Input to Training of the Human Factors Engineering Verification and Validation Personnel." The WCAP provides information on how insights are passed from the designer to the COL applicant.

While this description is acceptable, the staff has determined that it is necessary for the COL applicant to (1) address the training program development considerations in NUREG-0711, (2) address relevant concerns identified in the DSER review, and (3) to identify the minimum documentation that the COL applicant will provide to the staff to complete its review. This is COL Action Item 18.10-1.

Based on this interpretation of the COL action item, the training-related DSER items are considered satisfied.

Criterion 2: Training Requirements

*Criterion:* The discussion on training program development should address the applicable requirements of 10 CFR 50.120, 10 CFR Part 55, and other applicable regulations, as well as Section 13.2 of NUREG-0800.

Evaluation:

DSER Evaluation

The AP600 training program development documentation in the SSAR (Revision 0) did not discuss 10 CFR 50.120, 10 CFR Part 55, and other applicable regulations, as well as Section 13.2 of NUREG-0800. The material provided did not appear sufficiently detailed to allow the review to be conducted. Westinghouse should describe how the AP600 training program development will ensure consistency with the regulatory documents cited in this criterion. This was Open Item 18.10.3-2.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-2 is closed.

Criterion 3: Systems Approach

*Criterion:* A systems approach to training as defined in 10 CFR 55.4 should be used. The training development implementation plan should be consistent with the following five elements:

(1) systematic analysis of jobs to be performed

(2) learning objectives derived from the analysis that describe desired performance after training

(3) training design and implementation based on the learning objectives

(4) evaluation of trainee mastery of the objectives during training

(5) evaluation and revision of the training based on the performance of trained personnel in the job setting

*Evaluation:*

DSER Evaluation

The plant training program design process is graphically displayed in Figure 18.9.9-1 of the SSAR (Revision 0), and described in Sections 18.9.9.3 through 18.9.9.4 of the SSAR (Revision 0). The process described appeared to be a variant of the systematic approach to training (SAT) process currently used when developing training programs in the nuclear industry; however, the steps discussed in the SSAR (Revision 0) do not directly correspond to the five SAT steps. While the first four SAT steps appeared to be incorporated in the process described, the fifth step, involving the evaluation and revision of the training based on the performance of trained personnel in the job setting, is not discussed at all in the application. In addition, the fourth step, the evaluation of trainee mastery of the objectives during training is addressed under Section 18.9.9.4.2.3 of the SSAR (Revision 0) with the brief statement that "a periodic evaluation of trainees provides a means for identifying weaknesses and prescribing remediation."

Section 18.9.9.4.1 of the SSAR (Revision 0) discussed the use of cognitive task analysis to supplement the information obtained using a traditional SAT approach. A reference is given for cognitive task analysis, but it is not described in any detail in the application; therefore, it is not clear how the use of this approach will enhance the SAT process.

In summary, while the staff concluded that Westinghouse's general approach to SAT was acceptable, they requested that some of the details of the methodology should be provided. Westinghouse should provide additional information on the SAT approach that it is using, particularly with regard to the evaluation elements of the SAT process. Additionally, Westinghouse should provide information on how cognitive task analysis will supplement the information obtained using a traditional SAT approach. This was Open Item 18.10.3-3.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-3 is closed.

Criterion 4: Training Organizational Roles

*Criterion:* The roles of all organizations, especially those of the COL applicant and vendors, should be specifically defined for developing training requirements, information sources, and materials, as well as for implementing the training program. For example, the role of the vendor may range from merely providing input materials (e.g., emergency procedure guidelines) to conducting portions of specific training programs.

*Evaluation:*

DSER Evaluation

Section 13.2 of the SSAR (Revision 0) states that training is COL applicant-specific and is outside the AP600 design certification scope. No other reference is provided in the application to enable the staff to determine what the role of all organizations will be in developing training requirements, information sources, and materials, or in implementing training programs.

In summary, the material contained in the SSAR (Revision 0) did not provide the level of detail needed to enable the staff to determine what the role of all organizations will be in developing and implementing the training programs. Westinghouse should specifically define the roles of all organizations in developing and implementing the AP600 training programs. This was Open Item 18.10.3-4.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-4 is closed.

Criterion 5: Qualifications

*Criterion:* The qualifications of organizations and personnel involved in the development and conduct of training should be defined.

*Evaluation:*

DSER Evaluation

Section 18.9.9.4 of the SSAR (Revision 0) described the process by which expertise on the subject matter concerning the MCR operator will be developed. Specifically, currently licensed PWR training instructors will be used as MCR operators during the conduct of validation tests on the EOPs and the human engineering of the MCR. This experience, in combination with formal instruction by design engineers on the plant systems, cognitive problem-solving methods, and the man-machine interface systems, will prepare the instructors to become designers of the MCR operator training program.

Section 18.9.9.4.2.4 of the SSAR (Revision 0) discussed the formation of teams, (comprised of instructors familiar with the training program technical content as well as instructional technologists) to review material developed before the development of lesson designs. Other review points include similar types of individuals as well as utility owner's group representatives. (See Section 18.9.9.4.4 of the SSAR (Revision 0).)

No discussion was provided to define the qualifications of organizations and personnel involved in the conduct of training. Westinghouse should provide additional information on the qualifications of organizations and personnel to be involved in the development and conduct of training. This was Open Item 18.10.3-5.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-5 is closed.

Criterion 6: Training Scope

*Criterion:* The overall scope of training should be defined, including the following:

- categories of personnel (e.g., senior reactor operator) to be trained
- specific plant conditions (normal, upset, and emergency)
- specific operational activities (e.g., operations, maintenance, testing and surveillance)
- HSI components (e.g., MCR, emergency operations facility, remote shutdown panel, local control stations)

The scope of training should include the training of personnel participating in verification and validation of the plant design. (See Element 10, "Human Factors Verification & Validation" in Section 18.11 of this report.)

*Evaluation:*

DSER Evaluation

See the discussion in the DSER Evaluation section of Criterion 5, "Qualifications." In addition, Criterion 6, "Scope," above also requires that the SSAR (Revision 0) discuss the scope of training proposed to the personnel participating in the verification and validation of the plant design. Section 18.9.9.4 of the SSAR (Revision 0) states that currently licensed PWR training instructors will receive formal instruction by design engineers on the plant systems, cognitive problem-solving methods, and the man-machine interface systems before they participate in validation tests on the EOPs and on the human engineering of the MCR. How this training will be structured and developed is not described.

Westinghouse should provide additional information on how the AP600 training program will address the scope of training. This information should include categories of personnel (e.g.,

senior reactor operator) to be trained, as well as specific plant conditions (normal, upset, and emergency), operational activities (e.g., operations, maintenance, testing, and surveillance), and HSI components (e.g., MCR, emergency operations facility, remote shutdown panel, local control stations). This was Open Item 18.10.3-6.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-6 is closed.

Criterion 7: Learning Objectives — NUREG-0711

*Criterion:* Learning objectives should be derived from the analysis that describes desired performance after training. This analysis should include, but not be limited to, training issues identified in the following NUREG-0711 elements:

- operating experience review — previous training deficiencies and operational problems that may be corrected through additional and enhanced training, as well as positive characteristics of previous training programs
- function analysis and allocation — functions identified as new or modified
- task analysis — tasks identified during task analysis as posing unusual demands (including critical tasks identified by PRA/HRA; new or different tasks; and tasks requiring a high degree of coordination, high workload, or special skills)
- human reliability assessment — requirements for coordinating individual roles to reduce the likelihood and/or consequences of human error associated with critical human actions and the use of advanced technology
- HSI design — design features of which the purpose or operation may be different from the past experience or expectations of personnel
- plant procedures — tasks identified during procedure development as being problematic (e.g., those in which procedure steps that have undergone extensive revision as a result of plant safety concerns)
- verification and validation — training concerns identified during V&V (including HSI usability concerns identified during validation or suitability verification) and operator performance concerns (e.g., misdiagnosis of plant event) identified during validation trials

*Evaluation:*

DSER Evaluation

This criterion lists seven elements from which training issues should be identified. These issues should then be used to derive learning objectives. The development of learning objectives (termed instructional objectives in the SSAR, Revision 0) was generally discussed by Westinghouse in paragraphs 12 and 13 of Section 18.9.9.4.1 of the SSAR (Revision 0). These

two paragraphs define what learning objectives are, as well as the hierarchical manner in which they are developed. These two paragraphs do not, however, address any of the seven elements associated with this criterion. Westinghouse should describe how training issues will be identified from the seven elements listed above for use in deriving learning objectives. This was Open Item 18.10.3-7.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-7 is closed.

Criterion 8: Learning Objectives — Other Sources

*Criterion:* Learning objectives should also be derived from knowledge and skill requirements derived from the final safety analysis report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training.

*Evaluation:*

DSER Evaluation

As discussed in the DSER Evaluation section under Criterion 7, "Learning Objectives — NUREG-0711," the development of learning objectives is discussed in paragraphs 12 and 13 of Section 18.9.9.4.1 of the SSAR (Revision 0). These paragraphs define what learning objectives are, as well as the hierarchical manner in which they are developed. These paragraphs did not, however, address the use of any of the documents described in this criterion for the derivation of learning objectives. Additional information is needed for the staff to determine whether the training programs developed for the AP600 will fully meet this criterion. Westinghouse should describe how the training development process will allow a determination to be made of whether learning objectives will be derived from the final safety analysis report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training. This was Open Item 18.10.3-8.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-8 is closed.

Criterion 9: Training Presentation

*Criterion:* The design of the training program should be defined to specify how learning objectives will be conveyed to the trainee. The use of lecture, simulator, and on-the-job training to convey particular categories of learning objectives should be defined. Specific plant conditions and scenarios to be used in training programs, and training implementation considerations, such as the temporal order and schedule of training segments, should also be

defined. The training program specifications should include justifications based on HFE principles of training, training practices, and other criteria.

*Evaluation:*

DSER Evaluation

This criterion specifies that the training program design should specify how different methods of training delivery (e.g., simulator, lecture) will be used to convey different categories of learning objectives; how different plant conditions and scenarios will be defined for use in training programs; how training implementation considerations, such as temporal ordering, will be incorporated into training, and will specify justifications for training program specifications based on HFE principles of training, training practices, and other criteria.

Of the items listed in this criterion, only the training implementation considerations appeared to be specifically addressed in the SSAR (Revision 0). These items are addressed under Section 18.9.9.4.2.1 of the SSAR (Revision 0), which discusses the definition and sequencing of instructional units. Using the principles discussed, the curriculum should move from simple to complex, and component skills and knowledge should be integrated in a job context.

While the use of different training delivery methods is discussed, it was not discussed in the context of conveying different learning objective categories. The issue defining different plant conditions and scenarios for use in training programs is also not discussed. Westinghouse should describe how learning objectives will be conveyed to the trainee, and how the other items of this criterion are addressed. This was Open Item 18.10.3-9.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-9 is closed.

Criterion 10: Facilities and Resources

*Criterion:* Facilities and resources, such as plant-referenced simulator and part-task training simulators required to satisfy training design requirements, should be defined.

*Evaluation:*

DSER Evaluation

The SSAR (Revision 0) discussed the need to define the various facilities and resources for training design requirements, but does not discuss how this will be accomplished. Specifically, Section 18.9.9.4.3 of the SSAR (Revision 0) states that during the development of instructional devices and materials, a determination will be made of the instructional staff size, necessary computer equipment, number and size of classrooms, use of state of the art tools and equipment, and development of instructional materials. No discussion was provided concerning the method that will be used to make this determination. Westinghouse should discuss how the various facilities and resources needed to satisfy training design requirements will be identified. This was Open Item 18.10.3-10.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-10 is closed.

Criterion 11: Training Evaluation

*Criterion:* Methods for evaluating trainee mastery of training objectives should be defined, including written and oral tests, walkthroughs, and simulator exercises. Evaluation criteria for training objectives should be defined for individual training modules. Methods for assessing overall proficiency should be defined and coordinated with regulations, where applicable.

*Evaluation:*

DSER Evaluation

Section 18.9.9.4.2.3 of the SSAR (Revision 0) presented a very brief discussion of this criterion, stating that "a periodic evaluation of trainees provides a means for identifying weaknesses and prescribing remediation." The development of evaluation criteria is discussed in Section 18.9.9.4.1 of the SSAR (Revision 0), which indicates that, after the knowledge, skills, and abilities are assigned to the tasks and subtasks, the performance measures will be derived for each task. The discussion was limited, and did not adequately address the criterion. Westinghouse should define the processes by which to identify methods for evaluating trainee mastery of training objectives, as well as overall trainee proficiency. In addition, Westinghouse should specify how evaluation criteria will be defined. This was Open Item 18.10.3-11.

FSER Evaluation

See discussion under training program development Criterion 1: , Training Mission, above. Open Item 18.10.3-11 is closed.

Criterion 12: Adequacy of Materials

*Criterion:* Methods should be defined for verifying the accuracy and completeness of training course materials.

*Evaluation:*

DSER Evaluation

Section 18.9.9.4 of the SSAR (Revision 0) states that techniques, such as memory and sorting tasks and divided-attention tasks, provide a check on whether the training program is appropriate for the skill being trained; however, the SSAR (Revision 0) did not explain how this occurs. Westinghouse should provide additional information on the methods that will be used to verify the accuracy and completeness of training course materials. This was Open Item 18.10.3-12.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-12 is closed.

Criterion 13: Effectiveness of Training Program

*Criterion:* Methods for evaluating the overall effectiveness of the training programs should be defined, including review of operator performance in tests, walkthroughs, simulator exercises, and on-the-job performance.

*Evaluation:*

DSER Evaluation

Based on the material provided in the SSAR (Revision 0), it was not clear how the overall effectiveness of training programs will be evaluated. As discussed in this section under the evaluation of Criterion 3: Systems Approach, of the five steps of SAT, this is the step for which the least information was provided. Westinghouse should identify the process by which appropriate methods will be developed and used to evaluate the overall effectiveness of the training programs. This was Open Item 18.10.3-13.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-13 is closed.

Criterion 14: Training Program Update

*Criterion:* Procedures for refining and updating the content and conduct of training should be established, including procedures for tracking training course modifications.

*Evaluation:*

DSER Evaluation

Section 18.9.9.6 of the SSAR (Revision 0) discussed the use of training program configuration management computer systems, which are an important element in tracking the effects of curriculum changes and initiating changes resulting from plant or job description modifications for the AP600 plant. However, it was not clear how this system will be used to refine and update the content and conduct of training. Westinghouse should describe how the identified training program configuration management computer systems will be used to refine and update the content and conduct of training. This was Open Item 18.10.3-14.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-14 is closed.

Criterion 15: Industry Standards, Guidelines, and Practices

*Criterion:* The applicant's training program should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

No references to NUREG-0711 documents were identified in the training sections of the SSAR (Revision 0), particularly references to NRC documents or guidance documents. Westinghouse should describe how the training program is developed using the requirements and guidance of 10 CFR 50.120, "Training and Qualification of Nuclear Power Plant Personnel"; 10 CFR Part 55, "Operators' Licenses"; and ANSI/ANS 3.1-1981, "Selection, Qualification, and Training of Personnel for Nuclear Power Plants." This was Open Item 18.10.3-15.

FSER Evaluation

See discussion under training program development Criterion 1: Training Mission, above. Open Item 18.10.3-15 is closed.

18.10.4 Conclusions

The objective of the training program review is to ensure that Westinghouse establishes an approach for developing personnel training that incorporates the elements of a systems approach to training, evaluates the knowledge and skill requirements of personnel, coordinates training program development with the other elements of the HFE design process, and implements the training in an effective manner that is consistent with human factors principles and practices.

Following the DSER, Westinghouse identified training as a COL action item. Therefore, the staff did not require resolution of the concerns identified in the DSER for design certification. DSER training issues will be addressed by the COL applicant as part of post-certification design issues.

18.11 Element 10: Human Factors Verification & Validation

18.11.1 Objectives

The objective of this review is to ensure the following:

- the HFE/HSI design provides all necessary alarms, displays, and controls to support plant personnel tasks (HSI Task support verification)
- the HFE/HSI design conforms to HFE principles, guidelines, and standards (HFE design verification)

- the HFE/HSI design can be effectively operated by personnel within all performance requirements (integrated system validation)

- the HFE/HSI design resolves all of the identified HFE issues in the tracking system (human factors issue resolution verification)

- the final "as built" product conforms to the verified and validated design that resulted from the HFE design process (final plant HFE/HSI design verification)

18.11.2 Methodology

18.11.2.1 Material Reviewed

The staff used the following Westinghouse documents in this review:

- SSAR (through Revision 23)
- WCAP-14396 (Revision 2) dated January 27, 1997
- WCAP-14401 (Revision 3) dated May 8, 1997
- WCAP-14822 (Revision 0) dated February 25, 1997
- WCAP-14701 (Revision 1) dated May 9, 1997

18.11.2.2 Technical Basis

The staff focused its review on an evaluation of the Westinghouse documents with respect to the topics and general criteria of Element 10, "Human Factors Verification & Validation," of NUREG-0711.

In its response to RAI 620.79, Westinghouse indicated that a detailed V&V implementation plan will not be submitted for design certification. Westinghouse's response to RAI 620.51 further indicated that detailed verification and validation procedures will not be developed for design certification. The staff reviewed Westinghouse's V&V description at a programmatic review level, because Westinghouse will not complete an implementation plan in this area until after design certification.

18.11.2.3 DSER Item Resolution

To address Element 10 open items, Westinghouse submitted a Draft Document entitled "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan" (April 12, 1995). The document specified the V&V activities to be performed for the AP600 HFE at a high-level. The staff reviewed the draft and provided comments in a telephone conference on May 8, 1995. As a result of the staff's comments, Westinghouse provided a revision to the draft plan on May 10, 1995. Westinghouse published the revised plan as WCAP-14401 (Revision 2), "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan," (August 1996). The plan is referenced in the SSAR (Revision 14), Section 18.11; however, the primary focus of the staff's review was on WCAP-14401. The staff also reviewed additional Westinghouse support documents, WCAP-14701 (Revision 0), "Methodology and Results of Defining Issues for the AP600 Human System Interface Design Test Program," and WCAP-14396 (Revision 1), "Man-in-the-Loop Test Plan," as part of the evaluation of this element.

Element 10 is being reviewed at a programmatic review level; therefore, detailed evaluations using NUREG-0711 acceptance criteria are beyond the scope of the staff review for design certification. At a programmatic level review, NUREG-0711 criteria are used to determine whether the Westinghouse program provides a top-level identification of the substance of each criterion which, after design certification, will be developed (by Westinghouse) into a detailed implementation plan. ITAAC exist for completing the implementation plan and the commitment to the development of such a detailed implementation plan is described in the ITAAC.

Consistent with this approach, WCAP-14401 (Revision 3), indicated that "individual implementation plans that provide more detailed descriptions of the tests to be performed, and acceptance criteria to be used, will be developed for each of the V&V activities specified in this document" (p.1). The commitment to develop detailed implementation plans was reiterated in Section 1.3 of the WCAP.

18.11.3 Results

The staff reviewed the general criteria for V&V, HSI task support verification, HFE design verification, integrated system validation, human factors issue resolution verification, and final plant HFE/HSI design verification of the AP600 HFE program to determine whether it acceptably addresses the topics and general criteria of Element 10 of NUREG-0711.

18.11.3.1 General Criteria

Criterion 1: General Criteria

*Criterion:* As defined in Element 1, "Human Factors Engineering Program Management," the general scope of V&V should include the following for all applicable facilities:

- HSI hardware
- HSI software
- communications
- procedures
- workstation and console configurations
- design of the overall work environment
- trained personnel

The scope of the integrated system validation may be limited to those applicable facilities required for the evaluation of scenarios described in Criterion 4: Critical Human Actions, in Section 18.11.3.4 of this report.

*Evaluation:*

DSER Evaluation

The general scope of the V&V program plan contained in Sections 18.5 and 18.8 of the SSAR (Revision 0) addresses the identified aspects of the HSI. In its response to RAI 620.82, Westinghouse indicated that local control stations (LCSs) at which critical human actions for abnormal and emergency procedures will be performed will be included in the V&V plan.

Evaluation Issue 16 (described in Section 18.8.2.3.5.4 of the SSAR, Revision 0) and Evaluation Issue 17 (described in Section 18.8.2.3.5.5 of the SSAR, Revision 0) pertaining to Technical Support Center (TSC) inclusion need to be clarified for closure of this criterion.

Westinghouse should clarify the role of the TSC in Evaluation Issues 16 and 17. This was Open Item 18.11.3.1-1. This is also discussed under Criterion 1, "Personnel Task Requirements," in Section 18.11.3.3 and Criterion 2, "Dynamic Task Performance," in Section 18.11.3.4 of this report.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse clarified the scope of the V&V effort. Section 1.2 provides the scope of the V&V tests and includes the NUREG-0711 identified scope including the TSC. Westinghouse modified their scope from that provided in their response to RAI 620.82 and indicated that, although the current design of the AP600 does not require risk-significant actions to be taken at LCSs, such actions will be included in V&V should any be identified in future analyses.

Based on this information, Open Item 18.11.3.1-1 is closed and the NUREG-0711 criterion is satisfied.

Criterion 2: Sequence for V&V

*Criterion:* The sequence for completing V&V activities should be as follows:

(1) HSI task support verification
(2) HFE design verification
(3) integrated system validation
(4) human factors issue resolution verification
(5) final plant HFE/HSI design verification

*Evaluation:*

DSER Evaluation

Activities for human factors issue resolution, HSI task support verification, and final plant HFE/HSI design verification are not discussed in the SSAR (Revision 0). Therefore, the sequence for completing V&V activities cannot be addressed. This criterion cannot be addressed until the component V&V issues are addressed. Westinghouse should clarify (a) the role of human factors issue resolution, HSI task support verification, and final plant HFE/HSI design verification in the V&V activities, and (b) the sequence of V&V activities. This was Open Item 18.11.3.1-2.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse clarified the evaluations to be performed as part of the V&V effort. Section 1.1 identifies and defines the five evaluation activities as: task support verification, HFE design verification, integrated system validation, issue resolution verification, and final plant HFE verification. Figure 1 of WCAP 14401 (Revision 3), illustrates the sequence

of activities and is consistent with that specified in NUREG-0711 criterion. Based on this information, Open Item 18.11.3.1-2 is closed and the NUREG-0711 criterion is satisfied.

Criterion 3: Industry Standards, Guideline, and Practices

*Criterion:* The applicant's V&V effort should be developed using accepted industry standards, guidelines, and practices. A list of documents that may be used as guidance is provided in NUREG-0711.

*Evaluation:*

DSER Evaluation

The SSAR (Revision 0) does not identify the industry standards and guidelines that will guide the development of the V&V implementation plan. Westinghouse should describe the guidance documentation used to develop the V&V program. This was Open Item 18.11.3.1-3.

FSER Evaluation

In WCAP-14401 (\Revision 3), Westinghouse has clarified the technical basis of the V&V effort. Section 1.3 identifies the industry standards, guidelines, and supporting documents that will serve as the basis of V&V methodology development. These documents include the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronic Engineers (IEEE) guidelines as well as the NRC documents that are appropriate to V&V.

Based on this information, Open Item 18.11.3.1-3 is closed and the NUREG-0711 criterion is satisfied.

18.11.3.2 HSI Task Support Verification

Criterion 1: Verification of the HSI

*Criterion:* All aspects of the HSI (e.g., controls, displays, procedures, and data processing) that are required to accomplish human tasks and actions as defined by the task analysis, EOP analysis, and critical actions of the PRA and HRA should be verified as available through the HSI.

*Evaluation:*

DSER Evaluation

HSI task support verification was not clearly addressed as part of the V&V activities. In its response to RAI 620.81, Westinghouse indicated that the design review of displays and controls will confirm that needs identified through task analysis are satisfied at the HSI. However, the timing of such a review, and procedures for conducting such reviews as part of verification, were not identified.

Westinghouse should commit to developing a methodology for HSI task support verification and its related criteria. The implementation plan should describe how all aspects of the HSI required to accomplish the human tasks and actions demanded by the AP600 design will be verified. This was Open Item 18.11.3.2-1. This is also discussed below under Criterion 2: "Operator Tasks."

FSER Evaluation

See discussion under Criterion 2: Operator Tasks, below.

Criterion 2: Operator Tasks

*Criterion:* The applicant should verify that the HSI does not include information, displays, controls, and so forth, that do not support operator tasks. This includes non-functional, decorative details, such as borders and shadowing on graphical displays.

*Evaluation:*

DSER Evaluation

Westinghouse addressed this aspect of verification in its response to RAI 620.81, which indicates that unnecessary (as defined by task analysis) indications and controls will be deleted. During a meeting on December 13, 1994, the staff expressed concern that this decision should not be made on the basis of task analysis alone, and that an operational review should be performed to verify that deletion of any aspect of the HSI was acceptable. Westinghouse agreed with the staff's concern. This review should be addressed in the implementation plan.

Westinghouse should describe how the V&V methodology will verify that the HSI does not include information, displays, controls, and so forth, that do not support operator tasks. This was part of Open Item 18.11.3.2-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their approach to HSI task support verification. Section 2 identified the objective and high-level methodology for conducting the evaluation. The analysis will address the availability of HSI features for accomplishing personnel tasks and actions as defined by the task analyses, the EOPs, and the risk-important human tasks identified by the PRA. This commitment satisfactorily addresses Criterion 1.

The plan also indicated that the methodology shall describe how, in each case, the HSI design will be verified to ensure that the HSI does not include information, controls, and displays that do not support operator tasks. A process for checking such HSI features will include an analysis before any information is removed from the HSI. This commitment satisfactorily addresses Criterion 2.

Based on this information, Open Item 18.11.3.2-1 is closed and the NUREG-0711 criteria are satisfied.

18.11.3.3 HFE Design Verification

Criterion 1: Personnel Task Requirements

*Criterion:* All aspects of the HSI (e.g., controls, displays, procedures, and data processing) should be verified as designed to be appropriate to personnel task requirements and operational considerations as defined by design specifications. In addition, all aspects of the HSI should be consistent with accepted HFE guidelines, standards, and principles.

*Evaluation:*

DSER Evaluation

HFE design verification is described in Section 18.8.2.3.5.4.1 of the SSAR (Revision 0) under Evaluation Issue 16. The acceptance testing aspect of Evaluation Issue 16 addresses NUREG-0711 level verification. The focus of this verification is on evaluating that (a) individual M-MIS components satisfy human engineering criteria, and (b) the integration of M-MIS components satisfies human engineering criteria for work environments. The guidelines are applied to the MCR, remote shutdown station, and other local panels. The item regarding the verification of TSC M-MIS components discussed under Criterion 1: General Criteria, in Section 18.11.3.1 of this report applies to this verification.

Procedures for verification were not identified and are beyond the scope of design certification. The sources of guidance documents to be used in these verifications have not been precisely identified. Table 18.5.1 of the SSAR (Revision 0) identifies NUREG-0700, MIL-STD-1472, ANSI/HFS 100-1988, ASHRAE STD 55-1981, and EPRI-3659 as the documents included. The staff was concerned with the completeness and appropriateness of these documents for verification of an advanced control room, and requested additional information regarding the technical basis of verification guidelines in RAI 620.20 and RAI 620.59. Westinghouse indicated that the listed documents show an illustrative subset of the guidelines to be used. Additional documents will be reviewed for possible inclusion in the list. The actual verification will be based on six guideline documents addressing alarms, displays, controls, training, anthropometry, and subsystem integration. These documents were not provided to the staff. However, it is not apparent from the document titles that important topics, such as procedure HSI design and user-system interaction design (e.g., dialogue format and navigation tools) are addressed by the documents and, therefore, in the HFE design verification.

Westinghouse should commit to developing a methodology for HFE design verification and related criteria, taking into consideration the concerns identified in the staff's evaluation of this criterion. This was Open Item 18.11.3.3-1. This is also discussed below under Criterion 2: Deviations.

FSER Evaluation

See the discussion under Criterion 2: Deviations, that follows.

Criterion 2: Deviations

*Criterion:* Deviations from accepted HFE guidelines, standards, and principles should be acceptably justified based on a documented rationale, such as trade study results, literature-based evaluations, demonstrated operational experience, and tests or experiments.

*Evaluation:*

DSER Evaluation

Westinghouse did not address the handling of deviations in the SSAR (Revision 0). Westinghouse should describe how deviations identified in the criterion will be addressed in the V&V methodology. This was part of Open Item 18.11.3.3-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described the general approach to HFE Design Verification. Section 3 identifies the objective and high-level methodology for conducting the evaluation. The analysis will address the verification that all aspects of the HSI are consistent with accepted HFE guidelines, standards, and principles. The verification will utilize AP600-specific guidance documents and will cover alarms, displays, controls, data processing, navigation, computerized procedures, workstation and console configurations, and anthropometric considerations and their integration. The document identifies an illustrative subset of the documents that will be used in the development of the AP600-specific guidance. It includes the most recent control room design guidance including IEC 964 and NUREG-0700 (Revision 1). This commitment satisfactorily addresses the staff's DSER concerns with regard to Criterion 1.

The plan also identified the process through which guidelines deviations will be addressed and their technical basis documented. This commitment satisfactorily addresses Criterion 2.

Based on this information, Open Item 18.11.3.3-1 is closed and the NUREG-0711 criterion is satisfied.

18.11.3.4 Integrated System Validation

Criterion 1: Methodology

*Criterion:* The methodology for integrated system validation should address the following items:

- general objectives
- personnel performance issues to be addressed (e.g., crew coordination)
- test methodology and procedures
- test participants (operators to participate in the test program)
- test conditions (including plant conditions, operating sequences, and accident scenarios)
- HSI description
- performance measures
- data analysis

- criteria for evaluation of results
- use of evaluations

*Evaluation:*

DSER Evaluation

The technical review of this item is beyond the scope of the design certification review because it is within the framework of the V&V implementation plan. Westinghouse should commit to developing a methodology for integrated system validation and related criteria. This was Open Item 18.11.3.4-1. This is also discussed under Criteria 2 through 8, which follow.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described the general approach to integrated system validation. Section 4 identifies the objective and high-level methodology for conducting the evaluation. Section 4.1 identifies the aspects to the methodology that will be addressed in the implementation plan. Each of the topics identified in the NUREG-0711 is included. In addition, the plan addresses the process by which results will be used to evaluate potential design changes and, where made, their subsequent verification.

Based on this information, Open Item 18.11.3.4-1 is closed and the NUREG-0711 criterion is satisfied.

Criterion 2: Dynamic Task Performance

*Criterion:* Validation should be performed by evaluating dynamic task performance using tools that are appropriate to the accomplishment of this objective. The primary tool for this purpose is a simulator (i.e., a facility that physically represents the HSI configuration and that dynamically represents the operating characteristics and responses of the plant design in real time). The requirement to validate performance at plant HSIs outside the CR will depend on the applicant's design. Human actions at non-CR facilities, such as remote shutdown panels and LCSs, may be evaluated using mockups, prototypes, or similar tools.

*Evaluation:*

DSER Evaluation

Section 18.8.2.3.5.5.1 of the SSAR (Revision 0) and Westinghouse's response to RAI 620.18 describe the tools to be employed for validation testing. Specifically, Westinghouse will use a "near full-scope, high fidelity simulator consisting of integrated M-MIS components and a high-fidelity dynamic simulation of plant behavior." As indicated previously in the evaluation of Criterion 1: General Criteria, in Section 18.8.3.1 of this report, the role of the TSC needs clarification. Westinghouse should describe the tools to be used in evaluating dynamic task performance in the V&V methodology. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described the general approach to Integrated system validation. Section 4.2 addressed the tools for conduction validation. A "near full-scope" simulator will be used. "Near" means that features of the simulation that are not relevant to the tests being performed may not be high-fidelity. Personnel actions that are performed at non-control room facilities, such as remote shutdown panels and the TSC may be evaluated using static mock-ups or prototypes.

As a result of reviewing the SSAR (Revision 23) and several supporting WCAPs, the staff identified the need for further clarification from Westinghouse on their use of the simulator as an evaluation tool for the AP600 HSI design. Specifically, WCAP-14401 (Revision 3), Section 4.0, describes Westinghouse's approach for addressing integrated system validation. Westinghouse indicated that "integrated system validation will be performed using an AP600-specific, near full-scope, high-fidelity simulator of the AP600 control room that is *similar to a training simulator.* However, Figure 1.1 of WCAP-14401 (Revision 3), identifies that Integrated system validation will utilize an AP600-specific, near full-scope, high-fidelity, *trainingsimulator.* In WCAP-14396 (Revision 2), "Man-in-the-Loop Test Plan Description," Section 3.0, "Formal V&V of Final HSI Design," Westinghouse indicated that formal HFE/HSI design V&V will be performed when an AP600 plant has been purchased and will use an AP600 dynamic, high-fidelity *training simulator.* In Westinghouse's September 15, 1992, letter to the NRC (ET-NRC-92-3748), in addressing item F (Role of the Operator in a Passive Plant Control Room), Westinghouse stated that a high-fidelity, near full scope control room prototype (*equivalent to a training simulator*) is included near the end of the [man-in-the-loop testing] program to perform certain verification and validation tests. Westinghouse should clearly describe (1) the use of each simulator type (near full-scope, high-fidelity simulator that is similar to a training simulator; near full-scope, high-fidelity training simulator; training simulator); (2) the differences that exist among the simulator types; and (3) the guidance/information sources that might be used to support their development (e.g., ANSI 3.5, Reg. Guide 1.149; other industry-related guidance).

As was indicated in the discussion of Open Item 18.11.3.1-1 above, the staff recognizes that, at present, the AP600 design does not require risk-significant actions to be taken from LCSs, therefore they are not included in the scope of V&V. Further, as indicated in that discussion, this is acceptable to the staff because Westinghouse will include such LCSs in V&V evaluations should the further detailed design of the plant require a risk-important action to be performed at a LCS. Given this interpretation, the staff's DSER concerns with regard to Criterion 2 are addressed.

This commitment satisfactorily addressed Criterion 2; however, this was an open item until the staff's questions were addressed in a revision to the SSAR or an appropriate, docketed, secondary reference. On May 8, 1997, Westinghouse submitted WCAP-14401 (Revision 3), which formally addressed the staff's remaining concerns related to this open item.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 3: Integrated System Validation Evaluations

*Criterion:* The integrated system validation evaluations should incorporate the following:

- address the adequacy of the entire HSI configuration for achieving HFE program goals
- confirm allocation of function and the structure of tasks assigned to personnel
- address the adequacy of staffing and the HSI to support staff to accomplish their tasks
- address the adequacy of procedures
- confirm the dynamic aspects of the HSI for task accomplishment
- evaluate and demonstrate error tolerance to human and system failures

*Evaluation:*

DSER Evaluation

Section 18.8.2.3.5.5.1 of the SSAR (Revision 0) indicated that the general question being addressed is the support for operator performance during normal, abnormal, and emergency conditions provided by the integration of M-MIS components in the MCR. The purpose of the evaluation is to determine whether the M-MIS, as designed and implemented, supports the safe and efficient operation of the plant for the conditions addressed by the design mission. This approach is consistent with NUREG-0711 criterion; however, the SSAR (Revision 0) did not identify the specific types of evaluations that should be addressed in the implementation plan. Westinghouse should describe how the V&V methodology will address the objectives listed as part of this criterion. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their general approach to integrated system validation. Section 4.3 identified the objectives of Integrated system validation. The implementation plan will specifically address each of the objectives identified in NUREG-0711.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 4: Critical Human Actions

*Criterion:* All critical human actions (as defined by the task analysis, PRA, and HRA) including the performance of critical actions outside the control room, should be tested and found to be adequately supported in the design. The design of tests and evaluations to be performed as part of HFE V&V activities should specifically examine these actions.

*Evaluation:*

DSER Evaluation

In its response to RAI 620.51, Westinghouse identified WCAP-9817 and WCAP-12601 as describing "the scope and process for verification of the M-MIS to ensure that all critical human actions as defined by the task analysis and PRA have been adequately supported in the design, and that the V&V program explicitly addresses these issues." These WCAPs were not available

to the staff to support this stage of the review. Westinghouse should describe how the testing of critical human actions will be addressed in the V&V methodology. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described the general approach to integrated system validation. Section 4.4 identifies the specific commitment to validate the performance of risk-important tasks. These tasks are defined as (1) important and representative tasks defined in task analysis, (2) risk important tasks defined by the PRA threshold criteria, and design-basis and beyond-design-basis accident scenarios covered by the EOPs.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 5: Compliance with Regulatory Guide 1.33

*Criterion:* Appendix A to RG 1.33 contains several categories of activities that should be covered by procedures. The validation should evaluate selected evolutions based upon procedures developed to address this guide. The evaluation should include appropriate procedures in each relevant category, as follows:

- administrative procedures
- general plant operating procedures
- procedures for startup, operation, and shutdown of safety-related systems
- procedures for abnormal, offnormal, and alarm conditions
- procedures for combating emergencies and other significant events
- procedures for control of radioactivity
- procedures for control of measuring and test equipment
- procedures for surveillance tests, procedures, and calibration
- procedures for performing maintenance
- chemistry and radiochemical control procedures

*Evaluation:*

DSER Evaluation

This matter was not addressed in the SSAR (Revision 0). Westinghouse should describe how the V&V methodology will address the categories identified in Appendix A to RG 1.33 regarding procedure-related activities. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In discussions of this criterion, Westinghouse requested clarification of whether each category of procedures indicated in the NUREG-0711 criterion is to be addressed by validation. The staff indicated that RG 1.33 categories were included in NUREG-0711 because they encompass "typical safety-related activities that should be covered by written procedures." Thus, all of the above categories should be represented in the scenario sampling process. However, it is recognized that not all categories need to receive equal emphasis and some categories (e.g.,

administrative procedures and procedures for performing maintenance) may be best evaluated as an adjunct to other tests.

Administrative procedures are important to safe plant operation; however, they may not need to be tested as completely as EOPs. Instead, selected situations governed by such procedures should be reflected in validation scenarios to ensure that the AP600 MCR design, in conjunction with such procedures, can achieve their intended functions without interfering with plant operations. Thus, for example, situations involving equipment control (e.g., locking and tagging of equipment), shift and relief turnover, or maintenance of minimum shift complement and call-in of personnel, could be incorporated into selected test scenarios or validated separately.

Procedures for performing maintenance are least amenable to validation of the type covered by this NUREG-0711 criterion. While the staff considers the design for maintenance an important aspect of plant design and one which is addressed by the HFE program, it does not typically involve validation of an integrated system. The staff does think it is appropriate to validate maintenance that is to be performed in the MCR while the plant is being operated. This validation should show that it can be accomplished without interfering with operator tasks that are necessary for monitoring and controlling the plant. Thus, in this restricted context, procedures for performing maintenance should be included as a small part of validation tests.

As is indicated in RG 1.33, the procedures may be combined, separated, or deleted to conform to the applicant's procedures plan. The same approach is applicable to integrated system validation. The main goal of integrated system validation is to evaluate the performance of the integrated system in "operational" contexts, and not to validate procedures or any other single aspect of the design. Reference in NUREG-0711 to the procedure categories is to provide an aid to defining the range of operational contexts that are appropriate to the integrated system performance.

Westinghouse includes a discussion of their treatment of RG 1.33 procedures in WCAP-14401 (Revision 3). Section 4.5 indicates that Westinghouse will include test scenarios that create situations governed by sample procedures from selected RG 1.33 procedures to ensure the performance of plant operations.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 6: Dynamic Evaluations

*Criterion:* Dynamic evaluations should evaluate the HSI under a range of operational conditions and upsets, and should include the following events:

- normal plant evolutions (e.g., startup, full power, and shutdown operations)
- instrument failures (e.g., the SSLC unit, fault tolerant controller, local "field unit" for the MUX system, or a break in a MUX line)
- HSI equipment and processing failure (e.g., loss of VDUs, data processing, or the large overview display)

- transients (e.g., turbine trip, loss of offsite power, station blackout, loss of all feedwater, loss of service water, loss of power to selected buses or MCR power supplies, or SRV transients)

- accidents (e.g., main steamline break, positive reactivity addition, control rod insertion at power, control rod ejection, ATWS, and various sized LOCAs)

- reactor shutdown and cooldown from the remote shutdown panel

*Evaluation:*

DSER Evaluation

In RAI 620.60, the staff requested information regarding condition scenario types, such as instrument failures, HSI equipment and processing failures, and accidents. Westinghouse indicated that plant conditions (such as those identified in this criterion) will be addressed during validation, and scenario selection will be defined in terms of cognitive demands. When the cognitive selection criteria are mapped onto specific test scenarios, the resulting set of scenarios will include the types of events listed. However, at the present level of description provided in the SSAR (Revision 0), it is not possible to determine whether the proposed approach will result in the scenario diversity specified in NUREG-0711. Additional information regarding the identifications of test scenarios for Evaluation 17 should be included in the implementation plan.

Westinghouse should describe how the V&V methodology will evaluate performance under a range of operational conditions and upsets, and provide additional information about the Evaluation 17 test scenarios. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their general approach to integrated system validation. Section 4.6 discusses the selection of test scenarios. Test scenarios will be defined using a multi-dimensional set of criteria. The dimensions are identified and include all of the types of scenarios included in NUREG-0711. In addition, Westinghouse identified design features that are specific to the AP600 such as ADS, situations that are cognitively challenging to the crew such as complicated situation assessment under conflicting plant state information, and scenarios that would enable validation of key HRA assumptions.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 7: Realistic Validation Scenarios

*Criterion:* The validation scenarios should be realistic. Selected scenarios should include environmental conditions, such as noise and distractions, which may affect human performance in an actual nuclear power plant. For actions outside of the control room, the performance impacts of potentially harsh environments (i.e., high radiation) that require additional time should be realistically simulated (i.e., time to don protective clothing and access hot areas).

*Evaluation:*

DSER Evaluation

This matter was not addressed in the SSAR, (Revision 0). Westinghouse should describe how the validation scenarios will be made realistic as part of the V&V methodology. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their general approach to integrated system validation. Section 4.7 addresses how the scenarios selected for validation will be made realistic. Considerations regarding the incorporation of environmental conditions, communication demands, number of personnel in the control room are identified in the program description.

Based on this information, the NUREG-0711 criterion is satisfied.

Criterion 8: Adequacy of Performance Measures

*Criterion:* Performance measures for dynamic evaluations should be adequate to test whether all objectives, design goals, and performance requirements were achieved, and should include as a minimum the following items:

- system performance measures relevant to plant safety
- crew primary task performance (e.g., task times and procedure violations)
- crew errors
- situation awareness
- workload
- crew communications and coordination
- dynamic anthropometry evaluations
- physical positioning and interactions

*Evaluation:*

DSER Evaluation

Section 18.8.2.3.5.5.1 and Sheet 8 of Table 18.5-2 of the SSAR (Revision 0) identified task completion time and task completion success as the performance measures for validation. In addition, decision tracing will be used to evaluate participant decisions and actions. Following scenarios, participants will be debriefed to assess their understanding of plant conditions and how features of the M-MIS contributed to their performance.

In RAI 620.84, the staff requested information concerning the measurement of situation awareness and workload. In its response, Westinghouse indicated that workload will be assessed in validation studies. However, while situation awareness is a major consideration in concept tests, it will not "be a primary focus" in validation. Situation awareness would be assessed only indirectly through observation of task performance. Situation awareness should

be given consideration similar to workload. Westinghouse indicated that workload measures are most useful when complete integrated operator tasks are being performed. The same logic applies to situation awareness. Accurate situation awareness may be more difficult to establish when complete integrated operator tasks are being performed. At such a time, the operator's workload may be higher and the situations encountered more complex. In fact, workload and situation awareness are closely linked. When workload goes up, operators cognitively cope by employing information processing heuristic and task management strategies. Both can impact the operator's ability to form situation awareness.

Westinghouse should describe how the V&V methodology will address performance measures to test the achievement of all objectives, design goals, and performance requirements. This was part of Open Item 18.11.3.4-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their general approach to integrated system validation. Section 4.8 discusses performance measurement, and the aspects of integrated system performance identified in NUREG-0711 are included. Westinghouse indicated that the process by which objective acceptance criteria is developed for each measure will be defined in the implementation plan.

Based on this information, the NUREG-0711 criterion is satisfied.

18.11.3.5 Human Factors Issue Resolution Verification

Criterion 1: Verification of Issue Resolution

*Criterion:* All issues documented in the human factors issue tracking system of Element 1, "Human Factors Engineering Program Management," should be verified to be adequately addressed.

*Evaluation:*

DSER Evaluation

In RAI 620.80, the staff requested information concerning issue resolution verification. Westinghouse indicated that the issues were tracked using a "human factors checklist," and their closure is identified in system design documentation, which is subject to design reviews. In its response to RAI 620.51, Westinghouse identified WCAP-12601 as the document describing the process for closing open DCPs. However, as discussed in Section 18.2.3.4 of this report, Westinghouse had not yet described an acceptable HFE issues tracking system (Open Item 18.2.3.4-1). Until that open item was resolved, the staff could not determine the acceptability of using the approach described in Westinghouse's response to RAI 620.80. Westinghouse should commit to developing a methodology for human factors issue resolution verification and related criteria. This was part of Open Item 18.11.3.5-1. This is also discussed below under Criterion 2: Plant-Specific Items.

FSER Evaluation

See discussion under Criterion 2: Plant-Specific Items, below.

Criterion 2: Plant-Specific Items

*Criterion:* Issues that cannot be resolved until a plant is built should be specifically identified and incorporated into the process for final plant HFE/HSI design verification.

*Evaluation:*

DSER Evaluation

The SSAR (Revision 0) did not address the resolution of issues that remain until the plant is built. Westinghouse should describe how the V&V methodology will address issues that cannot be resolved until a plant is built, and how such issues will be incorporated into the process for final plant HFE/HSI design verification. This was part of Open Item 18.11.3.5-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described their general approach to issue resolution verification. Section 5 provides a commitment to develop a procedure to ensure that all issues documented in the HFE issue tracking system are verified to be completely addressed in the final HSI. This commitment satisfactorily addresses the staff's DSER concerns with regard to Criterion 1.

The program description further states that the implementation plan will describe a procedure for identifying and tracking HFE issues that cannot be resolved until a plant is built. This procedure will address how verification of these issues will be incorporated into the process for final plant HFE verification. This commitment satisfactorily addresses Criterion 2.

Based on this information, Open Item 18.11.3.5-1 is closed and the NUREG-0711 criteria are satisfied.

18.11.3.6 Final Plant HFE/HSI Design Verification

Criterion 1: Design Description

*Criterion:* Following design process V&V activities, a design description should be developed that describes the detailed design and its performance criteria.

*Evaluation:*

DSER Evaluation

The final plant HFE/HSI design verification was not addressed in the SSAR (Revision 0). Westinghouse should commit to developing a methodology for final plant HFE/HSI design

verification and related criteria. This was Open Item 18.11.3.6-1. This is also discussed below under Criterion 2: V&V for Additional Design Aspects, and Criterion 3: In-Plant HFE.

FSER Evaluation

See discussion under Criterion 3: In-Plant HFE, below.

Criterion 2: V&V for Additional Design Aspects

*Criterion:* Aspects of the design that were not addressed in design process V&V should be evaluated using an appropriate V&V method. Aspects of the design addressed by this criterion may include design characteristics, such as new or modified displays for plant-specific design features and features that cannot be evaluated in a simulator, such as control room lighting and noise.

*Evaluation:*

DSER Evaluation

The final plant HFE/HSI design verification was not addressed in the SSAR (Revision 0). Westinghouse should describe how the V&V methodology will address aspects of the design that cannot be addressed in design process V&V, and how they will be addressed as part of the final plant HFE/HSI design verification. This was part of Open Item 18.11.3.6-1.

FSER Evaluation

See discussion under Criterion 3: In-Plant HFE, below.

Criterion 3: In-Plant HFE

*Criterion:* The in-plant HFE should conform to the design that resulted from the HFE design process and V&V activities.

*Evaluation:*

DSER Evaluation

The SSAR (Revision 0) did not address the final plant HFE/HSI design verification. Westinghouse should describe how the V&V methodology will address conformance of the in-plant HFE to the design that resulted from the HFE design process and V&V activities. This was part of Open Item 18.11.3.6-1.

FSER Evaluation

In WCAP-14401 (Revision 3), Westinghouse described the general approach to final plant HFE/HSI design verification. Section 6 provides a commitment to develop a methodology for verifying that the in-plant HFE conforms to the HSI design that results for the HFE design process and V&V activities. The HSI is defined in the final functional requirements and design description. Conformance of the actual system to this description is verified during factory

acceptance tests and site acceptance tests. The implementation plan will specify the verifications to be performed. This commitment satisfactorily addresses Criteria 1 and 3.

The program description indicates that the implementation plan will include procedures for identifying and evaluating aspects of the HSI that were not addressed during prior V&V activities. This satisfies Criterion 2.

Based on this information, Open Item 18.11.3.6-1 is closed and the NUREG-0711 criteria are satisfied.

18.11.4 Conclusions

The V&V review was conducted at a program plan level of detail, and was directed toward determining whether the program plan addressed NUREG-0711 criteria at a high level. The staff expects the V&V program to be developed in greater detail in the implementation plan.

At a programmatic level, the most significant finding from the staff's DSER review was that several NUREG-0711 V&V criteria were not clearly addressed. NUREG-0711 identifies five types of V&V. The Westinghouse V&V program was directed towards HFE design verification and validation. HSI task support verification, human factors issue resolution verification, and final plant HFE/HSI design verification were not clearly addressed as V&V activities. Subsequent to the staff's DSER, Westinghouse acceptably addressed the DSER open items including those related to V&V types. The staff has completed its review of Element 10, "Human Factors Verification & Validation," of NUREG-0711 with all DSER open items having been closed. The COL applicant referencing the AP600 certified design has the responsibility for developing, documenting, and executing the implementation plan for the verification and validation of the AP600 human factors engineering program. This is COL Action Item 18.11-1.

18.12 Minimum Inventory

As part of the general resolution of the lack of control room detail, the staff requested that applicants for design certification identify the minimum group of fixed-position controls, displays, and alarms that are required for transient and accident mitigation. In RAI 620.50, the staff requested that the AP600 minimum inventory be determined on the basis of the AP600 ERGs and the operator actions that are determined by PRA analyses to be significant contributors to plant risk. The information regarding the minimum inventory for AP600 is contained in Sections 7.5 and 18.12 of the SSAR. It should be noted that the inventory is described as a "minimum" inventory to indicate that an applicant can add to it but cannot delete from it without changing the list in the AP600 Tier 1 material. This would require a significant rulemaking effort.

18.12.1 Objectives

The objective of this review is to ensure that analysis of the AP600 ERGs and operator actions, that are determined to be significant contributors to plant risk by PRA analyses, result in an acceptable minimum inventory of fixed-position controls, displays, and alarms for transient and accident mitigation.

18.12.2 Methodology

18.12.2.1 Material Reviewed

The staff reviewed the following material:

- SSAR (through Revision 23)
- WCAP-14651 (Revision 2)
- AP600 Emergency Response Guidelines (Revision 2), 12/31/96
- AP600 Emergency Response Guidelines Background Documents (Revision 2), 12/31/96
- List of AP600 critical actions contained in WCAP-14651 (Revision 2), "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan"

18.12.2.2 Technical Basis

The review was focused on evaluating the Westinghouse submitted material to ensure that proposed methodology met the overall intent of the staff request for a minimum inventory and that it was properly carried out by Westinghouse. Regulatory Guide (RG) 1.97, (Revision 3, May 1983), was used to support the identification of minimum inventory instrumentation.

18.12.2.3 DSER Item Resolution

The staff RAI 620.50 dated April 29, 1993, and DSER Open Item 18.12.3-1, requested Westinghouse to develop a minimum inventory of fixed-position controls, displays, and alarms, (CDAs) based on a detailed OSAs. The Westinghouse response was that the various analyses to be performed in support of the AP600 design will determine the need for CDAs and that a minimum inventory had not been developed to date. Subsequently, in a meeting on February 2, 1995, Westinghouse provided the staff with a draft proposal on the minimum inventory process. Based on that discussion, the staff and Westinghouse continued dialog to determine the scope of the minimum inventory. The staff provided Westinghouse its position on the development of a minimum inventory in a letter from the NRC to Westinghouse, dated August 21, 1995, which was followed up by various conference calls between the staff and Westinghouse. To address the staff's position, Westinghouse submitted SSAR Section 18.12 (Revision 9), dated August 9, 1996, "Displays, Alarms, and Controls," subsequently revised to SSAR Section 18.12, "Inventory," (Revision 10) which provided a description of the minimum inventory development process, including a proposed list of CDAs comprising the inventory.

The staff transmitted their review to Westinghouse by letter in January 1997. Conference calls were held on February 5 and 6, 1997, to discuss the Westinghouse proposed resolution to the identified issues. Westinghouse agreed to make additional changes to the SSAR and the minimum inventory to address staff concerns. SSAR revisions 14 through 23 were submitted with these changes incorporated.

18.12.3 Results

Criterion 1: Scope of Minimum Inventory

*Criterion:* The inventory should provide criteria that define a reasonable minimum set of fixed-position controls, displays, and alarms to adequately implement the ERGs for the AP600 design, account for the critical operator actions identified in the AP600 PRA, and mitigate transients and accidents associated with the ERGs and the PRA sensitivity study results.

*Evaluation:*

DSER Evaluation

The staff could not complete its evaluation of this criterion because Westinghouse had not defined a minimum inventory for the AP600 design. Westinghouse should submit an acceptable minimum inventory of fixed-position controls, displays, and alarms for transient mitigation. This was Open Item 18.12.3-1. This is also addressed under Criterion 6, "Minimum Inventory," in Section 18.5.3 of the DSER, and in the following Criteria 2 through 4.

FSER Evaluation

In Revision 14 of the SSAR, Westinghouse submitted their methodology for the determination of the minimum inventory, as well as the results of the method. This is contained in Sections 7.5 and 18.12 of the SSAR. The AP600 is designed such that the primary controls, displays, and alarms are computer-based and "soft." Soft controls and displays are software-defined and can be changed to perform different functions. Their locations are not dedicated like hard controls and displays. The basis for this design choice is described and justified in Chapter 18 of the SSAR. It is based upon a combination of operating experience, research, and testing.

In addition to the soft controls and displays, Westinghouse has committed to providing a minimum set or inventory of dedicated or fixed-position instrumentation. Per Section 18.12.2 of the SSAR, this minimum inventory is used (1) to monitor the status of CSF, (2) to manually actuate the safety-related systems that achieve these CSFs, and (3) to establish and maintain safe-shutdown conditions. These fixed-position controls, displays, and alarms are available at a fixed location. They are continuously available, but not necessarily continuously displayed to the operator. This is an acceptable approach.

In SSAR Section 18.12.2, Westinghouse described the characteristics or selection criteria which they used to develop the minimum inventory. The five criteria are as follows:

(1) RG 1.97 Types A, B, and C, Category 1 instrumentation

(2) dedicated controls for manual safety-related system actuation (reactor trip, turbine trip, and engineered safety feature actuation)

(3) controls, displays, and alarms required to perform critical manual actions as identified from the PRA analysis

(4) alarms provided for operator use in performing safety functions to respond to design-basis events for which there is no automatically-actuated safety function

(5) controls, displays, and alarms necessary to maintain the [EOP] CSF and safe-shutdown conditions

These characteristics or criteria address a reasonable minimum set of fixed-position controls, displays, and alarms for the minimum inventory. Each of these characteristics is discussed in more detail in the SSAR and are evaluated under subitem 2 below.

Based on this information, Open Item 18.12.3-1 is closed and the minimum inventory criterion is satisfied.

Criterion 2: Development of Actual Items in the Minimum Inventory

*Criterion:* The development of actual items in the minimum inventory should include an acceptable set of controls, displays, and alarms developed from the defined scope and criteria of the above Criterion 1. It should appropriately address required operator actions in the emergency procedures or procedure guidelines.

*Evaluation:*

DSER Evaluation

The staff could not complete its evaluation of this criterion because Westinghouse had not defined a minimum inventory for the AP600 design. Westinghouse should describe the technical basis for the minimum inventory. This was part of Open Item 18.12.3-1.

FSER Evaluation

As noted above, Westinghouse described five characteristics or criteria for defining the minimum inventory. These five characteristics are evaluated here.

(1) RG 1.97 Types A, B, and C, Category 1 instrumentation

RG 1.97 defines a method for the determination of plant variables to be monitored by control room operators, and for the definition of the appropriate instrumentation to be used for those variables. The criteria of the RG are separated into three categories that provide a graded approach to requirements depending on the importance of the measurement of a specific variable to safety. Category 1 provides the most stringent requirements and is intended for key variables. Thus, the limitation to Category 1 here is appropriate.

Type A variables provide primary information needed to permit the operators to take specified manual actions for which there are no automatic controls and that are required for safety systems to perform their safety function for design-basis events. Due to the passive nature of the AP600 and the specific systems design, there are no specific, preplanned, manual actions of this nature. Thus, there are no Type A variables for AP600.

Type B variables are defined in SSAR Section 7.5.3.2, Table 7.5.5, and SSAR Section 18.12.2. They are variables that provide information to the MCR operators to assess the process of accomplishing or maintaining the six CSF in the ERGs. Table 7.5-5 lists the Type B variables for AP600. Table 18.12.2.1 (Revision 9) lists the minimum inventory and indicates if the instrument is based upon a Type B or Type C variable. The six CFS status trees of the ERGs (AF-0.1 through AF-0.6) were reviewed to ensure that all Type B variables needed by the operators were included in Tables 7.5-5 and 18.12.2-1. RG 1.97, Table 3, provides a list of PWR Type B variables, which was compared to the Type B variables of AP600. The staff also compared Table 7.5-5 with Table 18.12.2-1 to ensure that all identified Category 1 Type B variables had been transferred over to the minimum inventory list. With the exception of the items noted below, no discrepancies were identified.

The staff noted that Westinghouse had included a display for each of the Type B variables in SSAR Table 18.12.2-1, but had not included any alarms. The staff indicated that it is not appropriate to exclude alarms, and that alarms corresponding to the parameter values in the CSF status trees would be appropriate. Westinghouse revised the table (Revision 13) to include appropriate alarms. Further, the following variables appeared to be missing from SSAR Tables 7.5-5 or 18.12.2-1.

- ERG AF-0.1 contains power range power percent, intermediate range startup rate (SUR), and source range SUR. RG 1.97 calls for monitoring neutron flux from 1E-6 percent to 100 percent. The tables in Chapters 7 and 18 only mentioned neutron flux and did not address the range or include SUR. Westinghouse clarified that Table 7.5-1 contains the ranges for all instruments and that only the instrument name is carried forward to the other tables. Table 7.5-1 indicates that neutron flux will be monitored from 1E-6 to 200 percent power. Westinghouse states that SUR is calculated from the same neutron flux instrument and also modified Table 18.12.2-1 to include startup rate. This is acceptable.

- AF-0.3 contains SG narrow range level, SG pressure, and total feedwater flow. These are not in the tables in SSAR Sections 7.5 or 18.2. Westinghouse stated that per the SSAR analyses, the design-basis cases only require passive residual heat removal (PRHR) as a heat sink and not the SGs. AP600 is different from current generation PWRs in that it uses PRHR in place of Auxiliary Feed Water (AFW) and the SGs for the safety-related heat sink. Thus, the SGs and SG parameters are not required variables to indicate whether the heat sink CSF is satisfied; and, as a result, do not have to be classified as Type B variables or included on the minimum inventory. Thus, for AP600 the SG parameters are classified as Category D variables. It is worthy of note that the SG parameters are in Table 7.5-1 as safety-related parameters, are included in the ITAAC, and hence are included on the QDPS. This is acceptable.

  Additionally, SG wide range level, appears to have been classified as a Category 2 variable, in the SSAR Section 7.5, and not Category 1 as recommended in RG 1.97, without adequate justification. The staff also noted that only one channel is required per SG rather than the usual two per SG. The

staff also asked if the indication channel is fed from the trip channel. Westinghouse stated that the AP600 design has no Category D1 variables, which is consistent with the general statement on page 3 of RG 1.97. Table 7.5-2 of the AP600 SSAR also shows no Category D1 variables.

Westinghouse further stated that this treatment of SG parameters was previously accepted by NRC for Vogtle and South Texas. In the AP600, the SGs are less important than at these two plants because, for the AP600, the PRHR is used as a safety-related heat sink instead of the AFW system and the SGs. Nonetheless, both narrow range (NR) and wide range (WR) SG level are qualified as PAMS instruments for harsh environments per SSAR Section 3.11. Westinghouse also stated that, per the SSAR, the indication channel is fed from the same instrument as the trip channel. The staff's question concerning SG wide range level being classified as a Category 2 variable rather than as Category 1 is being addressed by Westinghouse in their response to Chapter 7, "Instrumentation and Controls," issues.

- AF-0.4 contains RCS cooldown rate and $T_C$ compared to a limit, based on RCS pressure. The tables in SSAR Sections 7.5 and 18.2 did not contain any provision for determining the rate or the comparison to the varying temperature/pressure limit. These parameters can very easily be developed into integrated displays with the computer-based instrumentation system of the AP600. Westinghouse added these two parameters to Table 18.12.2-1. This is acceptable.

- AF-0.5 lists containment radiation level. This variable is not included in Table 7.5-5, but is listed in Table 18.12.2-1. Westinghouse indicated that it is included in Table 7.5-6 under RCS boundary, which is acceptable.

- AF-0.6 contains a requirement to monitor pressurizer (PZR) level and PZR level behavior. Both tables contain PZR level, but neither had any mention of instrumentation related to the time-dependent behavior of PZR level. Westinghouse added PZR level trend to Table 18.12.2-1. This is acceptable.

- RG 1.97 lists containment isolation valve (CIV) position. However, SSAR Table 7.5-5 inappropriately limits CIV position to remotely operated CIVs. SSAR Table 18.12.2-1 does not limit its coverage to remotely operated CIVs. Westinghouse stated that the AP600 intent is to only address remotely operated CIVs in both tables, and modified Table 18.12.2-1 to say that. Further, they justified this position by stating that all manual CIVs would be normally locked, under administrative controls, and would have local VPI as determined via the OER.

In summary, the coverage in the SSAR is satisfactory with respect to the Type B variables.

Type C variables are defined in SSAR Section 7.5.3.3, Table 7.5-6, and SSAR Section 18.12.2. They are variables that provide the control room operators with information to monitor the potential for breach or actual gross breach of (1) incore fuel

cladding, (2) RCS boundary, or (3) containment boundary. Type C variables are listed in SSAR Table 7.5-6. SSAR Table 18.12.2-1 (Revision 9) lists the minimum inventory and has a column that identifies if the instrument was based upon a Type B or Type C variable. The staff reviewed the six CSF status trees of the ERGs (AF-0.1 through AF-0.6) to ensure that all Type C variables needed by the operators were included in SSAR Tables 7.5-5 and 18.12.2-1. RG 1.97, Table 3 provides a list of PWR Type C variables, which the staff compared to the Type C variables of the AP600 design. Also the staff compared SSAR Table 7.5-6 with SSAR Table 18.12.2-1 to ensure that all identified Category 1, Type C variables had been transferred over to the minimum inventory list.

As with the Type B variables, it was noted that, for each of the Type C variables, Westinghouse had included a display in SSAR Table 18.12.2-1, but included no alarms. It did not appear appropriate to exclude alarms. Westinghouse thus revised Table 18.12.2-1 in SSAR Revision 14 to include appropriate alarms.

The only additional discrepancy noted for Type C variables (beyond those noted for Type B variables above) is based on RG 1.97, which calls for a measure of the radioactivity concentration or radiation level in the circulating primary coolant. This was not contained in either SSAR Table 7.5-5 or 18.12.2-1. This was being addressed by Westinghouse in their response to Chapter 7, "Instrumentation and Controls," issues.

(2) dedicated controls for manual safety-related system actuation (reactor trip, turbine trip, and engineered safety feature actuation)

SSAR Section 18.12.2 states that the selection criteria for AP600 minimum inventory include dedicated, fixed position controls to manually initiate system-level actuation signals for the safety-related systems and components that are used to achieve CSFs. The staff reviewed SSAR Table 3.2-3 to determine the list of safety-related systems. This was then compared with the manual actuation controls listed in SSAR Table 18.12.2-1 for the minimum inventory. One safety-related system was noted to be missing, the MCR emergency habitability system (VES). VES is used to ensure that the control room operators survive in the event that normal control room ventilation is unavailable and thus indirectly addresses all six CSFs. The staff determined that Westinghouse should address what additional dedicated controls need to be added for this system.

Westinghouse subsequently added a manual actuation control for the MCR VES to Table 18.12.2-1. This is acceptable.

(3) controls, displays, and alarms required to perform critical manual actions as identified from the PRA analysis

Westinghouse noted in SSAR Section 18.12.2 that fixed position controls, displays and alarms to support the critical actions will be included in the minimum inventory. SSAR Section 18.7 references WCAP-14651 (Revision 2), "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," Revision 2, which notes that there are no critical actions for AP600. The staff evaluation of SSAR

Section 18.7 and WCAP-14651 discusses the issue of the selection of critical human actions based upon the AP600 PRA and notes that the threshold criteria for selection is high. However, because Westinghouse also defines risk-important tasks and uses them for other portions of the control room design (where critical actions were intended to be used), the staff has accepted the Westinghouse position.

It should be noted that it is the staff's understanding that, although Westinghouse has not identified any critical human actions based on preliminary results from PRA studies completed in 1996, as PRA studies are completed and/or updated, critical human actions may be identified and thus used as input to the minimum inventory. It should also be noted that Westinghouse's approach to human system design uses input from task analyses (e.g., see Figures 18.5.2, and Figure 1-1 WCAP-14651) and, critical human actions and risk-important tasks derived from PRA are used as input to task analyses. Therefore, because task analyses are used to verify the minimum inventory (SSAR Revision 19, page 18.12.1) both critical human actions and risk-important task are used in determining the AP600 minimum inventory. Thus, the staff believes that all operator actions that are determined to be significant contributors to plant risk by PRA analyses are addressed by the AP600 minimum inventory.

Although the staff has accepted the Westinghouse criteria for defining critical human actions and risk-important tasks, the high threshold used by Westinghouse to define critical action selection has eliminated any entries to the minimum inventory that may be judged important based on operating experience and engineering judgement. In particular, the staff considers the manual actuation of ADS a very important action, and notes that it is also classified as a risk-important task by Westinghouse. Manual actuation of the ADS is based on level in the CMT reaching 67 percent and the ADS not actuating automatically. Consequently, CMT level is a key parameter needed to judge the necessity for an operator to manually actuate ADS. The staff thus believed that CMT level should be included in the minimum inventory list. Westinghouse subsequently added CMT level to Table 18.12.2-1. This is acceptable.

(4) alarms provided for operator use in performing safety functions to respond to design-basis events for which there is no automatically-actuated safety function

As noted in the discussion under (1) above, due to the passive nature of the AP600 and the specific systems design, there are no preplanned, manual actions required for safety systems to perform their safety function for design-basis events. Thus, because there are no operator actions of the type noted in (1), there are no alarms required to alert the operators to take this type of action.

(5) CDAs necessary to maintain the CSF and safe-shutdown conditions

With regard to the CDAs necessary to maintain the CSFs, these would be the same ones identified in (1) above, based upon the CSF Status Trees of the ERGs. Thus, the same discrepancies identified in (1) pertain here also. These were all corrected by Westinghouse with SSAR revisions.

With regard to CDAs to maintain the CSFs and safe-shutdown conditions, the discussions under (2), (3), and (4) above indicate that Westinghouse had not included

CDAs in the minimum inventory. If one were to go beyond single failure and use the ERG functional restoration guidelines, which are entered from the CSF status trees, then additional controls would be obtained. However, this would add many more dedicated CDAs than appears appropriate in the highly computerized AP600 control room. If required, this added number of fixed controls, may actually be counterproductive to safety, due to creating requirements that are not appropriately integrated into the overall human factors engineering of the control room.

The Westinghouse ERGs also define a CSF associated with shutdown conditions. While the Westinghouse criterion refers to safe-shutdown, the staff considers this criterion applicable to all shutdown conditions. With regard to the controls, displays, and alarms necessary to maintain shutdown conditions, the staff reviewed the ERG shutdown safety status tree to determine if all required items to implement the Tree were on the minimum inventory list. The following items from the shutdown safety status tree were not in the minimum inventory list:

- RCS hot leg level
- indication of RNS in service
- alarm for neutron flux doubling
- display to tell if RCS pressure/temperature meet the cold overpressure limits
- alarm/indication that RCS temperature has changed by more than 5 degrees in the last 10 minutes

In addition, the ability to control the normal RNS appears to be essential to maintain the plant in cold shutdown. RNS is used to assist in achieving the CSF of core cooling, heat sink, and RCS inventory in cold shutdown conditions. The staff requested Westinghouse to define the minimum RNS CDAs that should be part of the minimum inventory.

In response to this item, Westinghouse added the following indications to Table 18.12.2-1:

- RCS hot leg level
- Neutron flux doubling
- Display to tell if RCS pressure/temperature meet the cold overpressure limits
- Indication that RCS temperature has changed by more than 5 degrees in the last 10 minutes

Westinghouse further stated that, as described in Sections 6.3 and 7.4 of the SSAR and in the shutdown evaluation report, RNS is not required for the safety case evaluation of safe-shutdown. For the safety case, the AP600 uses the IRWST, which has both automatic and manual actuation. The manual actuation and related indications are included in the minimum inventory. Thus, RNS CDAs are not "necessary" to maintain the CSFs or the safe-shutdown conditions. Hence, they are not required to be in the minimum inventory per Criterion 5. This is acceptable.

With respect to alarms on the minimum inventory list, Westinghouse revised the SSAR to include alarms (alerts) in Table 18.12.2-1 and to include appropriate alarms (alerts) in the minimum inventory and on the QDPS. The staff noted that, when the design is finalized,

the alarm acknowledgment scheme should be coordinated between the QDPS and the main alarm system so that operators are not required to acknowledge the same alarm in two different places.

Based on this information, Open Item 18.12.3-1 is closed and the minimum inventory criterion is satisfied.

Criterion 3: Consideration of Operator Tasks

*Criterion:* An inventory of fixed-position controls, displays, and alarms necessary to permit execution of the operator tasks to place and maintain the plant in a safe-shutdown condition should be identified.

*Evaluation:*

DSER Evaluation

The staff could not complete its evaluation of this criterion because Westinghouse had not defined a minimum inventory for the AP600 design. Westinghouse should describe how an inventory of fixed-position controls, displays, and alarms necessary to permit execution of the operator tasks to place and maintain the plant in a safe-shutdown condition will be identified. This was part of Open Item 18.12.3-1.

FSER Evaluation

SSAR (Revision 23) Section 18.12, "Inventory," and Section 7.4.3, "Safe Shutdown from Outside the Main Control Room," discuss the development of the minimum inventory of CDAs needed to place and maintain the plant in a safe-shutdown condition from either the MCR or the remote shutdown workstation (RSW). Westinghouse has provided a minimum inventory of fixed position CDAs for the MCR. The characteristics for selection of minimum inventory items established by Westinghouse and satisfactorily reviewed under subitems 1 and 2 above, address operator actions or tasks needed to maintain CSF and safe-shutdown conditions. SSAR Section 18.12.3 states that the CDAs of Table 18.12.2-1 are also retrievable from the RSW.

Based on this information, the minimum inventory criterion is satisfied.

Criterion 4: HFE Input

*Criterion:* The inventory contains a list of key minimum displays, controls, and alarms necessary to carry out operator actions associated with the ERGs. The applicant will also need to identify and further define additional detailed characteristics of these controls, displays, and alarms (e.g., ranges, scales, physical dimensions, and actual information presentation) during the detailed task analysis and HSI design efforts. The HFE design process should provide adequate assurance that these detailed characteristics will be defined and implemented.

*Evaluation:*

DSER Evaluation

The staff could not complete its evaluation of this criterion because Westinghouse had not defined a minimum inventory for the AP600 design. Westinghouse should describe how additional detailed characteristics of these controls, displays, and alarms (e.g., ranges, scales, physical dimensions, and actual information presentation) will be identified, defined, and implemented. This was part of Open Item 18.12.3-1.

FSER Evaluation

The commitments provided in SSAR (Revision 23), Sections 18.5, 18.8, 18.11 that address Task Analysis, HSI Design, and HSI design test program (including verification and validation) provide an acceptable assurance that these additional detailed characteristics of the controls, displays, and alarms will be defined, designed, tested, and implemented. The detailed review of these sections of the SSAR is provided elsewhere in this document.

Based on this information, the minimum inventory criterion is satisfied.

Criterion 5: Task Analysis Input Into Minimum Inventory

(DSER Section 18.5, Element 4, Task Analysis, Criterion 6)

*Criterion:* The task analysis results should be used to define a minimum inventory of controls, displays, and alarms necessary to perform crew tasks based upon both task and I&C requirements.

*Evaluation:*

DSER Evaluation

This item was addressed under 14401 (Revision 3) Minimum Inventory, in Section 18.12 of this report. Westinghouse should describe how the task analysis will define a minimum inventory of alarms, displays, and controls necessary to perform crew tasks. This was addressed under Open Item 18.12.3-1.

FSER Evaluation

Westinghouse defined a method and criteria that will be used to define the minimum inventory. These are delineated in SSAR Section 18.12 and have been previously reviewed. The method does not directly use the task analyses, but provides an acceptable alternative that uses a combination of RG 1.97, the design features of the AP600, and the emergency response guidelines.

SSAR Section 18.5.2.1, "Function-Based Task Analyses (FBTAs), indicates that the FBTAs are used as a completeness check on the availability of needed indications, parameters, and controls. The SSAR also indicates that the OSAs will provide information on the inventory of

alarms, controls, and parameters needed to perform sequences selected for analysis, which include those addressed in the discussion of Task Analysis Criterion 1: Scope, discussed in Section 18.5.

Based on this information, the minimum inventory criterion is satisfied.

Criterion 6: Development of the Remote Work Station Minimum Inventory

(SSAR, Section 7.4.3.1.1, Remote Shutdown Workstation)

*Criterion:* In conjunction with the effort by Westinghouse to develop a MCR minimum inventory of CDAs for use in the mitigation of transient and accidents, the staff requested that Westinghouse provide a list of CDAs that would be available at the RSW for use in establishing and maintaining shutdown conditions in the event the MCR was uninhabitable. The staff does not consider it necessary that any RSW CDAs be fixed-position. However, a minimum inventory of CDAs accessible from the RSW should be well described in the SSAR.

*Evaluation:*

DSER Evaluation

Not Reviewed in the DSER.

FSER Evaluation

The issue was discussed during a number of conference calls between the staff and Westinghouse, dated September 12, 1995; April 17, 1996; and July 11, 1996. To address the staff's request, Westinghouse submitted SSAR (Revision 9), Section 18.12, dated August 9, 1996, "Displays, Alarms, and Controls," subsequently revised to SSAR Section 18.12, "Inventory," (Revision 14); Section 7.4 (Revision 5), "Systems Required for Safe Shutdown," dated February 29, 1996; and Section 7.5 (Revision 8), "Safety-Related Display Information," dated June 19, 1996. These documents provided descriptions of the systems required for safe-shutdown, a table of post accident monitoring system information, and a summary of RG 1.97 variables by type and category. However, the staff could not complete its evaluation of this issue because Westinghouse had not defined the list of CDAs that would be available at the RSW.

In SSAR (Revision 23) Section 7.4.3.1.1, Remote Shutdown Workstation, and Section 18.12.3, "Remote Shutdown Workstation Displays, Alarms, and Controls," Westinghouse indicated that the same CDAs contained in the MCR workstations will be retrievable from the RSW. This acceptably addresses the staff's questions related to establishing a minimum inventory of CDAs for the RSW.

Based on this information, the minimum inventory criterion is satisfied.

18.12.4 Conclusions

Westinghouse defined a minimum inventory of controls, displays, and alarms for the AP600 design that satisfies the staff's criteria.

18.13 Summary and Conclusions

The overall purpose of the AP600 HFE review is to ensure the following:

- Westinghouse has integrated HFE into plant development and design
- Westinghouse has provided HSIs that make possible safe, efficient, and reliable performance of operation, maintenance, test, inspection, and surveillance tasks
- The HSI reflects "state-of-the-art human factors principles" [10 CFR 50.34(f)(2)(iii), as required by 10 CFR 52.47(a)(1)(ii)] and satisfies all specific regulatory requirements as stated in Title 10 of the Code of Federal Regulations.

In addition, the review included Westinghouse's proposed resolutions of unresolved safety issues, generic safety issues, and related human factors considerations addressed in Chapters 6, 7, 9, 13, 14, 16, 19, and 20 of the SSAR.

In its DSER evaluation, the staff identified open items concerning detailed aspects of Westinghouse's human factors engineering. These items were acceptably addressed by Westinghouse during the staff's subsequent review.

In conclusion, the Westinghouse HFE SSAR and supporting materials reviewed describe a comprehensive HFE program that is acceptable and consistent with the staff's review criteria.

18.14 Tier 2* Information:

As a result of its review of the AP600 HFE program, the staff has determined that the following information in Chapter 18 of the AP600 SSAR must be designated as Tier 2* information in the AP600 design control document. The rationale for selecting this information is provided in parentheses. This information is similar to Tier 2* HFE information for the evolutionary plants and, as with the evolutionary design certifications, the Tier 2* information identified herein is not subject to expire at first full power. Furthermore, any proposed change to Tier 2* information, by a COL applicant or licensee, will require NRC approval prior to implementation.

SSAR Sections:

18.2.1.3 Applicable Facilities (assures scope of HFE Program)

18.2.1.4 Applicable Human System Interfaces (assures scope of HFE Program)

18.2.1.5 Applicable Plant Personnel (assures scope of HFE Program)

18.2.1.6 Technical Basis (assures that HFE Program will be developed in accordance with specified standards, guidelines, an accepted professional practices)

18.2.2.1 Responsibility (assures preservation of HFE Program Design Team integrity)

18.2.2.3 Composition [first paragraph and listing of design team disciplines only] (assures preservation of design team multidisciplinary composition)

18.2.3.1 General Process and Procedures [last paragraph of Design Review of Human Factors Engineering Products only] (assures commitment to design issues tracking system implementation)

18.2 Human Factors Engineering Program Management, Figure 18.2-1, Human System Interface (HSI) Design Team Process (assures commitment to conduct of HFE Process)

18.5.1 Task Analysis Scope (assures commitment to Task Analysis scope and process, implementation of which will be verified by ITAAC)

18.5.2 Task Analysis Implementation Plan (assures commitment to scope and methodology for Task Analysis Plan, implementation of which will be verified by ITAAC)

18.7 Integration of Human Reliability Analysis with Human Factors Engineering (assures commitment to details of HRA Integration are preserved, implementation of which will be verified by ITAAC)

18.8.2 Safety Parameter Display System (SPDS) through 18.8.2.7, inclusive (assures function of SPDS will be incorporated as part of overall HSI program, implementation of which will be verified by ITAAC)

18.8.3.2 Main Control Area Mission and Major Tasks (assures commitment to MCR mission, conduct of operation, and major components of MCR covered by HFE Program are preserved)

18.8.3.4 Remote Shutdown Workstation Mission and Major Tasks implemented (assures commitment to RSW mission, conduct of operation, and major components of RSW covered by HFE Program are preserved)

18.8.3.5 Technical Support Center Mission and Major Tasks (assures commitment to TSC mission, conduct of operation, and major components of TSC covered by HFE Program are preserved)

18.11 Human System Interface Design Test Program (assures commitment to scope and conduct of HSI Test Program are preserved, implementation of which will be verified by ITAAC)

18.12 Inventory [through 18.12.3, Remote Shutdown Workstation Displays, Alarms, and Controls] (assures commitment to scope and development of Minimum Inventory is preserved for future iterations of the AP600 PRA)

SSAR Supporting Documents:

WCAP- 14396 (Rev.2)
Man-In-The-Loop Test Plan Description (principal design document supporting 18.11)

WCAP- 14401 (Rev.3)
Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan (principal design document supporting 18.11)

WCAP- 14651 (Rev.2)
Integration of Human Reliability Analysis With Human Factors Engineering Design Implementation Plan (principal design document supporting 18.7)

WCAP-14695 (Rev.0)
Description of the Westinghouse Operator Decision-Making Model and Function-Based Task Analysis Methodology (principal design document supporting 18.5.1)

WCAP- 14701 (Rev.1)
Methodology and Results of Defining Evaluation Issues for the AP600 Human System Interface Design Test Program (principal design document supporting 18.2, 18.8.2)

WCAP- 14822, (Rev.0)
AP600 Quality Assurance Procedures Supporting NRC Review of AP600 SSAR Sections 18.2 and 18.8 (principal design document supporting 18.2, 18.8.)

Table 18.1-1 Level of HFE Review

| REVIEW TOPIC AND FSER SECTION | LEVEL OF DETAIL |
|---|---|
| Element 1 - HFE Program Management (18.2) | Complete Element |
| Element 2 - Operating Experience Review (18.3) | Complete Element |
| Element 3 - Functional Requirements Analysis and Allocation (18.4) | Complete Element (Note 1) |
| Element 4 - Task Analysis (18.5) | Implementation Plan |
| Element 5 - Staffing (18.6) | COL Item (Note 2) |
| Element 6 - Human Reliability Analysis (18.7) | Implementation Plan |
| Element 7 - Human-System Interface Design (18.8) | Implementation Plan (Note 3) |
| Element 8 - Procedure Development (18.9) | COL Item (Note 2) |
| Element 9 - Training Program Development (18.10) | COL Item (Note 2) |
| Element 10 -Human Factors Verification & Validation (18.11) | Programmatic |
| - Minimum Inventory (18.12) | Complete |

Notes:

1. At the time of the DSER, this element was reviewed at the implementation plan level. As a result of discussions between Westinghouse and the staff and work performed by Westinghouse following the DSER, it was agreed to evaluate this element at a complete element level.

2. At the time of the DSER, this element was reviewed at the implementation plan level. From discussion between Westinghouse and the staff following the DSER, it was agreed that this element will be addressed by the COL.

3. Safety parameter display system (SPDS) requirements were reviewed as part of HSI design.

Table 18.3-1 Summary of Review of AP600 Applicable Issues from Westinghouse Draft OER Report (WCAP-14645)

| | Total Items Reviewed | Acceptably Addressed | Not Acceptably Addressed in Draft WCAP-14645* |
|---|---|---|---|
| USI/GSI | 20 | 15 | 5 |
| HF Gen Issues | 7 | 7 | |
| TMI Items | 27 | 22 | 4 |
| GLs/INs | 5 | 5 | |
| BNL OER Report | 43 | 40 | 3 |
| HSI Tech | 38 | 30 | 9 |
| Operator Interviews | 8 References | 8 | |
| AEOD Items | 13 | 13 | |
| Totals | 161 | 140 | 21 |

Notes:

1. All items of the draft WCAP-14645 were reviewed with the exception of the items in the BNL OER Report. In this category about 50 percent of the items were reviewed.

2. The "Acceptably Addressed" column includes items classified as N/A by Westinghouse, excluded by NRC and Westinghouse in conference call, placed in the tracking system by Westinghouse, and those with adequately described activities to address the HFE concern associated with the item. There were 18 items that were either N/A by Westinghouse or excluded per the NRC/Westinghouse call; three items entered into the tracking system; and 119 with adequately described activities.

3. The one item added to the criterion for this element beyond those listed in the Appendix was the TMI item I.C.5, which Westinghouse satisfactorily addressed in SSAR Sections 1.9.3 [item (3)(i)]; 13.5; 18.9; and WCAP-14690 (Revision 1).

*These items were acceptably addressed in subsequent revisions to WCAP-14645.

Table 18.4-1 Relationship of NUREG-0711 Criteria, DSER Open Items, and New Open Items

| NUREG-0711 Criterion | DSER Status | New Item/Criterion |
|---|---|---|
| General Criterion 1 | Satisfied (Reopened)* | |
| General Criterion 2 | Open Item 18.4.3.1-1 | 1 |
| Fun. Req. Anal. 1 | Open Item 18.4.3.2-1 | 2 |
| Fun. Req. Anal. 2 | Open Item 18.4.3.2-2 | 2 |
| Fun. Req. Anal. 3 | Open Item 18.4.3.2-3 | 2 |
| Fun. Req. Anal. 4 | Open Item 18.4.3.2-4 | 2 |
| Fun. Req. Anal. 5 | Satisfied | Not Applicable |
| Fun. Req. Anal. 6 | Open Item 18.4.3.2-5 | 2 |
| Fun. Req. Anal. 7 | Open Item 18.4.3.2-6 | 2 |
| Fun. Req. Anal. 8 | Open Item 18.4.3.2-7 | 2 |
| Fun. Allocation 1 | Open Item 18.4.3.3-1 | 3 |
| Fun. Allocation 2 | Open Item 18.4.3.3-2 | 3 |
| Fun. Allocation 3 | Open Item 18.4.3.3-3 | 3 |
| Fun. Allocation 4 | Satisfied (Reopened)* | 3 |
| Fun. Allocation 5 | Open Item 18.4.3.3-4 | 4 |
| Fun. Allocation 6 | Open Item 18.4.3.3-5 | 3 |
| Fun. Allocation 7 | Open Item 18.4.3.3-6 | 3 |
| Fun. Allocation 8 | Open Item 18.4.3.3-7 | 4 |
| Fun. Allocation 9 | Satisfied (Reopened)* | 4 |
| Fun. Allocation 10 | Satisfied (Reopened)* | 3 |

*Note: On the basis of information obtained following the publication of the DSER, several NUREG-0711 criteria that had been identified as "Satisfied" were reopened and their substance was incorporated into the new items.

## 19 SEVERE ACCIDENTS

Background

Federal regulations for the design, construction, licensing, and operation of commercial nuclear power plants are defined in Chapter 1 of Title 10 of the Code of Federal Regulations (CFR). The U.S. Nuclear Regulatory Commission (NRC) evaluated the design against these regulations, as documented in the various chapters of this report. Compliance with the Commission's regulations ensures adequate protection of the public health and safety regarding operating of a nuclear power plant. In previous applications, the final safety analysis report demonstrated compliance with these regulations and set forth the design basis of the plant. The Commission has developed guidance and goals for resolving safety issues related to reactor accidents more severe than design-basis accidents. These "severe accidents" are those in which substantial damage is done to the reactor core whether or not there are serious offsite consequences.

Following the accident at the Three Mile Island Nuclear Plant, Unit 2, in 1979, when it was recognized that severe accidents needed further attention, the NRC evaluated, generically, the capability of existing plants to tolerate a severe accident. It was found that the design-basis approach contained significant safety margins for the analyzed events. These margins permitted operating plants to accommodate a large spectrum of severe accidents. Based on this information, the Commission, in the Severe Accident Policy Statement, concluded that existing plants posed no undue risk to public health and safety, and that no basis existed for immediate action on generic rulemaking or other regulatory changes for these plants because of severe accident risk. For operating plants in the long term, the NRC developed the "Integration Plan for Closure of Severe Accident Issues" (SECY-88-147), in which the NRC identified the following necessary elements for closure of severe accidents:

- performance of an individual plant examination
- assessment of generic containment performance improvements (CPI)
- improved plant operations
- a severe accident research program
- an external events program
- an accident management program

Progress continues in these areas for operating plants.

The Commission expects that new designs, like the AP600, will achieve a higher standard of severe accident safety performance than previous designs. In an effort to provide this additional level of safety in the design of advanced nuclear power plants, the NRC has developed guidance and goals for which designers should strive in accommodating events that are beyond what was previously known as the design basis of the plant. The nuclear industry, through the Electric Power Research Institute (EPRI), has also recognized the need to establish

a higher standard for advanced designs. The EPRI has developed additional standards that designers should conform to for severe accidents.

For advanced nuclear power plants, including both the evolutionary and passive designs, the staff concluded that vendors should address severe accidents during the design stage. This will allow the designers to take full advantage of the insights gained from such input as probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase has been demonstrated to be much more cost effective than modifying existing plants.

Regulatory Guidance

The NRC has issued guidance for addressing severe accidents. This guidance is found in the following documents:

- NRC Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants (*Federal Register* (50 FR 32138) dated August 8, 1985)
- NRC Policy Statement on Safety Goals for the Operations of Nuclear Power Plants (*Federal Register* (51 FR 28044) dated August 4, 1986)
- NRC Policy Statement on Nuclear Power Plant Standardization (*Federal Register* (52 FR 34844) dated September 15, 1987)
- 10 CFR Part 52, "Early Site Permits; Standard Design Certification; and Combined Licenses for Nuclear Power Plants"
- SECY-90-016 "Evolutionary Light Water Reactor Certification Issues and Their Relationship to Current Regulatory Requirements," and the corresponding staff requirements memorandum (SRM) dated June 26, 1990
- SECY-93-087 "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," and the corresponding SRM dated July 21, 1993
- SECY-96-128 "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design," and the corresponding SRM dated January 15, 1997
- SECY-97-044 "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design," and the corresponding SRM dated June 30, 1997.

Whereas, the first three documents provide guidance as to the appropriate course for addressing severe accidents, 10 CFR Part 52 contains general requirements for addressing severe accidents, and the SRMs relating to SECY-90-016, SECY-93-087, SECY-96-128, and

SECY-97-044 give Commission-approved positions for implementing features in new designs for preventing severe accidents and mitigating their effects.

Severe Accident Policy Statement

The Commission issued the "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants," on August 8, 1985. The focus of severe accident issues in this policy statement was prompted by the NRC's judgment that accidents of this class, which are beyond the traditional design-basis events, constitute the major remaining risk to the public associated with radioactive releases from nuclear power plant accidents. A fundamental objective of the Commission's severe accident policy was to take all reasonable steps to reduce the chances that a severe accident involving substantial damage to the reactor core will occur and to mitigate the consequences of such an accident, should one occur. This statement described the policy that the Commission intended to use to resolve safety issues related to reactor accidents more severe than design-basis accidents (DBAs). The main focus of the statement was on the criteria and procedures the Commission intended to use to certify new designs for nuclear power plants. Regarding the decision process for certifying a new standard plant design, an approach the Commission strongly encouraged for future plants, the policy statement affirmed the Commission's belief that a new design for a nuclear power plant could be shown to be acceptable for severe accident concerns if it met the following criteria and procedural requirements:

- demonstration of compliance with the procedural requirements and criteria of the current Commission regulations, including the Three Mile Island (TMI) requirements for new plants as reflected in the 10 CFR 50.34(f)

- demonstration of technical resolution of all applicable unresolved safety issues (USI) and the medium- and high-priority generic safety issues (GI), including a special focus on assuring the reliability of decay heat removal (DHR) systems and the reliability of both ac and dc electrical supply systems

- completion of a probabilistic risk assessment (PRA) and consideration of the severe accident vulnerabilities the PRA exposes along with the insights that it may add to providing assurance of no undue risk to public health and safety

- completion of a staff review of the design with a conclusion of safety acceptability using an approach that stresses deterministic engineering analyses and judgment complemented by PRA

The Commission believed that an adequate basis existed from which to establish an appropriate set of criteria. This belief was supported by the current operating reactor experience, ongoing severe accident research, and insights from a variety of risk analyses. The Commission recognized the need to strike a balance between accident prevention and consequence mitigation and in doing so expected that vendors engaged in designing new standard plants will achieve a higher standard of severe accident safety performance than they achieved with their previous designs.

Safety Goals Policy Statement

The Commission issued the "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants" on August 4, 1986. This policy statement focused on the risks to the public from nuclear power plant operations with the objective of establishing goals that broadly define an acceptable level of radiological risk that might be imposed on the public as a result of nuclear power plant operation. These are the risks from release of radioactive material from the reactor to the environment from normal operations as well as from accidents. The Commission established two qualitative safety goals that are supported by two quantitative objectives. The qualitative safety goals follow:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The following quantitative objectives were to be used in determining achievement of the above safety goals:

- The risk to an average individual in the vicinity of a nuclear power plant of a prompt fatality that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

This statement of NRC safety policy expresses the Commission's views on the level of risks to public health and safety that the industry should strive for in its nuclear power plants. The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize such features as the containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy. The Commission approves the use of the qualitative safety goals, including use of the quantitative health effects objectives, in the regulatory decisionmaking process.

Standardization Policy Statement

The Commission issued the "Policy Statement on Nuclear Power Plant Standardization" on September 15, 1987. The policy statement encouraged the use of standard plant designs and contained information concerning the certification of plant designs that are essentially complete in scope and level of detail. The intent of these actions was to improve the licensing process and to reduce the complexity and uncertainty in the regulatory process for standardized plants. In relation to severe accidents, the policy statement expected applicants for a design

certification to address the four licensing criteria for new plant designs as given in the Commission's Severe Accident Policy Statement.

10 CFR Part 52

The Commission issued 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," on April 18, 1989. This rule provides for issuing early site permits, standard design certifications, and combined licenses with conditions for nuclear power reactors. It states the review procedures and licensing requirements for applications for these new licenses and certifications, and was intended to achieve the early resolution of licensing issues and to enhance the safety and reliability of nuclear power plants. Relating to severe accidents, 10 CFR Part 52 codified some of the guidance in the Severe Accident Policy Statement and the Standardization Policy Statement. Specifically, 10 CFR 52.47 requires an application for design certification to include the following:

- demonstrate compliance with any technically relevant portions of the TMI requirements given in 10 CFR 50.34(f)
- propose technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues which are identified in the version of NUREG-0933 current on the date 6 months prior to application and which are technically relevant to the design
- contain a design-specific PRA

SECY-90-016

On January 12, 1990, the NRC staff issued SECY-90-016 which requested Commission approval for the staff's recommendations concerning proposed departures from current regulations for the evolutionary light water reactors (LWR). The issues in SECY-90-016 were significant to reactor safety and fundamental to the NRC decision on the acceptability of evolutionary LWR designs. The positions in SECY-90-016 were developed as a result of the following activities:

- NRC's reviews of current-generation reactor designs and evolutionary LWRs
- consideration of operating experience, including the TMI-2 accident
- results of PRAs of current-generation reactor designs and the evolutionary LWRs
- early efforts conducted in support of severe accident rulemaking
- research to address previously identified safety issues.

The Commission approved some of the staff positions stated in SECY-90-016 and provided additional guidance regarding others in an SRM dated June 26, 1990.

SECY-93-087

On April 2, 1993, the NRC staff issued SECY-93-087 which sought Commission approval for the staff's positions pertaining to evolutionary and passive LWR design certification policy

issues. This paper was an evolution of SECY-90-016. Preventive feature issues addressed in SECY-93-087 relating to the AP600 include the following:

- anticipated transient without scram (ATWS)
- mid-loop operation
- station blackout
- fire protection
- intersystem loss-of-coolant accident

Mitigative feature issues addressed in SECY-93-087 relating to the AP600 include the following:

- hydrogen control
- core debris coolability
- high-pressure core melt ejection
- containment performance
- dedicated containment vent penetration
- equipment survivability
- containment bypass potential resulting from steam generator tube ruptures

The Commission approved some of the staff positions from SECY-93-087 and provided additional guidance regarding others in an SRM dated July 21, 1993.

SECY-96-128

On June 12, 1996, the NRC staff issued SECY-96-128 which sought Commission approval for the staff's position pertaining to the AP600 reactor design. The issues involving severe accidents in this paper include the following:

- prevention and mitigation of severe accidents
- external reactor vessel cooling

The Commission provided additional guidance concerning prevention and mitigation of severe accidents, and approved the staff's position concerning external reactor vessel cooling in an SRM dated January 15, 1997.

SECY-97-044

On February 18, 1997, the NRC staff issued SECY-97-044 which provided the Commission with additional information regarding prevention and mitigation of severe accidents. This paper was in response to the Commission's SRM dated January 15, 1997. Specifically, this paper provided additional information regarding the type of non-safety-related system that would achieve an appropriate balance between prevention and mitigation of severe accidents for the AP600 reactor design. The Commission approved the staff's position in an SRM dated June 30, 1997.

Severe Accident Resolution

The basis for resolution of severe accident issues for the AP600 is 10 CFR Part 52, and SECY-93-087, SECY-96-128, and SECY-97-044, as approved by the Commission. In 10 CFR Part 52, the NRC requires the following criteria:

- compliance with the TMI requirements in 10 CFR 50.34(f)
- resolution of unresolved safety issues and generic safety issues
- completion of a design-specific PRA

The staff evaluates these criteria in Sections 20.3, 20.1 and 20.2, and 19.1 of this report, respectively.

The Commission-approved positions on the issues discussed in SECY-93-087, SECY 96-128, and SECY-97-044 form the basis for the staff's deterministic evaluation of severe accident performance for the AP600. The staff evaluates the AP600 relative to these criteria in Section 19.2 of this chapter.

## 19.1 Probabilistic Risk Assessment

### 19.1.1 Introduction

As part of the AP600 advanced design certification application, Westinghouse submitted a PRA in accordance with the requirements of 10 CFR 52.47 and the Commission's policy "Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants." The NRC staff's assessment consisted of the traditional evaluation of events that could lead to core damage and offsite consequences as well as an evaluation of what the PRA revealed about the AP600 design.

#### 19.1.1.1 Background and NRC Review Objectives

The general objectives of the NRC staff's review of the AP600 design PRA included the following activities:

- identify safety insights based on systematic risk-based evaluations of the design
- support the process used to determine whether regulatory treatment of non-safety systems (RTNSS) was necessary
- determine in a quantitative manner whether the design represents a reduction in risk over existing plants
- assess the balance of preventive and mitigative features of the design
- assess the reasonableness of the risk estimates documented in the PRA
- support design certification requirements, such as inspection, tests, analyses, and acceptance criteria (ITAACs), design reliability assurance program (D-RAP), technical

specifications (TS), as well as combined operation license (COL) and interface requirements.

In addition, the staff used the AP600 PRA to determine how the risk associated with the design relates to the safety goals of core damage frequency (CDF) less than 1E-04/yr and large release frequency (LRF) of less than 1E-06/yr, and to uncover design and operational vulnerabilities.

The objectives are drawn from 10 CFR Part 52, the Commission's Severe Reactor Accident Policy Statement regarding future designs and existing plants, the Commission's Safety Goal Policy Statement, the Commission approved positions concerning the analyses of external events contained in SECY-93-087, and NRC interest in the use of PRA to help improve future reactor designs. In general, these objectives have been achieved by the AP600 PRA and the NRC staff's review.

During the construction stage, the COL applicant will be able to consider as-built information. The Commission believes that updated PRA insights, if properly evaluated and used, could strengthen programs and activities in areas such as training, emergency operating procedures development, reliability assurance, maintenance, and 10 CFR 50.59 evaluations. The design-specific PRA, developed as part of the design certification process, should be revised to account for site-specific information, as-built (plant-specific) information refinements in the level of design detail, technical specifications (TS), plant specific emergency operating procedures, and design changes. This is COL Action Item 19.1.1-1. These updates are the responsibility of the COL applicant. As plant experience data accumulates, failure rates (taken from generic data bases) and human errors assumed in the design PRA are to be updated and incorporated, as appropriate, into the operational reliability assurance program (O-RAP).

19.1.1.2 Evaluation of PRA Quality and Closure of Open Issues

The NRC staff has completed its review of the quality and completeness of the AP600 PRA. These attributes are essential in using the PRA to gain insights about how the design is robust and tolerant to severe accidents, and to provide risk-based input to pre and post-certification activities, thus achieving the objectives itemized above (Section 19.1.1.1). The staff reviewed the quality of the PRA submittal by evaluating the models, techniques, methodologies, assumptions, data, and calculational tools that were used by Westinghouse. In addition, the staff checked the AP600 PRA for completeness by engaging in the following activities:

- comparing it with PRAs performed for current generation and evolutionary pressurized water reactor (PWR) designs to ensure that known safety significant PWR issues either do not apply to AP600 design or they were appropriately modeled in the PRA

- ensuring that the final resolution of various deterministic issues, raised by the staff during the certification process, was appropriately incorporated into the PRA models

The review of the quality and completeness of the PRA submittal involved the issuance of requests for additional information (RAI) to the Westinghouse, followed by the evaluation of Westinghouse's responses to the RAI. In conducting the technical review, the staff followed guidance existing in the "PRA Review Manual" (NUREG/CR-3485). Reported PRA results, as well as results of sensitivity, uncertainty, and importance analyses, were used to focus the

review. A sharper focus was also achieved by using PRA experience in the review process. The staff used applicable insights from previous PRA studies about key parameters and design features controlling risk. The staff also placed a special emphasis on PRA modeling of novel and passive features in the design as well as addressing issues related to these features, such as the issue of thermal-hydraulic (T-H) uncertainties.

The need to assess the impact of T-H uncertainties on the performance of passive systems was identified early in the AP600 PRA review and was documented in the draft safety evaluation report (DSER). The AP600 design has unique features that distinguish the AP600 design from both operating and advanced evolutionary LWR designs. Although it uses both active and passive systems for accident prevention and mitigation, only the passive systems are safety graded. Passive safety systems rely on natural forces, such as gravity, to perform their functions. Such driving forces are small compared to those of pumped systems and the uncertainty in their values, as predicted by a "best-estimate" T-H analysis, can be of comparable magnitude to the predicted values themselves. Therefore, some accident sequences with frequency high enough to impact results, which are not predicted to lead to core damage by a "best-estimate" T-H analysis, may actually lead to core damage when T-H uncertainties are considered in the PRA models. The evaluation of the approach and associated analyses performed by Westinghouse to address the issue of T-H uncertainties and its impact on PRA models is discussed in Section 22.5.4.1 of this report.

Although the review has been a continuous process, it involved two distinct stages. The first stage of the review ended with the issuance of a DSER. In the DSER, the staff identified two classes of items that they believed needed additional attention by Westinghouse. The two classes identified were:

(1) open items (i.e., areas where the staff disagreed with the submittal or required additional supporting documentation)

(2) COL action items (i.e., areas where the COL applicant should factor in plant or site-specific information at the COL stage)

The second stage of the review involved the resolution of all DSER open items, the inclusion of all identified COL action items, and the preparation of the final safety evaluation report (FSER). The resolution (closure) of DSER open items involved close interaction between the staff and Westinghouse, including several rounds of RAIs and Westinghouse's responses. A summary of DSER open items and the associated resolutions is given in section 19.1.10 of this chapter.

The NRC staff concludes that the quality and completeness of the AP600 PRA are adequate for its intended purposes, such as supporting the design and certification processes. The approaches used by Westinghouse for both the core-damage and containment analyses are logical and sufficient to achieve the desired goals of describing and quantifying potential core-damage scenarios and containment performance during severe accidents. All open items reported in the DSER were resolved satisfactorily.

The special advanced design features that were incorporated into the AP600 design for the purpose of preventing and mitigating accidents are briefly presented in Section 19.1.2 below. Safety insights about the AP600 design, drawn from the internal events risk analysis for

operation at power, are presented in Section 19.1.3. Safety insights about the AP600 design, drawn from the internal events risk analysis for low power and shutdown operation are reported in Section 19.1.4. Safety insights from the external events risk analysis (seismic, internal fires and internal floods), for both at-power and shutdown operation, are reported in Section 19.1.5. In Section 19.1.6, Westinghouse provides examples of use of PRA in the design process. In Section 19.1.7, Westinghouse reports the PRA input to the RTNSS process, while in Section 19.1.8, Westinghouse presents the PRA input (derived from PRA insights and assumptions) to the design certification process. Finally, in Section 19.1.9, Westinghouse summarizes the major conclusions and findings about the design consistent with the objectives of the PRA and its use in the design and certification processes.

### 19.1.2 Special Advanced Design Features

The AP600 standard design evolved from current pressurized (light) water reactor (PWR) technology through incorporation of several passive design features and other design changes intended to make the plant safer, more available, and easier to operate. Insights from operating reactor PRAs, helped in designing such passive features as well as in identifying other design changes. Therefore, the AP600 design incorporates features intended to improve plant safety, and thus reduce risk, when compared to current generation nuclear power plants.

Some of these special advanced design features are preventive in nature while others are mitigative. Preventive features aim to accomplish the following objectives:

- minimize the initiation of plant transients
- arrest the progression of plant transients once they start
- prevent severe accidents (core damage).

Mitigative features aim to arrest the progression of core damage and prevent breach of the reactor vessel and containment pressure boundary. The major preventive and mitigative special advanced design features of the AP600 design are described in this report in Sections 19.1.2.1 and 19.1.2.2, respectively. In these descriptions, a brief qualitative discussion points out the effect that each of these features has on various elements involved in severe accident prevention and mitigation. More details about these features are found in the appropriate chapters of the AP600 Standard Safety Analysis Report (SSAR).

#### 19.1.2.1 Special Advanced Design Features for Preventing Core Damage

Major features incorporated into the AP600 design for the purpose of limiting plant transients and preventing severe accidents are discussed below.

Passive Safety-Related Systems

The AP600 design relies on passive safety-related systems for accident prevention and mitigation. The passive systems rely on natural forces, such as gravity and stored energy, to perform their safety functions (once actuated and started). In order for such systems to actuate and start, certain active components, such as air operated valves (AOVs) or check valves (CVs), must open. Such components do not require ac power for operation (to open) or for control, and no support systems are needed after actuation. This significantly reduces, as compared to operating nuclear power plants, the risk contribution from loss of offsite power and

station blackout (LOOP/SBO) events. In addition, because of the passive systems, several important contributions to risk for operating nuclear power plants have been eliminated in the AP600 design: They are associated with failure of support systems (e.g., ac power and component cooling) and failure of active components (e.g., pumps and diesel generators) to start and run. Finally, the passive nature of the safety systems reduces, as compared to operating reactor designs, the reliance on operator actions to mitigate accidents. For a fair comparison to operating and evolutionary reactor designs, which use mostly active safety-related systems, the potential impact of T-H uncertainties on the performance of passive systems needs to be considered and appropriately included in the PRA models. Analyses performed by Westinghouse (e.g., WCAP-14800, 1997) concluded that the AP600 design is "robust" with respect to T-H uncertainties. The staff's review is discussed in Section 22.5.4.1 of this report.

Defense-In-Depth Active Non-Safety-Related Systems

The AP600 design incorporates several active systems which are capable of performing some of the same functions performed by the safety-related passive systems. The availability of such redundant systems minimizes the challenge to the safety-related passive systems by providing core cooling during normal plant shutdowns and a first line of defense during accidents. Operation of the non-safety-related startup feedwater (SFW) system prevents challenging the passive residual heat removal (PRHR) heat exchanger during anticipated transients. For accidents occurring during power operation, the non-safety-related normal residual heat removal system (RNS) provides additional defense-in-depth to the "feed" portion of the "feed-and-bleed" core cooling function (provides an alternate "pumped" means of low pressure injection from the in-containment refueling water storage tank (IRWST) and long-term recirculation from the containment sump). The diverse actuation system (DAS) provides an alternate means for initiating automatic and manual reactor trip and actuation of selected engineered safety features which is diverse from the safety-related protection and safety monitoring system (PMS).

In-Containment Refueling Water Storage Tank (IRWST)

Important characteristics and functions of the IRWST include the following:

- large capacity
- acts as a heat sink for the PRHR
- provides water for low pressure emergency core cooling (IRWST injection and RNS injection) after reactor coolant system depressurization
- serves as the heat sink for the first three stages of the Automatic Depressurization System (ADS)
- provides debris cooling following a severe accident.

The IRWST is a central feature in the AP600 design which contributes to the simplicity and reliability of the passive safety systems. As the heat sink for the PRHR heat exchanger, it

allows reliable core cooling at high reactor coolant system (RCS) pressures when cooling through the steam generators (SGs) fails during anticipated transients and steam generator tube rupture (SGTR) events (reduces the need for RCS depressurization and use of "feed-and-bleed" cooling). It is a reliable source of borated water for low pressure emergency core cooling and eliminates the need for switching over from the injection mode to the recirculation mode during emergency core cooling operations (a risk-important failure at operating PWRs).

Redundant Decay Heat Removal Systems

Redundant decay heat removal systems provide defense-in-depth during all possible scenarios of an accident. Alternative means for core cooling include the following:

- main feedwater and condensate
- startup feedwater
- automatically actuated (with manual actuation backup capability) PRHR
- automatic with manual backup "feed and bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two core makeup tanks (CMTs), two accumulators, the two RNS pumps and the two IRWST gravity injection lines) and the "bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage)

Automatic Depressurization System (ADS)

The function of the ADS is to provide a safety-related means of reducing RCS pressure in a controlled fashion during accidents to allow safety injection. This constitutes the "bleed" portion of the "feed-and-bleed" means of core cooling. ADS is actuated automatically, with manual backup actuation capability, and has incorporated redundancy (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage) and defense against common-cause failures (motor operated valves (MOVs) in the first three stages, explosive valves in the fourth stage).

Redundant Safety Injection Systems

The AP600 design includes redundant and diverse means of providing safety injection (i.e., the "feed" portion of the "feed-and-bleed" core cooling function) throughout the RCS depressurization range. Safety injection is provided by safety-related systems (two CMTs, two accumulators and two IRWST gravity injection lines) as well as by non-safety-related "defense-in-depth" systems (the two chemical and volume control pumps and the two normal residual heat removal pumps).

Redundant Long-Term Recirculation Systems

RCS recirculation is required for long-term core cooling during loss-of-coolant accidents (LOCAs) and whenever "feed-and-bleed" is used to cool the core during an accident. In the

AP600, recirculation can be either by gravity (through the safety-related IRWST injection lines) or pumped (through the non-safety-related normal residual heat removal system) with suction from the containment sump. There are two redundant recirculation lines (one for each of the two redundant IRWST injection lines). Furthermore, each recirculation line has two redundant paths.

Redundant Passive Containment Cooling Systems

Containment cooling, as the ultimate heat sink function for all accidents involving loss of feedwater (main and startup) to both steam generators, is very important in the AP600 design. The containment cooling function is performed by two highly reliable and redundant means which remove thermal energy from the containment atmosphere to the environment via the steel containment vessel by (1) natural external air circulation and (2) evaporation of water drained by gravity from an elevated tank.

Canned Reactor Coolant Pumps (RCPs)

Because of the canned motor RCPs, RCP seal LOCA (an important contributor to risk for operating nuclear power plants) has been eliminated in the AP600 design.

Improved Control Room Design/Digital I&C Systems

The AP600 Control Room design is an advanced design that is expected to provide more as well as more useful information to the operator during an accident than currently operating reactor designs. The AP600 Control Room is still being designed. For this reason, no credit was taken in the PRA for the impact of the advanced control room on normal operations (e.g., initiating event frequency) and emergency response.

Larger Pressurizer/Lower Power Density

The larger pressurizer, as compared to operating plants, reduces the frequency of reactor scrams by increasing transient operation margins. This feature also moderates the pressure rise during certain transient events, such as loss of main feedwater, thus reducing the likelihood of challenging the primary safety valves. A larger pressurizer volume also helps lower the peak pressure that can be reached after a postulated ATWS event.

Physical Separation of Safety System Redundant Trains

The design provides physical separation of safety systems or trains of systems that perform redundant safety-related functions. This increases the availability of systems due to their protection from failures associated with internal fires, internal floods, and similar common cause failures. Except for support systems, such as class 1E dc power and instrumentation and control (I&C) systems, and the passive containment cooling system (PCS), all passive safety-related systems are located inside the containment where external events, such as fires, floods and tornados, are less likely to occur. This contributes to the reduction of risk as compared to current plant designs.

Highly Reliable dc Power Supply With 72-Hour Station Blackout Coping Capability

Each of the four independent and physically separated divisions of 125V dc Class 1E vital instrumentation and control power is provided with a separate and independent Class 1E 24-hour battery bank. In addition, two of the four divisions are provided with a Class 1E 72-hour battery bank. This permits operating instrumentation and control loads, associated with safety systems that may be required following the loss of ac power concurrent with a design-basis accident, for 72 hours. This feature contributes to the large reduction of risk associated with station blackout accidents as compared to current plant designs.

19.1.2.2 Special Advanced Design Features for Core Damage Consequence Mitigation

The following design features improve the ability of the containment to accommodate the challenges associated with severe core damage accidents. The impact of these features on severe accident mitigation and containment performance is modeled in the AP600 PRA and/or supporting deterministic analyses. The staff's evaluation of these models and analyses is provided later in Section 19.1.10 and 19.2 of this report.

Automatic Depressurization System (ADS)

In addition to providing a core damage prevention function, the ADS also serves a mitigative function. Specifically, in core damage events in which early depressurization is not successful, late actuation of ADS (before significant core damage and debris relocation into the lower plenum of the reactor vessel) can reduce or eliminate the potential for creep rupture of the steam generator tubes and the reactor vessel. Prevention of reactor vessel breach precludes severe accident phenomena associated with vessel failure -- direct containment heating (DCH), large hydrogen combustion events at vessel breach, ex-vessel steam explosions, and core concrete interactions -- thereby reducing the probability of early containment failure. The ADS also reduces the amount of fission products released to the containment atmosphere since a portion of the discharge flow (from ADS stages 1 through 3) is routed through a sparger network in the IRWST. However, because the 4th stage of ADS vents to the containment airspace at the time when most fission products are released, the potential for fission product scrubbing is not fully realized. Finally, RCS depressurization can reduce or terminate fission product releases to the environment during steam generator tube rupture events.

Large Passively-Cooled Steel Containment

The AP600 design includes a large, passively cooled steel containment. The containment building volume to reactor power ratio for AP600 is greater than most operating PWRs. The increased volume to power ratio reduces the potential for developing detonable concentrations of hydrogen under severe accident conditions and the potential for containment overpressure from non-condensible gas buildup. These challenges would otherwise be more severe in AP600 due to the relatively greater mass of zircaloy associated with the lower power density core in AP600. The containment pressure capacity is sufficiently large that the pressure loads associated with early challenges, e.g., hydrogen combustion and direct containment heating, are at or below Westinghouse's Service Level C estimate (90 psig) and pose an insignificant threat to containment integrity (a containment failure probability of less than one percent).

The PCS provides water to the external surface of the containment shell from the PCS water storage tanks or the post-72 hour water tank. Alternative water sources can be provided via separate connections outside containment in accordance with accident management guidelines to be developed by the COL applicant (see COL Action Item 19.2.5-1). However, even without operation of the PCS, air cooling alone is sufficient to maintain containment pressure below Westinghouse's Service Level C estimate in the long term (provided the core is retained in-vessel), and the additional failure of air cooling would not result in pressures above Westinghouse's Service Level C estimate until about 30 hours. In the event that the reactor vessel is breached and core concrete interactions occur, air cooling alone is sufficient to prevent the containment from exceeding Westinghouse's Service Level C estimate until well after 3 days.

In-Containment Refueling Water Storage Tank (IRWST)

The AP600 design incorporates an IRWST. In addition to serving the typical function of the RWST at operating plants, this system performs water collection, delivery, and heat sink functions inside the containment during accident conditions. The IRWST is important to the progression of a severe accident due to its ability to condense steam and scrub fission products for releases into the IRWST via stages 1 through 3 of ADS, and to reduce the likelihood of reactor vessel failure and core-concrete interaction (CCI) by enabling reactor cavity flooding via gravity draining. The potential for hydrogen-rich mixtures to form in the vicinity of the IRWST (as a result of steam condensation as the hydrogen-steam blowdown passes through the IRWST) represents a unique containment challenge for AP600, but is minimized by locating the discharge from break compartments and the 4th stage ADS valves in areas where diffusion flames will not impinge on the containment shell.

External Reactor Vessel Cooling

The capability to fully flood the AP600 reactor cavity and depressurize the RCS in the majority of core melt sequences minimizes the potential for reactor vessel breach by molten core debris. By maintaining reactor vessel integrity, the potential for large releases due to ex-vessel severe accident phenomena is substantially reduced, however, a residual threat from hydrogen combustion remains. The ability to flood the reactor cavity is enhanced in the AP600 design by the following attributes:

- a containment and reactor cavity arrangement which permits breakflow from the RCS to drain to the cavity without significant holdup in containment

- the inclusion of manually-actuated safety-grade valves which allow additional water from the IRWST to be drained to the cavity

The operator action to flood the cavity is specified in ERG FR.C-1, which instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission product releases as determined by a core damage assessment guideline. The effectiveness of external reactor vessel cooling is enhanced in AP600 by the following three items:

- a lower power density core relative to operating plants

- a reactor vessel lower head which contains no in-core instrument or other penetrations
- a reactor vessel insulation system which limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents

Reactor Cavity Design

The AP600 design relies primarily on safety grade RCS depressurization and reactor cavity flooding capabilities to prevent high pressure core melt events and reactor vessel breach. In the event that vessel breach occurs, the AP600 reactor cavity design is sufficient to accommodate the loads associated with ex-vessel severe accident phenomena without early loss of containment integrity. These challenges include DCH, fuel-coolant interactions (FCI), and CCI. The specific reactor cavity features to deal with each challenge are summarized below.

**DCH:** The paths from the reactor cavity to the upper containment volume in AP600 include the following:

- the area around the reactor vessel flange
- the area where the coolant loops penetrate through the biological shield
- a ventilation shaft from the roof of the reactor coolant drain tank room that leads to the steam generator compartments.

These paths are convoluted, hence a portion of the corium will be de-entrained and removed from the atmosphere before reaching the upper containment region, thereby reducing the pressure rise associated with DCH. The peak containment pressure for a postulated DCH event, estimated using the NRC-developed model for resolution of the DCH issue (Pilch et al., NUREG/CR-6338) is sufficiently small (81 psig) that the corresponding probability of containment failure is negligible (less than 0.1 percent).

**FCI:** The reactor vessel cavity concrete structure has a high dynamic pressure capacity, as discussed in Appendix B to Revision 11 of the PRA. The deterministic evaluation of ex-vessel FCIs (Section 19.2.3.3.5.2 of this report) indicates that the impulse loads from ex-vessel steam explosions would fail the reactor cavity floor and wall structures, but that the integrity of the embedded steel liner will be maintained. The evaluation also indicates that containment vessel integrity will not be compromised by the displacement of the reactor pressure vessel (RPV) as a result of the impulse loading.

**CCI:** The AP600 reactor cavity design incorporates features generally consistent with the EPRI utility requirements document (URD) criteria, including the following:

(1) a cavity floor area that provides for debris spreading based on a criteria of $0.02 m^2/MW_{th}$

(2) a minimum 0.85m (2.8ft) layer of concrete to protect the embedded containment shell, with an additional 1.8m (6ft) of concrete below the liner elevation

(3) a manually-actuated reactor cavity flood system for the purpose of covering the core debris with water and maintaining long-term debris coolability.

The enhanced capability to retain a molten core in-vessel, in conjunction with these design features, result in a low expected frequency of basemat melt-through in the AP600 PRA.

Compared to other advanced light-water reactors (ALWRs), the AP600 ex-vessel debris bed is deeper (due to the higher ratio of zircaloy to fuel in the AP600 core), and the concrete basemat is thinner. In addition, the AP600 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls. Although these factors tend to increase the severity of basemat erosion, analyses using the MELTSPREAD and MAAP codes indicate that in the event of unabated CCI, containment basemat penetration or containment over-pressurization will not occur until after 72 hours, regardless of concrete composition.

For a limestone basemat (which maximizes non-condensible gas generation and minimizes concrete ablation) containment pressure will not reach Westinghouse's Service Level C estimate (90 psig) until about 11 days following the onset of core damage; basemat penetration would occur even later. Use of basaltic concrete (which maximizes concrete ablation and minimizes non-condensible gas generation) would reduce the time of basemat melt-through to about 3 days, but over-pressure failure would not occur until much later. Thus, in the event that core debris is not retained in vessel, the AP600 design provides adequate protection against early containment failure and large releases due to core concrete interactions.

Hydrogen Igniter System

The AP600 design incorporates a distributed ignition system to promote combustion at lean hydrogen concentrations and minimize the potential for large deflagrations or detonations. The igniter system is non-safety-related but is subject to investment protection short-term availability controls as described in Section 16.3 of the SSAR. The system uses 64 glow plug igniters powered from the non-safety-related onsite ac power system and is manually actuated from the control room when core exit temperature exceeds 1200 °F, as the first step in the AP600 emergency response guideline (ERG) FR.C-1. The hydrogen igniter system is capable of being powered by either offsite ac power or onsite non-essential diesel generators. In the event of a station blackout, which represents less than 1 percent of the core damage frequency, the system can be powered from the non Class 1E batteries via dc-to-ac inverters. However, this feature was added late in the design process and is not credited in the PRA. The AP600 design also includes four passive autocatalytic recombiners (PARs). The PARs are provided primarily to cope with hydrogen production during design-basis accidents, and are also not credited in the PRA. Nevertheless, they are expected to function to reduce combustible gas concentrations during severe accidents. The proven design of the glow plug igniters and the diverse means of powering the system, in conjunction with the small fraction of core melt sequences involving loss of onsite power in the AP600 design, significantly reduce the threat of containment failure due to hydrogen deflagrations or detonations. The use of PARs further reduces the threat from hydrogen burns in those events in which the igniters are unavailable.

Non-Safety Containment Spray System

The AP600 includes a non-safety containment spray system for severe accident management. The system consists of two spray rings located above the containment polar crane, with flow supplied from the normal fire main header. The source of water is provided by either the primary or secondary fire protection system water tank (depending on tank and inventory availability) using either the motor-driven or diesel-driven fire protection system pump. The non-safety grade containment spray system was added to the AP600 design subsequent to Revision 8 of the PRA. As such, its impact on containment response and fission product releases is not reflected in the Level 2 and 3 PRA results. Containment sprays could significantly reduce the estimated risk in the baseline PRA since the sprays would be effective in reducing the source terms in the risk-dominant release categories.

Containment Vent

The AP600 design configuration includes a containment vent path that can be used to control containment pressure in the unlikely event of long-term over-pressurization of containment. With the RCS depressurized and open to the containment atmosphere via either the ADS or the reactor vessel breach, the containment may be vented to the spent fuel pool via the residual heat removal suction lines. The manual valve from the spent fuel pool to the RNS pump suction would be opened and then the RNS hot-leg suction isolation valves would be operated remotely to control the vent process.

19.1.3 Safety Insights From the Internal Events Risk Analysis (Operation at Power)

These insights include:

- dominant accident sequences contributing to the core damage frequency
- areas where certain AP600 design "passive" and "defense-in-depth" features were the most effective in reducing risk with respect to operating reactor designs
- major contributors to the estimated CDF from internal events, such as hardware failures, system unavailabilities, and human errors
- major contributors to maintaining the "built-in" plant safety (to ensure that risk does not increase unacceptably)
- major contributors to the uncertainty associated with the estimated CDF
- sensitivity of the estimated CDF from internal events to potential biases in numerical values, to assumptions made, to lack of modeling details in certain areas, and to previously raised safety issues
- core damage sequences and accident classes contributing to containment failure
- frequency and conditional probability of containment failure

- leading contributors to containment failure and risk
- important insights and supporting sensitivity analyses from the levels 2 and 3 of the PRA

19.1.3.1 Level 1 Internal Events PRA

Westinghouse estimated the mean CDF for the AP600 design, from internal events during operation at power, to be about 2E-07 per year. In addition, CDFs for various initiating event categories were estimated and are summarized in Table 19.1-1. Ranges of mean CDFs, by initiating event category, for currently operating PWR reactor designs (NUREG-1560, 1996) are also shown for comparison. The total CDF for the AP600 design was estimated by Westinghouse to be roughly two orders of magnitude smaller than the total CDF of an average operating PWR reactor.

For the AP600 design, the various LOCA categories of initiating events essentially dominate the CDF profile (~80 percent contribution) followed by ATWS sequences (~6 percent) and reactor vessel rupture (~6 percent). Contributions from "transient" events (~3 percent), SGTR events (~3 percent) and LOOP/SBO (less than 1 percent) are relatively small.

In Section 19.1.3.1.1, Westinghouse presents the dominant accident sequences and the major contributors to the CDF estimates for the AP600 design. The design features that contribute to the reduced CDFs, as compared to operating PWRs, are described in Section 19.1.3.1.2. Finally, in Sections 19.1.3.1.3, 19.1.3.1.4 and 19.1.3.1.5 are reported the insights drawn from the uncertainty analysis and the importance and sensitivity studies.

19.1.3.1.1 Dominant Accident Sequences Leading to Core Damage

Westinghouse's PRA results identify 50 sequences, initiated by internal events, which contribute 99 percent of the estimated CDF from internal events. The top 12 sequences, contributing about 90 percent of the total CDF from internal events, are summarized below.

Sequence #1, with a CDF of about 4E-08 per year and 20 percent contribution, is initiated by a break in one of the two safety injection lines (a LOCA event) followed by failure of the IRWST injection line which is not affected by the break to remove decay heat from the core (CMT injection and RCS depressurization via the ADS system are successful). In addition to the initiating event, risk important failures appearing in this sequence are listed below:

- common cause failure (CCF) of the two check valves in the intact IRWST discharge line
- CCF of the two explosive (squib) valves in the intact IRWST discharge line
- plugging of the IRWST discharge line strainer in the intact line.

Sequence #2, with a CDF of 4E-08/yr and 20 percent contribution, is initiated by a large LOCA event (equivalent break diameter greater than 9 inches but smaller than a vessel rupture) followed by failure of IRWST injection (injection by at least one accumulator is successful and

containment isolation either is not needed or is successful). Risk important failures, in addition to the initiating event, appearing in this sequence are listed below:

- CCF of hardware in the PMS engineered safety feature (ESF) input logic groups (causes CMT injection actuation failure which results in failure of automatic IRWST injection actuation with no adequate time for manual actuation)
- CCF of CMT level sensors which prevents IRWST injection actuation
- CCF of CMT injection air-operated valves to open
- CCF of CMT injection check valves to open
- CCF of the four check valves in the two IRWST discharge lines
- CCF of the four explosive (squib) valves in the two IRWST discharge lines
- CCF of both IRWST discharge lines due to plugging of both IRWST tank strainers

Sequence #3, with a CDF of about 3E-08 per year and 15 percent contribution, is initiated by an intermediate LOCA event (2 to 6 inches equivalent break diameter) followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (high pressure injection by the CMTs, depressurization and low pressure injection are successful). Risk important failures, in addition to the initiating event, appearing in this sequence are listed below:

- CCF of the four explosive (squib) valves in both sump recirculation lines to open
- CCF of both sump recirculation lines due to sump screen plugging
- CCF of all IRWST level transmitters (causes failure of automatic actuation of sump recirculation)
- operator failure to manually actuate sump recirculation (when automatic actuation fails).

Sequence #4, with CDF of 1E-08/yr and 5 percent contribution, is a reactor vessel rupture event which leads directly to core damage.

Sequence #5, with a CDF of about 8E-09/yr and 4 percent contribution, is initiated by a large LOCA event followed by failure of both accumulators to inject. The failure that dominates this sequence, in addition to the initiating event, is CCF of check valves in both accumulator injection lines (at least one of the two in each line) to open.

Sequence #6, with a CDF of 7E-09/yr and 4 percent contribution, is initiated by a medium LOCA event (6 to 9 inches equivalent break diameter) followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (high pressure injection by the CMTs, depressurization and low pressure injection are successful). Risk

important failures, in addition to the initiating event, appearing in this sequence are listed as follows:

- CCF of the four explosive (squib) valves in both sump recirculation lines to open
- CCF of both sump recirculation lines due to sump screen plugging
- CCF of all IRWST level transmitters (causes failure of automatic actuation of sump recirculation)
- operator failure to manually actuate sump recirculation (when automatic actuation fails).

Sequence #7, with a CDF of about 6E-09/yr and 3 percent contribution, is initiated by an event that results in loss of main feedwater (MFW) to both steam generators followed by reactor trip failure (ATWS event with loss of MFW precursor). If the ATWS event happens to occur early in the fuel cycle when an adverse moderator temperature coefficient (MTC) exists and the operator fails to actuate control rod insertion via the plant control system within one minute (to insert sufficient negative reactivity to allow adequate pressure relief through the safety valves), core damage is assumed. Risk important failures appearing in this sequence, in addition to the initiating event and the length of the unfavorable exposure time (time when an adverse MTC exists), are listed below:

- CCF of the PMS reactor trip breakers to open (mechanical failure)
- CCF of the reactor trip portion of PMS hardware or software (no signal to open the PMS reactor trip breakers)
- failure of a motor-generator (M-G) set circuit breaker to open by DAS (mechanical failure)
- operator failure to manually trip the reactor within one minute through PMS or DAS when automatic trip fails
- failure of automatic DAS function (hardware or software)
- failure of the turbine impulse pressure transmitter (DAS trip permissive).

Sequence #8, with a CDF of about 5E-09 per year and 3 percent contribution, is initiated by a small LOCA event (3/8 to 2 inches equivalent break diameter) followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (high pressure injection by the CMTs, heat removal by the PRHR, depressurization and low pressure injection are successful). Risk important failures, in addition to the initiating event, appearing in this sequence are listed below:

- CCF of the four explosive (squib) valves in both sump recirculation lines to open
- CCF of both sump recirculation lines due to sump screen plugging

- CCF of all IRWST level transmitters (causes failure of automatic actuation of sump recirculation)

- operator failure to manually actuate sump recirculation (when automatic actuation fails)

Sequence #9, with a CDF of about 4E-09 per year and 2 percent contribution, is initiated by a break in one CMT line followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (CMT injection, depressurization and low pressure injection are successful). Risk important failures, in addition to the initiating event, appearing in this sequence are shown as:

- CCF of the four explosive (squib) valves in both sump recirculation lines to open

- CCF of both sump recirculation lines due to sump screen plugging

- CCF of all IRWST level transmitters (causes failure of automatic actuation of sump recirculation)

- operator failure to manually actuate sump recirculation (when automatic actuation fails)

Sequence #10, with a CDF of 3E-09/yr and 2 percent contribution, is an ATWS event with loss of MFW precursor followed by successful heat removal (by either the SFW or the PRHR) and successful operator actuation of control rod insertion (via the plant control system) so sufficient negative reactivity is inserted to allow adequate pressure relief through the safety valves even when an adverse MTC exists. Although pressure relief through the safety valves is successful, boration of the RCS (by the chemical and volume control system or by CMT injection) fails. This is assumed to lead to core damage. Risk important failures appearing in this sequence are listed below:

- CCF of sensors in high pressure environment

- CCF of pressurizer level sensors

- operator failure to manually trip the reactor within one minute through PMS or DAS when automatic trip fails.

Sequence #11, with a CDF of about 3E-09 per year and 2 percent contribution, is initiated by an intermediate LOCA event (2 to 6 inches equivalent break diameter) followed by successful high pressure injection by the CMTs and successful RCS depressurization for low pressure injection. However, low pressure injection (either by the RNS or by IRWST injection) fails. This leads to core damage. Risk important failures appearing in this sequence are:

- CCF of the four check valves in the two IRWST discharge lines to open
- CCF of the four explosive (squib) valves in the two IRWST discharge lines to open
- CCF of both IRWST discharge lines due to plugging of both IRWST tank strainers
- single failure of any of three RNS isolation valves (V011, V022, V023) to open
- CCF of two RNS injection stop check valves (V15A and V15B) to open

Sequence #12, with a CDF of about 3E-09 per year and 2 percent contribution, is initiated by a break in one of the two safety injection lines (a LOCA event) followed by successful CMT injection but failure of full RCS depressurization (to allow low pressure IRWST injection). The failure that dominates the risk associated with this sequence is the CCF of ADS stage #4 explosive (squib) valves.

19.1.3.1.2 Risk Important Design Features

Listed below are major features that contribute to the reduced CDF of the AP600 design as compared to operating PWR designs, for each of the initiating event categories contributing the most to this reduction.

Loss of Offsite Power and Station Blackout Sequences

The following are the most important features of the AP600 design which contribute to the reduction in the estimated CDF associated with LOOP, including station blackout (SBO), sequences (CDF reduced to 1E-09/yr from the 7E-05/yr to 1E-08/yr range corresponding to CDFs associated with LOOP/SBO at operating PWR reactors):

- Safety-related passive systems that do not rely on ac power for operation. They rely on natural forces, such as gravity and stored energy, to perform their accident mitigation functions once actuated and started. When power is needed to actuate and start such passive systems, dc power provided by Class 1E batteries is used.

- The PRHR is automatically actuated, without the need for any electrical power, to provide core cooling upon LOOP (AOVs "fail safe" in the open position).

- Class 1E dc batteries with capability to support all front line passive safety-related systems for 72 hours.

- Defense-in-depth, which provides alternative means for removing decay heat from the RCS during a LOOP/SBO accident. Most current PWR plants rely on two alternative means for core cooling:

  (1) an Auxiliary Feedwater System, with at least one turbine driven pump for SBO events, in addition to motor driven pump(s)

  (2) a manual "feed and bleed" capability when onsite ac power is available

  The AP600 design provides better and more reliable defense-in-depth by relying on the following alternative means for core cooling:

  (1) the automatically actuated non-safety-related Startup Feedwater (SFW) system when onsite ac power is available

  (2) the automatically actuated safety-related PRHR system

(3) an automatic with manual backup "feed and bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two CMTs, two accumulators, the two RNS pumps and the two IRWST gravity injection lines) and the "bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage)

- The improved reliability of the PRHR system (as compared to the AFW system used in most current PWR plants) contributes significantly to the reduced risk associated with LOOP/SBO sequences (the function of the PRHR following a LOOP/SBO event is similar to the AFW system function in operating PWRs).

- Canned reactor coolant pumps eliminate seal LOCAs, which are likely in operating PWRs during an SBO accident.

"Transient" Sequences

The following are the most important features of the AP600 design which contribute to the reduction in the estimated CDF associated with "transient" sequences (CDF reduced to 5E-09/yr from the 3E-04/yr to 5E-07/yr range corresponding to CDFs associated with "transients" at operating PWR reactors):

- Defense-in-depth which provides several alternative means for core cooling during all possible scenarios of the accident. Most current PWR plants rely on three alternative means for core cooling following a "transient" initiator (main feedwater and condensate, auxiliary feedwater, and manual "feed and bleed"). The AP600 design provides better and more reliable defense-in-depth by relying on the following alternative means for core cooling:

  (1) main feedwater and condensate

  (2) startup feedwater

  (3) automatically actuated (with manual actuation backup capability) PRHR

  (4) automatic with manual backup "feed and bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two CMTs, two accumulators, the two RNS pumps and the two IRWST gravity injection lines) and the "bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage)

- A reliable PRHR system (which is needed only when the non-safety-related SFW system is unavailable) reduces significantly the need for RCS depressurization and reliance on "feed and bleed" cooling, as compared to operating PWRs, and contributes to the reduced risk associated with "transient" sequences (the functions of the SFW and PRHR following a "transient" event are redundant and similar to the function performed by the AFW system in operating PWRs).

- Use of two redundant and diverse engineered safety feature (ESF) actuation systems with automatic and manual actuation capability (one is safety-related) minimizes the likelihood of actuation failures, including common-cause actuation failures.

- Use of passive safety-related systems which do not need several traditional support systems, such as component cooling water and ac power, to operate eliminates all failures associated with such support systems in operating PWRs and contributes significantly to the increased reliability of most AP600 safety-related systems as compared to systems for operating plants performing similar functions.

- The use of a larger pressurizer than those at comparable operating PWR plants reduces the frequency of "transient" initiating events by increasing transient operation margins.

Steam Generator Tube Rupture (SGTR) Sequences

The following are the most important features of the AP600 design which contribute to the reduction in the estimated CDF associated with steam generator tube rupture (SGTR) sequences (CDF reduced to about 6E-09/yr from the 3E-05/yr to 9E-09/yr range corresponding to CDFs associated with SGTR at operating PWR reactors):

- Three lines of defense against core damage following an SGTR event:

  (1) use of non-safety-related systems (CVS and SFW) and manual SG isolation

  (2) use of passive safety-related systems (PRHR, CMT and PCS) and automatic SG isolation

  (3) use of "feed and bleed" if the leak cannot be isolated (ADS, CMT, Accumulators, RNS, IRWST injection, PCS).

  For comparison, operating PWRs have two lines of defense: One is similar to AP600 design's first line of defense but uses safety-related systems (HPSI, AFW) and the other is manual "feed and bleed" using the pressurizer PORVs.

- Redundant means for reactor coolant inventory control:

  (1) automatic chemical and volume control system (CVS) injection at the upper end of the RCS pressure range

  (2) automatic CMT injection once an "S" signal is generated

  (3) manual ADS actuation to allow accumulator injection if CMT injection fails

- The improved reliability of the PRHR, as compared to the AFW system used in operating PWR plants, reduces the reliance on "feed and bleed" cooling as the last defense against core damage.

- The ADS provides an alternative decay heat removal path through primary "feed and bleed" which is much more reliable and faster than the high-pressure manual "feed and bleed" cooling of currently operating PWRs.

- Good capability for long-term recovery from unisolable SG leaks, which bypass the containment, exists by venting the RCS into the containment through the large ADS stage #4 valves to allow low-pressure core cooling by IRWST gravity injection and containment sump recirculation. The large IRWST capacity, combined with the capability to refill either the IRWST or the containment sump, prevents depletion of borated water through the open path that bypasses the containment and ensures the water level in the sump is adequate to establish recirculation by gravity.

- Steam generators have a secondary-side water inventory, which is larger than comparable operating plants extends the time available to recover feedwater or other means of core heat removal.

LOCA Sequences

The following are the most important features of the AP600 design which contribute to the reduction in the estimated CDF associated with LOCA sequences (CDF reduced to about 1.5E-07/yr from the 8E-05/yr to 1E-06/yr range corresponding to CDFs associated with LOCA at operating PWR reactors):

- Defense-in-depth, which provides several alternative means for coolant makeup, at both high and low pressures, using both safety and non-safety-related systems (CVCS pumps, CMTs, Accumulators, RNS, and IRWST injection) increases the reliability of the coolant makeup function. For comparison, most operating PWRs use CVCS pumps and HPSI pumps for high pressure injection while for low pressure injection accumulators and LPSI pumps are provided.

- Defense-in-depth, which provides several alternative means for core cooling during all possible scenarios and sizes of a LOCA accident, using both safety and non-safety-related systems increases the reliability of the core cooling function (both in the short and long term). Operating PWRS rely on fewer and less reliable alternative means for core cooling during LOCAs (e.g., manual “feed and bleed” as compared to automatic with manual backup “feed and bleed” capability of the AP600 design).

- The ADS provides an alternate decay heat removal path through primary "feed and bleed" which is much more reliable and faster than the high pressure manual "feed and bleed" cooling of currently operating PWRs.

- The AP600 design is expected to have a reduced frequency of LOCA initiators (breaks) as compared to operating PWR plants because the number of welds in the AP600 RCS pressure boundary was significantly reduced and "leak-before-break" was applied in the design of all piping larger than 3 inches.

ATWS Sequences

The following are the most important features of the AP600 design which contribute to the reduction in the estimated CDF associated with ATWS sequences (CDF reduced to 1E-08/yr from the 4E-05/yr to 1E-08/yr range corresponding to CDFs associated with ATWS at operating PWR reactors):

- The AP600 design has two redundant and diverse reactor trip systems. The non-safety-related DAS is a reliable system capable of initiating automatic and manual reactor trip via the motor-generator sets when the reactor fails to trip via the PMS. At operating reactors the DAS can not automatically initiate a reactor trip.

- The ADS allows use of the low-pressure injection systems (accumulators, RNS pumps, IRWST injection) for long-term reactivity control and core cooling when the charging pumps are unavailable. At operating reactors the less reliable PORVs must be used to allow low-pressure injection.

- Because the AP600 reactor uses a larger pressurizer than those at comparable operating plants, the frequency of ATWS precursors is reduced by increasing transient operation margins.

In the following sections, insights from the uncertainty analysis (Section 19.1.3.1.3) and from risk importance (Section 19.1.3.1.4) and sensitivity (Section 19.1.3.1.5) studies are presented.

19.1.3.1.3 Insights from the Uncertainty Analysis

Westinghouse performed an uncertainty analysis to determine the magnitude of uncertainties that characterize the level 1 PRA results (CDF from internal events) as well as the major contributors to these uncertainties. The AP600 CDF estimates, for internal events, are reported in terms of a mean value and an associated error factor (EF). The EF[1] is a measure of uncertainty that expresses the spread of a fitted log-normal distribution. The total CDF from internal events, as estimated by Westinghouse, has a mean value of about 2E-07/yr and an EF of approximately 5. Thus, the 95th and 5th percentiles are about 1E-06/yr and 4E-08/yr, respectively. It should be emphasized that only uncertainties associated with reliability and availability data were considered. Uncertainties associated with modeling (or lack of modeling) of accident sequences, system failure modes and human errors, were not included. The following conclusions can be reached from the results of the uncertainty analysis:

- The majority of the major contributors to the dominant accident sequences, and total CDF, have relatively small uncertainties associated with them.

[1]The "error factor" is the ratio between the 95th percentile and the median (50th percentile) of the assumed log-normal distribution (which is the same as the ratio between the median and the 5th percentile).

- The following are major contributors to the uncertainty associated with the plant CDF estimate:

  - LOCA initiating event frequencies, such as safety injection line break, LOCA breaks of all sizes (large, intermedium, medium and small) and CMT line break
  - reactor vessel failure probability
  - containment sump screen plugging probability (both single and common cause failures)
  - IRWST discharge line strainer plugging probability (both single and common cause failures)
  - CCF probability of hardware in the PMS engineered safety feature ESF input logic groups
  - CCF probabilities of several sensor groups, such as CMT level sensors, tank level transmitters, pressurizer level sensors, and sensors in high pressure environment
  - failure probability of the turbine impulse pressure transmitter (DAS trip permissive)
  - CCF probability of the reactor trip breakers to open (mechanical failure)
  - CCF of the reactor trip portion of PMS hardware or software (no signal to open the PMS reactor trip breakers)
  - failure probability of a motor-generator (M-G) set circuit breaker to open by DAS (mechanical failure)
  - failure probability of the automatic DAS function (hardware or software)

As a result of the lack of adequate data, the probability distribution function parameters associated with some risk-important events (e.g., software failures, CCF of explosive valves to operate and CCF of IRWST injection line check valves to open under small differential pressures) are rather subjective point estimates. The low confidence level in the point estimates (especially mean values) of such events, was addressed by the performance of sensitivity studies. The insights from these studies are discussed, together with insights from other sensitivity studies, in Section 19.1.3.1.5 of this report.

19.1.3.1.4 Insights from the Risk Importance Studies

Westinghouse performed studies to determine important contributors to risk as well as to maintaining the existing "designed-in" risk level. The staff, when necessary, used Westinghouse's PRA results to perform additional risk importance studies to gain more complete insights. Such studies address the following two general objectives: (1) risk reduction, and (2) safety or reliability assurance. The first objective, i.e., risk reduction, was

achieved by the identification and ranking of dominant contributors to risk in order to identify areas in which the plant risk can be reduced by design and/or operational changes. The second objective, i.e., reliability assurance, was achieved by the identification of dominant contributors to maintaining the "built-in" risk level (to ensure that risk does not increase and is as low as the PRA indicates it is). To meet these two objectives, Westinghouse used the following two risk importance measures to rank systems, structures, components (SSCs) and human actions:

- Risk Reduction Worth that gives the factor by which the core damage frequency decreases when an SSC or human action is assumed to be perfectly reliable (perfect component or no error). Provides indication of existing margin for improvement.

- Risk Achievement Worth that gives the factor by which the core damage frequency increases when an SSC or human action is assumed not to be there or to be failed (event probability is assumed to be 1). Provides indication of the importance of maintaining the existing reliability.

The "risk achievement worth" importance measure is useful in identifying SSCs for which it is particularly important to do good maintenance, since poor reliability/availability of this equipment would significantly increase the CDF estimate. The "risk reduction worth" importance measure is useful in identifying SSCs which would benefit the most from improved testing and maintenance by minimizing equipment unavailability and failures.

Risk importance studies were performed at both the system and component level. The major insights drawn from the importance analysis are summarized below:

- The most important systems for core damage prevention or, equivalently, the systems that are the most "worthy" in achieving the low CDF level assessed in the PRA (i.e., systems with the highest "risk achievement worth"), are the protection and safety monitoring system (PMS), the Class 1E dc power, the ADS, containment sump recirculation, gravity injection from the IRWST, the CMTs and the accumulators.

- Events that would decrease significantly the "built-in" reliability, i.e., those with highest "risk achievement worth," are hardware common-cause failures and software errors. This is attributable to the redundancy and diversity of the AP600 safety systems, which ensure that single independent hardware faults are not among those events whose occurrence would have a large impact on the CDF from internal events.

- Common-cause failure of the following sets of components was found to have a large impact on the estimated CDF from internal events (i.e., sets of components with highest "risk achievement worth"):

    - Containment recirculation line components, such as the explosive (squib) valves, and sump screens (plugging). If both recirculation lines are unavailable due to a CCF and the plant keeps operating at power, the plant CDF would increase by almost four orders of magnitude.

- IRWST gravity injection components, such as squib valves, check valves and tank discharge line strainers (plugging). If both IRWST injection lines are unavailable because of a CCF and the plant keeps operating at power, the plant CDF would increase by about three orders of magnitude.

- PMS ESF hardware components, such as output drivers and input logic groups (hardware). If such components are unavailable because of a CCF and the plant keeps operating at power, the plant CDF would increase by about three orders of magnitude.

- ADS stage #4 explosive (squib) valves. If these valves become unavailable to open when demanded because of CCF and the plant keeps operating at power, the plant CDF would increase by about three orders of magnitude.

- PMS reactor trip components, such as reactor trip breakers and reactor trip logic hardware. If such components become unavailable to operate when demanded because of CCFs and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

- CMT sensors and sump level heated RTD sensors. If such components become unavailable to operate when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

- CMT and accumulator components, such as CMT AOVs, CMT check valves, and accumulator check valves. If such components become unavailable to operate when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

- Tank level transmitters (IRWST, BAT), sensors in high pressure environment, and pressurizer level sensors. If any of these sets of components become unavailable to operate as designed when demanded because of CCFs and the plant keeps operating at power, the plant CDF would increase by about two orders of magnitude.

- Reactor coolant pump (RCP) breakers. If the RCP breakers become unable to open to trip the RCPs and the plant keeps operating at power, the plant CDF would increase by almost two orders of magnitude.

- Class 1E dc batteries. If the plant operates without Class 1E batteries, the plant CDF would increase by over one order of magnitude.

- PRHR AOVs. If both such AOVs become unable to open and the plant keeps operating at power, the plant CDF would increase by over one order of magnitude.

• The AP600 relies on digital I&C systems which are complex combinations of hardware and software (i.e., computer programs) components. Although computer software does not wear out, as hardware does, it could fail because of the excitation of residual design

errors when a particular combination of inputs occurs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a common mode software failure in all channels (or divisions) at the same time, i.e., it would be a CCF of redundant channels or divisions. The following types of software error were found to have a large impact on the estimated CDF (i.e., highest "risk achievement worth"):

- Software for the PMS and PLS logic cards. This type of CCF accounts for potential design errors in "common functions" software (i.e., software controlling fundamental processor functions, such as I/O, processing and communications). Because such functions, and its associated software, are repeated across all major subsystems of PMS and PLS, such software design errors could impact the reactor trip and ESF portions of PMS as well as all the PLS functions (and fail both their automatic and manual functions). If a software fault of this kind existed and showed up every time an accident occurred without being detected, the plant CDF would increase by more than four orders of magnitude. (In reality residual software faults do not show up, and thus they do not cause a software failure, unless the program is exposed to an environment for which it was not designed or tested).

- PMS ESF software components, such as input logic software, output logic software and actuation logic software. This type of CCF accounts for potential design errors in "application" software (i.e., software controlling the actual algorithms, protective and actuating functions that the PMS is designed to provide). Because a different application software controls each major PMS subsystem, this type of software CCF is contained within subsystems performing same or similar functions. If a software fault of this kind existed and showed up every time an accident occurred without being detected, the plant CDF would increase by about three orders of magnitude.

- PMS ESF manual input multiplexer software. If the plant is operated with a fault in the multiplexer software which is assumed to fail the function of the multiplexer during an accident, the plant CDF would increase by over one order of magnitude.

- The AP600 design is significantly less dependent on human actions for safety than operating reactors. If operators always failed to perform the human actions modeled in the PRA, the plant CDF would increase by about two orders of magnitude (from 2E-07/yr to 2E-05/yr). Operator failure to perform the following actions was found to have the largest impact on the estimated CDF from internal events (i.e., operator actions with highest "risk achievement worth"):

  - diagnose an SGTR event

  - manually actuate containment sump recirculation when automatic actuation fails

- manually actuate ADS for "feed and bleed" cooling when automatic actuation fails
- perform a controlled shutdown to control and mitigate an RCS leak event

- Westinghouse identified the following operator actions in the Level 2 analysis as important to large release frequency on the basis of sensitivity/importance analyses:
  - diagnose and actuate the ADS after core damage to prevent RPV failure or temperature-induced SGTR (LPM-REC01 and ADN-REC01)
  - diagnose and actuate the ADS after core damage in SGTR events to terminate releases from containment (PDS6-MANADS)
  - open recirculation valves to flood the reactor cavity (REN-MAN03)
  - actuate the hydrogen igniter system (VLN-MAN01)

- Failure of the following single components was found to have a significant impact on the estimated CDF from internal events (i.e., single components with highest "risk achievement worth"):
  - plugging of one IRWST discharge line strainer (important for a safety injection line break which disables one of the two redundant IRWST injection lines)
  - non-class 1E dc distribution panel EDS3 EA 1 (supplies power to DAS which is important for ATWS sequences)
  - plugging of the CMT flow tuning orifice
  - plugging or leak in the PRHR heat exchanger
  - CMT injection check valves
  - Class 1E dc switchboard DS1 and distribution panel DD1

- Failures of components associated with the following events were found to be major contributors to the estimated CDF from internal events ( i.e., they have the highest "risk reduction worth"):
  - initiating events, such as LOCAs (large, safety injection line break, intermediate, and medium), reactor vessel rupture, ATWS precursor with no MFW and SGTR.
  - CCF of the four explosive (squib) valves in both sump recirculation lines to open
  - failure of an IRWST discharge line strainer (plugged)
  - CCF of PMS ESF input logic groups (hardware)

- CCF of the four check valves in the two IRWST discharge lines
- CCF of the four explosive (squib) valves in the two IRWST discharge lines
- CCF of the IRWST level transmitters
- CCF of CMT AOVs to open
- CCF of ADS stage #4 explosive (squib) valves to operate on demand
- CCF of CMT injection check valves to open
- CCF of accumulator check valves to open

- Operator failure to perform the following actions were found to be significant contributors to the estimated CDF from internal events; (i.e., these actions have the highest "risk reduction worth"):
  - manually trip the reactor via PMS or DAS within one minute (given automatic trip failed)
  - manually actuate containment sump recirculation (when automatic actuation fails)
  - manually step-in the control rods within one minute, given automatic and manual scram failure
  - manually actuate safety systems through DAS, given failure to do so through PMS

The risk importance of non-safety-related "defense-in-depth" systems, credited in the AP600 PRA, was also assessed. The major insights gained from such studies are summarized below:

- If the DAS becomes unavailable and the plant continues operating at power, the plant CDF would increase about 40 times.
- If the RNS becomes unavailable and the plant continues operating at power, the plant CDF would increase about four times.
- If the SFW becomes unavailable and the plant continues operating at power, the plant CDF would increase about two times.
- If both diesel generators become unavailable and the plant continues operating at power, the plant CDF would increase about two times.
- If all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase by about two orders of

magnitude (from 2E-07/yr to about 1E-05/yr). Most of the contribution to such an increase in CDF is associated with transient and ATWS sequences.

- The DAS is very important in reducing the CDF associated with transient initiators (such as loss of main feedwater, loss of condenser and loss of component cooling water) and ATWS events. If all non-safety-related "defense-in-depth" systems with the exception of DAS become unavailable and the plant continues operating at power, the plant CDF would increase by less than one order of magnitude (from 2E-07/yr to about 1E-06/yr).

As mentioned above, details on SSCs and human actions that were found to be risk significant by the applicant are documented in Chapter 50 of the AP600 design PRA (for internal events at power operation). This information was integrated with similar information from external events and shutdown risk analyses as well as information from the containment and offsite consequences analyses (levels 2 and 3 of the PRA) to form the basis for the following two lists:

(1) a list of important SSCs which the COL applicant should incorporate in the D-RAP program. This was identified as COL Action Item 19.1.3.1-1 in the DSER. Westinghouse included such a list of important SSCs in Chapter 17.4 of the SSAR.

(2) a list of risk-important operator tasks which should be taken into account in the control room design as well as for implementing procedures and developing training programs. This was identified as COL Action Item 19.1.3.1-2 in the DSER. This list should be taken into account by the COL applicant in developing and implementing procedures, training and other human reliability related programs. Chapter 18 of the SSAR discusses the use of such information in developing and implementing procedures, training and other human reliability related programs for the plant.

Westinghouse, in performing the Level 1 PRA for internal events at power operation, identified the following examples of risk-important tasks (with their PRA designators inside the parentheses), which must be performed by the operator to prevent or mitigate severe accidents. These tasks, documented also in WCAP-14651, should be taken into account in the control room design. The process for inclusion of these tasks is addressed in Section 18.7 of this report.

- Operator fails to manually actuate ADS (ADN-MAN01)
- Operator fails to manually trip reactor via PMS within one minute (ATW-MAN03)
- Operator fails to manually trip reactor via DAS (ATW-MAN04C)
- Operator fails to manually trip reactor via PMS within five minutes (ATW-MAN05)
- Operator fails to diagnose a SGTR event (CIB-MAN00)
- Operator fails to isolate failed SG (CIB-MAN01)
- Operator fails to recognize need for manual depressurization during a small LOCA or transient event (LPM-MAN01)

- Operator fails to recognize need for manual depressurization during a medium LOCA (LPM-MAN02)
- Operator fails to actuate a system using DAS only (REC-MANDAS)
- Operator fails to actuate containment sump recirculation when automatic actuation fails as a result of IRWST level signal failure (REN-MAN04)
- Operator fails to perform controlled shutdown (OTH-SDMAN)

Additional risk-important operator tasks related to shutdown operation and to containment performance (Level 2 PRA) are reported in Section 19.1.4.5 and Section 19.1.3.2, respectively.

In designing the AP600 control room, it is important that no new significant human errors be introduced. To this end, during the main control room validation process, the COL applicant should qualitatively confirm that the "findings" from the integrated system validation do not lead to a risk-significant increase in error potential over that represented in the AP600 PRA HRA. If this is not confirmed, the COL applicant should model the additional risk-significant errors in an updated HRA. This is COL Action Item 19.1.3.1-3.

19.1.3.1.5 Insights from the Sensitivity Studies

Westinghouse performed several sensitivity studies to gain insights about the impact of uncertainties (and potential lack of detailed models) on the estimated CDF. The staff used Westinghouse's PRA results to perform additional sensitivity studies to gain more complete insights when it was necessary. The sensitivity studies performed by the applicant and the staff, have the following objectives:

(1) determine the sensitivity of the estimated CDF from internal events to potential biases in numerical values, such as initiating event frequencies, failure probabilities, and equipment unavailabilities

(2) determine the impact of potential lack of modeling details, such as long-term cooling with the PRHR following a transient or a LOOP/SBO event, on the estimated CDF from internal events

(3) determine the sensitivity of the estimated CDF to previously raised issues, such as passive system check valve reliability

In addition, sensitivity studies were performed to investigate the impact of uncertainties on PRA results under the assumption of plant operation at power without credit for the non-safety-related "defense-in-depth" systems ("focused" PRA model). These studies provided additional insights about the risk importance of the "defense-in-depth" systems which were taken into account in selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process. Insights related to CDF are reported in this section while similar insights related to large release frequency and conditional containment failure probability (CCFP) are reported in Section 19.1.3.2.

19.1.3.1.5.1 Sensitivity to Potential Biases in Numerical Values

Results of studies to determine the sensitivity of the estimated CDF from internal events to potential biases in numerical values, such as failure probabilities, are summarized below.

Explosive (Squib) Valve Reliability

Squib valves are used in all ADS stage #4 lines, all IRWST injection lines and all containment sump recirculation lines. Because of the lack of adequate data for the AP600 squib valves and uncertainties in the extrapolation of data from other designs and sizes to AP600 operating conditions, there is uncertainty in the mean value of the failure probability of a squib valve to operate. Increasing the failure probability by a factor of five (i.e., the value recommended in EPRI's URD), the CDF would increase by about a factor of two. This indicates some sensitivity of the CDF to reasonable increases of the mean value of the failure probability of squib valves used in the PRA but not large enough, by itself, to impact PRA conclusions and insights about the design.

Circuit Breaker Reliability

The most important circuit breakers (CBs) modeled in the AP600 PRA are the reactor trip, the motor-generator (M-G) set trip, and the RCP trip CBs. Failure to open any of several sets of four reactor trip CBs causes failure of reactor trip through the PMS. Failure to open both M-G set trip CBs causes failure of the alternate means of tripping the reactor through DAS. Failure of any of several sets of RCP CBs causes failure of one or more RCPs to trip following an accident initiating event and potential failure of CMT injection and ADS automatic actuation. There is uncertainty in the mean values of the failure probabilities of CBs to open used in the AP600 PRA. The uncertainty is the result of the use of failure rates for CBs to open on demand that are lower than generic failure rates, the linear extrapolation of failure rates to longer testing intervals and potential approximations in calculating CCF probabilities. A sensitivity study was performed to assess the impact of this uncertainty on PRA results and insights.

- Increasing the CB failure to open probabilities used in the AP600 PRA by an order of magnitude, the CDF would increase by about a factor of three. This indicates some sensitivity of the CDF to reasonable increases in the mean value of the failure probabilities of CBs to open on demand but not large enough, by itself, to impact PRA conclusions and insights about the design.

- Increasing the CB failure to open probabilities used in the AP600 PRA by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase about 150 times from 2E-07/yr to about 3E-05/yr (based on risk importance study results, unavailability of the non-safety-related systems alone would increase the plant CDF by about two orders of magnitude). This indicates that if the plant is operating without the non-safety-related "defense-in-depth" systems, the CDF is sensitive enough to reasonable increases in the mean values of CB failure to open probabilities used in the PRA to impact PRA conclusions and insights about the design (e.g., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

- Increasing the CB failure to open probabilities used in the AP600 PRA by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems, with the exception of DAS, become unavailable and the plant continues operating at power, the plant CDF would increase by about one order of magnitude (from 2E-07/yr to about 2E-06/yr). Since the unavailability of the non-safety-related systems alone would increase the plant CDF by about a factor of five (based on risk importance study results), the plant CDF is not as sensitive to reasonable increases in the mean values of CB failure to open probabilities used in the PRA when the plant is operating without all non-safety-related "defense-in-depth" systems but DAS. This underlines the importance of the reactor trip function of DAS in reducing the impact of uncertainties associated with CB failure probabilities on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

Digital I&C System Software Reliability

Digital I&C systems are designed as complex combinations of hardware and software (i.e., computer programs) components. Although computer software does not wear out, as hardware does, it can fail as a result of the excitation of residual design errors when a particular combination of inputs occurs. If one could eliminate all the design errors before a software product is put in operation, it would work perfectly forever. However, it is impossible to be certain that a software product is error free. On the contrary, experience shows that there are always residual faults which do not manifest themselves, and thus they do not cause a software failure unless the program is exposed to an environment for which it was not designed or tested. Exposure to such an environment is possible because, as a result of the large number of possible states and inputs in most software programs, it is extremely difficult to perfectly comprehend program requirements and implementation and it is virtually impossible to test more than a small subset of all possible input combinations during development. Thus, software reliability is essentially a measure of the confidence one has in the design of the software and its ability to function properly in its expected environment.

Quantification of software reliability may be too difficult, especially for software which must meet high reliability requirements such as those used in the AP600 design. This is as a result of the random nature of a large number of possible inputs, the unknown mechanisms of human failure which create errors during the development process, and the randomness of the testing process used to detect errors. However, regardless of whether the reliability of software can be accurately quantified, the design goal must be to minimize the number of residual errors, their frequency of occurrence, and their effect on system performance. This can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program. For these reasons, each software product is unique and extrapolation of statistical data for other products is meaningless.

From the basic properties of software it follows that commonly used hardware redundancy techniques do not improve software reliability. The several defense mechanisms against hardware CCFs that are incorporated in the design (such as redundancy, separation, operational testing, maintenance, and immediate detectability of failure provided by the on-line diagnostics) cannot be relied upon to prevent software CCFs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a

common mode software failure in all channels (or divisions) at the same time, i.e., it would be a CCF of redundant channels or divisions. Thus, a highly reliable software product is needed whenever the same program is executed in two or more channels (or divisions) in parallel. Since the reliability of a software product is basically determined during development and testing, the importance of the software development process in achieving high reliability cannot be overestimated.

Although it is not easy to quantify software reliability, it is generally accepted that high reliability can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program. The AP600 design PRA assumes high reliability for all software used in the digital I&C systems. Westinghouse expects to develop highly reliable software for the AP600 I&C systems by setting reliability goals and design requirements and by incorporating features in the software design which act as "defenses" against CCFs. Such requirements and design features include the following four items:

(1) requirements for formalized design phases, for following design standards and for performing formal design reviews

(2) requirement for an expected use-based software testing/verification program

(3) incorporation of "fail safe" capability in the design, i.e., incorporation of mechanisms (independent of the source of error) for detecting errors at the module or intermediate level and producing a well defined output which results in an application specific safe action

(4) incorporation of "functional diversity" which allows initiation of automatic protection functions even when errors associated with some plant parameters are present (different plant parameters initiate same automatic protection function independently)

A sensitivity study was performed by the staff, using Westinghouse's PRA models and results, to assess the impact of uncertainty in the mean value of software failure probabilities used in the AP600 PRA on PRA results and insights. The major findings of this study are summarized below:

- Increasing software failure probability by an order of magnitude, the CDF would increase by about 40 percent (from 2E-07/yr to 2.8E-07/yr). This indicates a rather small sensitivity of the plant CDF to reasonable increases in the mean values of software failure probabilities used in the PRA.

- Increasing software failure probability by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase by about three orders of magnitude from 2E-07/yr to almost 1E-04/yr. (Based on risk importance study results, unavailability of the non-safety-related systems alone would increase the plant CDF by about two orders of magnitude). This indicates that if the plant is operating without the non-safety-related "defense-in-depth" systems, the CDF is sensitive enough to reasonable increases in the mean values of software failure probabilities used in the PRA to impact PRA conclusions and insights about the design

(e.g., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

- Increasing software failure probability by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems, with the exception of DAS, become unavailable and the plant continues operating at power, the plant CDF would increase by about one order of magnitude (from 2E-07/yr to about 2E-06/yr). Since the unavailability of the non-safety-related systems alone would increase the plant CDF by about a factor of five (based on risk importance study results), the plant CDF is not as sensitive to reasonable increases in the mean values of software failure probabilities used in the PRA when the plant is operating without all non-safety-related "defense-in-depth" systems but DAS. This underlines the importance of the engineered safety features (ESF) actuation function of DAS in reducing the impact of uncertainties associated with software failure probabilities on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

19.1.3.1.5.2 Sensitivity to Potential Lack of Modeling Details

Results of sensitivity studies performed to determine the impact of potential lack of modeling details on the estimated CDF from internal events are summarized below.

Modeling Sump Recirculation in a Safety Injection Line Break Accident

In modeling a safety injection (SI) line break accident in the PRA, it was assumed that success of recirculation through the containment sump recirculation lines is not needed since the same function can be performed by the pipe break. However, when the pipe break occurs in one of three valve compartments inside the containment, success of recirculation through the containment sump recirculation lines is needed. A sensitivity study has shown that the impact of this modeling assumption on the estimated CDF is rather small (the plant CDF from internal events would increase by about 15 percent if sump recirculation were assumed to be always needed following a SI line break).

Modeling Spurious Actuation of Squib Valves

Westinghouse assessed contributions of spurious ADS valve actuation, caused by faults in I&C systems (PMS and DAS), to the various LOCA initiating event frequencies. This assessment, however, did not include faults in I&C copper cables (e.g., hot shorts) from the protection logic cabinets (PLCs) to the squib valve operators. A hot short in one of these cables could increase the current to the value that causes detonation of the squib valve operator. It was assumed in the AP600 PRA that the frequency and impact on PRA results of this spurious actuation mechanism is very small, except in the presence of a fire. According to Westinghouse, spurious actuation of squib valves as a result of hot shorts, caused by cable insulation degradation or mechanical damage and the presence of humidity, is expected to be a very low frequency event for nuclear plant safety-grade cabling.

A study performed by the staff, using Westinghouse's PRA models and results, underlined the importance of incorporating features in the design of ADS cabling which will minimize the

probability of hot shorts actuating an ADS squib valve. Westinghouse responded by incorporating additional features in the AP600 design which further reduce the likelihood of spurious actuation of a squib valve, such as using a valve controller circuit which requires multiple hot shorts for actuation and physical separation of potential hot short locations.

Modeling of ATWS Accidents with MFW Initially Available

If MFW is initially available when an ATWS event occurs, no unfavorable exposure time (UET) was modeled in the ATWS accident sequences. This implies that the RCS pressure will be contained within safe levels (i.e., below 3200 psig) even in the presence of an adverse moderator temperature coefficient (as is the case at the beginning of the fuel cycle) and without any pressure relief through the pressurizer safety valves. Because of concerns regarding this modeling assumption, the staff performed a sensitivity study to assess the potential impact on PRA results and insights. In the sensitivity study it was conservatively assumed that the plant responds to all ATWS precursors in the same way it responds to a loss of MFW event.

This sensitivity study has shown that the impact of this modeling assumption on the estimated CDF is rather small (the plant CDF from internal events would increase by less than 20 percent if it were assumed that the plant responds to all ATWS precursors in the same way it responds to a loss of MFW event). In addition, this sensitivity study indicated that this modeling assumption does not impact PRA conclusions and insights about the design.

19.1.3.1.5.3 Sensitivity to Previously Raised Issues

Results of studies performed to determine the sensitivity of the estimated CDF to previously raised issues are summarized below.

Check Valve Reliability

The applicability of generic failure data to check valves (CVs), present in several passive safety systems of the AP600 design, has been an issue in the AP600 PRA review. While CVs are not unique to the AP600, the conditions under which they will be operating in the plant are different from those in current generation nuclear plants. Such CVs will have to open under very low differential pressures (created by the gravity driving head only) after long periods of being held closed (tested every 2 years at refueling) in the presence of stagnant borated water. To account for "less than ideal conditions" which may exist at the time the valves are demanded, EPRI has recommended ("Advanced Light Water Reactor Utility Requirements Document", Volume III, ALWR Passive Plant) increasing the standby failure rate of check valves in passive systems by a factor of five as compared to CVs in "pumped" systems used in operating reactor designs. Westinghouse, however, did not use the higher failure rate recommended by EPRI in the AP600 PRA. This is justified, according to Westinghouse, because the CVs used in the IRWST injection lines, which are the most risk-important check valves in the AP600 design, have two important features which compensate for the above-mentioned adverse conditions. First, contrary to most CVs at operating nuclear power plants, the gate and seat design of these CVs allows for small leaks and makes them less susceptible to binding or sticking when they are closed. Second, because of the presence of the squib valves, there is no pressure holding the IRWST injection CVs closed which could force the disk to stick in the seat. The staff agrees that these features most likely improve CV reliability. However, Westinghouse did not submit data or analyses that could be used to show to what degree such features "compensate" for the

adverse operating conditions of the AP600 CVs (i.e., having to open under very low differential pressures after long periods of being held closed in the presence of stagnant borated water).

Another issue on CVs, which became apparent during the AP600 PRA review, involves common cause failure (CCF) histories at operating reactors and their applicability to AP600 CVs. The CCF probabilities of check valves, assumed in the AP600 PRA, are based on information provided in the last revision (Revision 6) of EPRI's "Utility Requirements Document" (URD). The information on CCF of check valves, as revised in the last revision of EPRI's URD, leads to a decrease by about an order of magnitude in the value of CCF probability recommended in previous URD revisions which was used in previous PRAs for evolutionary designs and operating reactors. According to Westinghouse, this is a result of better understanding of individual events involving failure of check valves at nuclear power plants and that "EPRI found no common cause failures to open of check valves (other than failure modes unique to testable check valves)." An NRC-sponsored evaluation of LER and NPRDS events (see Common-Cause Failure data Collection and Analysis System, INEL-94/0064, December 1995), which occurred between 1980 and 1993 at operating nuclear power plants, has found about 20 events involving common cause failure of check valves. Although it can be argued that only a portion of such events are applicable to the AP600 design, the staff believes that there is still significant uncertainty in the data used to calculate CCF probabilities of CVs in the AP600 PRA.

A sensitivity study was performed by the staff using Westinghouse's PRA models and results. The study assessed the impact of uncertainties associated with the CV failure rate and the common cause failure data, assumed in the AP600 PRA, on PRA results and insights. The major finding of this study are summarized below:

- increasing the CV failure rate by a factor of 5, as recommended by EPRI, would increase the CDF by about 60 percent

- increasing the CV common cause failure multiplier by an order of magnitude, as in previous PRAs, would increase the CDF by a factor of 3

- increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV common cause failure multiplier by an order of magnitude (as in previous PRAs), would increase the CDF by over an order of magnitude (from 2E-07/yr to over 2E-06/yr)

- Increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV common cause failure multiplier by an order of magnitude (as in previous PRAs), and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase by almost two orders of magnitude (from 2E-07/yr to almost 2E-05/yr).

- Increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV common cause failure multiplier by an order of magnitude (as in previous PRAs) and at the same time assuming that all non-safety-related "defense-in-depth" systems with the exception of DAS become unavailable and the plant continues operating at power, the plant CDF would increase about 15 times (from 2E-07/yr to about 3E-06/yr). If, in addition to the above changes, the explosive valve failure rate is also increased by a

factor of 5 (as explained in above mentioned study), the CDF would increase about 20 times (from 2E-07/yr to about 5E-06/yr).

- Increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV common cause failure multiplier by an order of magnitude (as in previous PRAs) and at the same time assuming that all non-safety-related "defense-in-depth" systems with the exception of DAS and the normal residual heat removal system (RNS) become unavailable and the plant continues operating at power, the plant CDF would increase by almost one order of magnitude (from 2E-07/yr to almost 2E-06/yr). Such an increase in CDF is not affected significantly when the failure rate for the explosive valves is also increased by a factor of five. This indicates that the availability of RNS significantly reduces the impact of uncertainties associated with failure probabilities of check valves and explosive (squib) valves on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

Intersystem CCF of Check Valves

No CCFs of check valves belonging to different systems, such as CMTs and accumulators, have been modeled in the AP600 PRA. A sensitivity study was performed by the staff, using Westinghouse's PRA models and results, to assess the impact of potential intersystem CCF of CVs on PRA results and insights. The major findings are summarized below.

- The plant CDF increases by about 25 percent when intersystem CCF of CVs is considered, with CCF of CMT and accumulator CVs being the dominant contributor.

- The plant CDF increases by over one order of magnitude (from 2E-07/yr to over 2E-06/yr) when intersystem CCF of CVs is considered and the probability of such CCF is based on the higher failure rate (increased by a factor of 5) and the higher common cause failure multiplier (increased by an order of magnitude) used in the above sensitivity study concerning CV reliability.

- Intersystem CCFs of CVs add significantly to both the CDF and the LRF of the plant, if the plant operates at power without the non-safety-related "defense-in-depth" systems.

Westinghouse addressed this issue by using different types of CVs in the CMT lines from the CVs used in the accumulator lines. The accumulator CVs are swing disk type (similar to current plants) and are normally closed. The CVs in the CMT lines are tilt disk type and are normally open (biased open, closed on back flow). Since the largest impact is related to CCF of CVs in these two systems, the diversity between the CMT CVs and accumulator CVs minimizes (or eliminates) the concern associated with intersystem CCF of CVs.

Success Criteria for Full Depressurization

A sensitivity study was performed to investigate the impact of potential uncertainties in the success criteria for full RCS depressurization (minimum number of stage #4 ADS paths required to open) on the plant CDF. The success criterion, used in the PRA, requiring the successful opening of at least 2 of the 4 stage #4 squib valves for full depressurization to allow IRWST injection, was changed to require opening of at least 3 squib valves. This resulted in a

rather small increase in the plant CDF (smaller than 10 percent). The study has further indicated that this holds true even when the plant is operating at power without all non-safety-related "defense-in-depth" systems. This finding indicates the plant CDF is not sensitive to reasonable uncertainties in the success criteria used in the PRA for ADS full depressurization.

Motor Operated Valve Reliability

A sensitivity study, performed by the staff based on Westinghouse PRA models and results, indicated that the AP600 CDF from internal events is not very sensitive to reasonable increases in motor operated valve (MOV) failure rates. This result shows that the AP600 design is not very sensitive to the concern that generic MOV failure rates may have been underestimated.

Mission Times for Systems Providing Long-Term Cooling

Westinghouse assumes, in the PRA, a mission time of 24 hours for long-term cooling independent of plant condition. The staff identified the following four categories of accident sequences that require long-term (beyond 24 hours) operator actions and/or system operation, and which could impact PRA results and insights about the design:

(1) LOCA sequences with impaired containment (no long-term recovery actions to replenish lost inventory were modeled)

(2) transient non-LOOP sequences with the PRHR available (no long-term recovery actions and system failures needed to replenished the lost inventory, as a result of boiling in the IRWST and failure to return the condensate back to the IRWST, or to depressurize the plant and continue core cooling by recirculation were modeled)

(3) LOOP sequences (an operator decision to block automatic depressurization and continue cooling the core with the PRHR if ac power is lost for 22 hours was not modeled)

(4) sequences with an open path outside containment (the potential need to replenish the lost IRWST or sump inventory was not modeled)

Westinghouse responded to these concerns by performing the following activities:

- changing the design to include a reliable safety-related IRWST gutter system for returning the inventory lost by boiling back to the IRWST

- developing emergency response guidelines (ERGs) for long-term operator actions.

A sensitivity study performed by the staff has shown that the impact of this issue on the estimated CDF is rather small (the plant CDF from internal events would increase by about 5 percent if long-term operator and/or system failures were included in the PRA models). In addition, the sensitivity study indicated that this issue does not have a significant impact on PRA conclusions and insights about the design.

19.1.3.1.5.4 Summary of Major Insights from the Sensitivity Studies

The most important insights from the sensitivity studies are summarized below:

- The estimated CDF from internal events is very sensitive to several CCF probabilities. This underlines the importance of those design features and operational requirements which prevent common cause failures, namely divisional separation, diversity of redundant components, as well as appropriate maintenance and training programs.

- The AP600 CDF from internal events is not very sensitive to reasonable changes in single component failure probabilities or initiating event frequencies.

- The estimated CDF is not sensitive to further reductions in safety system outage times for test and maintenance during power operation or to further reductions in human error probabilities.

- Uncertainties associated with failure probabilities of reactor trip components, such as circuit breakers, could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the reactor trip (RT) function of DAS provides an efficient means for minimizing the impact of such uncertainties on PRA conclusions and insights about the design.

- Uncertainties associated with failure probabilities of ESF actuation components, such as software, could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the ESF actuation function of DAS provides an efficient means for minimizing the impact of such uncertainties on PRA conclusions and insights about the design.

- Uncertainties associated with failure probabilities of passive system check valves and explosive (squib) valves could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the RNS reduces significantly the impact of such uncertainties on PRA conclusions and insights about the design.

- Diversity between the CMT and accumulator CVs minimizes the impact of intersystem CCF of CVs on PRA conclusions and insights about the design.

- A reduction in the effectiveness of features incorporated into the design of ADS cabling to minimize the probability of hot shorts actuating an ADS squib valve could have a significant impact on PRA insights and conclusions.

- PRA conclusions and insights about the AP600 design are not very sensitive to reasonable uncertainties in the success criteria used in the PRA for ADS full depressurization.

- PRA conclusions and insights about the AP600 design are not very sensitive to the concern that generic MOV failure rates may have been underestimated.

The insights from the sensitivity studies were integrated with insights from the uncertainty analysis and the risk importance studies and were used, in conjunction with the assumptions made in the PRA, to identify the design certification requirements reported in Section 19.1.8.

19.1.3.2 Results and Insights from the Level 2 PRA (Containment Analysis)

In the sections that follow, results and insights from the Level 2 portion of the PRA are presented. This includes the frequency of the various accident classes considered in the Level 2 analysis, the frequency and conditional probability of containment failure, a breakdown of containment failure frequency in terms of important containment failure/release modes, and a summary of the risk-significant insights from the Level 2 PRA and supporting sensitivity analyses.

19.1.3.2.1 Core Damage Sequences and Accident Classes Contributing to Containment Failure

In the AP600 PRA, the end states of the Level 1 system event trees (core damage sequences) are binned into 11 accident classes on the basis of initiating event and RCS conditions at the onset of core damage. The definition of each accident class is provided in Table 19.1-2, along with the representative RCS pressure at the onset of core damage, and the core damage frequency assigned to the class in the baseline PRA for internal events at power.

The majority of Level 1 sequences (about 85 percent) involve events with at least partially successful RCS depressurization, and relatively low RCS pressure (<150 psig) at the time of core uncovery. For high pressure core melt sequences, the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary is further evaluated in the Level 2 event tree. Thus, an even larger fraction of the core melt sequences (about 93 percent) is estimated to involve a depressurized RCS at the time of RCS pressure boundary challenge.

Accident class frequencies are propagated through the containment event tree (CET) to evaluate the potential for operator actions, safety system response, and the containment structure to mitigate the release. The CET includes top events/nodes that address the following:

- RCS depressurization after core uncovery
- containment isolation
- reactor cavity flooding (by gravity draining or manual actuation)
- reactor vessel reflooding and associated hydrogen production
- reactor vessel integrity
- passive containment cooling
- hydrogen igniter system availability
- diffusion flames at IRWST and valve vault exits
- early hydrogen detonation (during hydrogen release to containment)

- global deflagration
- intermediate hydrogen detonation (after hydrogen is mixed in containment)

The CET is quantified separately for each accident class. For system related top events, split fractions are quantified by linking to the system fault trees (i.e., top events for RCS depressurization, containment isolation, reactor cavity flooding, and hydrogen igniter system). For the balance of the top events, split fractions are assigned scalar values based on a characterization of the underlying processes/phenomena.

Each end state of the CET is assigned to one of six containment release categories (RC). Westinghouse considered all containment release/failure categories except intact containment (IC) to constitute a large release, which is conservative. As such, the LRF reported in the PRA is equivalent to the core damage frequency less the frequency of the IC RC. The conditional containment failure frequency for each accident class is presented in Table 19.1-3 for the baseline PRA for internal events at power. The conditional containment failure probability for accident classes 1A, 1AP, 3A, and 6 (33 to 97 percent) is considerably higher than other classes because of failure of late depressurization in these sequences, which leads directly to containment bypass. The conditional containment failure probability for accident classes 3BL and 3BR (0.2 percent) is lower than other classes (e.g., 3BE and 3D/1D) because reactor cavity flooding occurs as a consequence of gravity draining in these accident classes. In contrast, 3BE and 3D/1D sequences require manual actuation of the cavity flooding system, with a typical failure probability of about 0.05.

The frequencies of the various containment release categories and the fractional contributions by release category to the total large release frequency are presented in Figure 19.1-1 and Table 19.1-4. The leading contributors to the various release classes are discussed further in Section 19.1.3.2.2 of this report.

19.1.3.2.2 Leading Contributors to Containment Failure from the Level 2 PRA

Comparison of the results presented in the original and the updated PRA (Revision 9) shows that resolution of the issues raised in the DSER have resulted in substantive changes in the treatment of severe accident challenges and a reordering of leading contributors to containment failure and risk. However, the CCFP and overall risk for the AP600 design remain acceptably low as discussed in Section 19.2.4 of this report.

The contributions to total release frequency are significantly changed relative to the original PRA. The breakdown of results from the updated PRA reveals that about 11 percent of the core damage events result in large release/containment failure. Similar to the original PRA, the bulk of these releases (about 62 percent) involve containment bypass. Early containment failures, which were a relatively small contributor in the original PRA, account for about 36 percent of the containment failure frequency in the updated PRA. Containment isolation failure contributes about 2 percent in the updated PRA, compared to 15 percent in the original PRA. Intermediate containment failure (as a result of hydrogen detonation) and late containment failures (attributable to containment pressurization as a result of passive containment cooling system (PCCS) drain blockage) together contribute less than 1 percent in the updated PRA, compared to a combined frequency of about 7 percent in the original PRA. Basemat melt-through, which accounted for 3 percent of the containment failure frequency in the original PRA, is not treated as a separate failure mode in the updated PRA. Rather, all

events which result in reactor vessel melt-through are considered to result in early containment failure, as discussed below.

Important contributors to each of these release categories are identified in Figure 19.1-2, and discussed further in the sections that follow.

Containment Bypass (BP)

Accident sequences in which fission products are released directly from the RCS to the environment via the secondary system or other interfacing system are classified as containment bypass. The total frequency of containment bypass failure in the baseline PRA is 1.1E-08/y, or about 62 percent of the containment failure frequency.

As shown in Figure 19.1-2, pressure and temperature-induced SGTR sequences account for 63 percent of the containment bypass frequency. High-pressure core melt sequences are conservatively assumed to result in failure of the SG tubes as a result of either of the two following conditions:

(1) high differential pressures in ATWS sequences (accident class 3A) with failure of RCP trip, CMT injection, or PRHR

(2) thermally induced creep rupture in high pressure core melt sequences (accident classes 1A and 1AP) in which late depressurization is unsuccessful

Hot-leg creep rupture is not credited to prevent steam generator tube failure or high pressure vessel failure. Conservatively assuming that these events result in containment bypass obviates the need for additional thermal-hydraulic and probabilistic analyses of the following:

(1) the likelihood of RCS piping versus steam generator tube over-pressure failures in ATWS events

(2) the likelihood of containment failure from DCH pressure loads in high pressure core melt accidents

(3) the relative threat and timing of creep-rupture failures in RCS piping and steam generator tubes in high pressure core melt accidents

SGTR-initiated core melt sequences with failure to depressurize the RCS prior or subsequent to core uncovery (accident class 6) account for the balance of the bypass frequency (approximately 37 percent). The potential for RCS depressurization is evaluated in the Level 2 analysis. Depressurization is credited in sequences in which the following occurs:

(1) PRHR is successful and ADS fails by operator error initially but is successfully recovered before extensive core damage

(2) PRHR and ADS are successful (core melt occurs in these sequences as the result of failure of sump recirculation).

RCS depressurization is successful in approximately half of the Level 1 SGTR sequences in the baseline PRA. SGTR sequences with successful depressurization are not considered to result in containment bypass due to low RCS pressure and high water level in the faulted steam generator, and therefore are not reflected in the 37 percent contribution from SGTR events in Figure 19.1-2. Instead, these events are further evaluated in the CET, where they generally result in an intact containment and a benign source term. The assumption that the steam generator level will be maintained above the break in such sequences is important to LRF and dose results, and will be further assured by inclusion of appropriate guidance on SGTR response within the severe accident management guidance to be developed by the COL applicant.

In previous PRAs interfacing system LOCA sequences are typically a major concern for containment bypass. However, as a result of piping system upgrades discussed previously, the frequency for ISLOCA sequences is very low for AP600 (5E-11/y). As such, the contribution of interfacing-systems loss-of-coolant accident (ISLOCA) sequences to core damage frequency and risk is negligible.

The containment bypass release category is characterized in the PRA by a loss of feedwater transient with subsequent creep rupture of five steam generator tubes and the failure of a steam generator safety valve to reseat. The fission product release to the environment begins approximately at the onset of fuel damage, and there is no attenuation of the source term beyond that which occurs by natural processes in the RCS, secondary system, or interfacing system. Westinghouse applied a decontamination factor (DF) of 100 to the aerosol release fractions calculated from the MAAP code to account for impaction on the steam generator tubes, which is not modeled in MAAP. Because containment bypass is the frequency dominant release category for AP600, this modeling assumption significantly impacts the offsite risk for the design, but the large release frequency and CCFP are not impacted since bypass events are considered to result in a large release regardless of the DF.

Early Containment Failure (CFE)

Accident sequences in which containment failure occurs within the period between onset of core damage and the end of core relocation are classified as early containment failure. In the baseline PRA, containment failures in this time period are caused by events involving reactor pressure vessel (RPV) failure or hydrogen detonation. The total frequency of early containment failure in the baseline PRA is 6.6E-09/y, or about 36 percent of the containment failure frequency. The early containment failure release category is represented in the PRA by a direct vessel injection (DVI) line break with failure of IRWST injection, successful cavity flooding and in-vessel retention, and failure of hydrogen igniters. The hydrogen generated in the primary system is released to the IRWST, containment, and valve vault. An early detonation is assumed to occur in the valve vault, causing containment failure. The fission product release to the environment begins approximately at the time of containment failure. The containment function is impaired during fission product release, thereby reducing the potential for attenuation of the source term.

Nearly all of the early failure frequency in the baseline PRA is associated with failure of the RPV. The majority of the early containment failures (85 percent) involve 3BE and 3D sequences with failure of reactor cavity flooding. The remainder (15 percent) are attributed to

spontaneous reactor pressure vessel failure events (3C) in which the vessel is not able to be reflooded to prevent debris relocation. The major cause of cavity flooding failure are:

(1) common cause failure of strainers in IRWST tank
(2) common cause failure of actuation software and hardware
(3) common cause failure of recirculation MOVs to open
(4) operator failure to open the IRWST valves to flood the reactor cavity

Early containment failure is assumed to occur as a result of ex-vessel phenomena associated with debris relocation into the reactor cavity in low pressure core melt sequences. This assumption conservatively bounds uncertainties related to ex-vessel fuel coolant interactions (FCI), core concrete interactions (CCI), and impingement of corium on the containment shell. High pressure core melt sequences, which could potentially challenge the containment from DCH, do not contribute to early containment failure in the updated PRA since these sequences are assumed to result in containment bypass, as discussed previously.

The assumption that RPV failure leads to early containment failure was made in view of the following:

(1) the high probability that the reactor cavity will be flooded in a core melt accident

(2) high confidence that molten core debris would be retained in-vessel due to the incorporation of external reactor vessel cooling features in the AP600 design

(3) the lack of deterministic calculations of ex-vessel phenomena at the time of the PRA update.

Deterministic calculations subsequently performed by Westinghouse and documented in Appendix B of the PRA indicate that containment integrity would be maintained despite localized structural failures predicted for an ex-vessel FCI (interaction of molten fuel with residual break flow expected to be present in the cavity with failure of reactor cavity flooding). The potential for containment failure from DCH events was also evaluated by Westinghouse and judged negligible on the basis of a comparison of DCH pressure loads (calculated using the methodology developed by Sandia National Laboratory for resolution of the DCH issue) with the AP600 conditional containment failure probability distribution. Although many of the events contributing to CFE frequency could be expected to result in later or no containment failure on the basis of these calculations, the bounding assumption was retained in view of the uncertainties in the resulting endstates. This assumption dominates the probability of early containment failure in the AP600 PRA.

Early containment failures as a result of hydrogen combustion account for only about 0.5 percent of the CFE frequency in the updated PRA. Dominant sequences involve early hydrogen detonation because of failure of the hydrogen igniters system from the following:

(1) common cause failure of igniters
(2) failure of the 12 volt distribution panel
(3) operator failure to actuate the hydrogen control system
(4) station blackout

The actual frequency of containment failure from hydrogen burn is quite small resulting from the high reliability of the hydrogen igniter system and the small fraction of core damage sequences involving station blackout sequences in the AP600 design.

Westinghouse evaluated the potential for early containment failure from deflagrations and diffusion flames in the development of the Level 2 event trees, but judged the contribution to be insignificant. Deflagrations were not considered to contribute to early containment failure because of the limited quantities of combustible gases produced when core debris is successfully retained in-vessel, and are not modeled as a contributor to early containment failure in the containment event tree. (Failure to retain the core debris in-vessel would result in larger amounts of combustible gases, but such sequences are already assumed to result in early containment failure as discussed above.) In contrast, diffusion flames are modeled as a potential contributor to early containment failure within the containment event tree, but the probability that a diffusion flame would lead to containment failure was assigned a zero value based on a Larson-Miller creep-rupture failure assessment of the containment shell for a postulated diffusion flame.

As discussed in Section 19.2.3.3.2 of this report, there is considerable uncertainty regarding diffusion flame behavior at the IRWST vents. If the flame remains anchored to the vent, as assumed in the baseline PRA, the resulting radiative and convective heat loads do not challenge the integrity of the containment shell. However, if the flame becomes attached to the containment shell, which the staff considers a more likely situation, the thermal loads would be substantially greater and would produce heating of the containment shell sufficient to result in localized creep rupture. At the staff's request, Westinghouse requantified the Level 2 PRA assuming that all sequences involving sustained releases through the IRWST (i.e., successful operation of ADS stages 1-3, with failure of stage 4) result in containment failure. Under this bounding assumption, the frequency of early containment failure increases by 8E-09/y (about a factor of 2 increase in the frequency of CFE) and the CCFP increases from 10.8 to 15.4 percent. Although this represents a relatively large increase in both the frequency of early failure and the CCFP, the increase in release frequency is still very small in absolute terms.

The non-safety grade containment spray system was added to the AP600 design subsequent to Revision 8 of the PRA. As such, its impact on containment response is not reflected in the Level 2 and 3 PRA results. The use of sprays is generally considered to be beneficial in terms of reducing containment pressure and enhancing fission product removal. However, in view of the potential for the sprays to adversely impact containment response by increasing the likelihood and magnitude of hydrogen combustion events, the staff requested Westinghouse to evaluate the impact of spray operation on hydrogen combustion modeling and assumptions in the Level 2 analysis, and to confirm that containment performance (and containment failure frequency) will not be adversely impacted. Westinghouse assessed the effect of sprays on the evaluation of containment failure for each combustion mode treated in the PRA, and determined that the operation of the non-safety-related spray system has no significant impact on the containment failure probability determined in the AP600 hydrogen assessment (White paper provided by Westinghouse letter dated November 12, 1997). The staff considers these assessments to be acceptable.

Additional mechanisms that contribute to early containment failure in other PRAs include in-vessel FCI (alpha mode failure), rocket mode failure, and corium impingement as a result of high pressure melt ejection. Westinghouse evaluated these mechanisms and found them to be

insignificant based on deterministic and probabilistic considerations. The potential for containment failure from in-vessel FCI was addressed for AP600 using ROAAM, and judged to be physically unreasonable (see Section 19.2.3.3.5.1 of this report). Even if NUREG-1150 mean values are used to quantify the conditional containment failure probability from this containment failure mode, the absolute value of containment failure frequency as a result of alpha mode would be very small. Reactor vessel displacements associated with postulated ex-vessel steam explosions were also considered and determined to not affect the integrity of the containment and associated equipment. Corium impingement on the containment shell is precluded by the AP600 containment layout and the inclusion of a protective layer of concrete in the reactor cavity, as described in Section 19.2.3.3.3 of this report.

Intermediate Containment Failure (CFI)

Intermediate containment failures are defined as events in which containment failure occurs in the time period between the end of core relocation and 24 hours after the onset of core damage. All contributors to intermediate containment failure involve failure of the hydrogen igniter system and containment failure due to hydrogen detonation in the intermediate time frame. The total frequency of intermediate containment failure in the baseline PRA is 1.3E-11/y, or less than 0.1 percent of the containment failure frequency.

The intermediate containment failure release category is represented in the PRA by a DVI line break with failure of IRWST injection, successful cavity flooding and in-vessel retention, and failure of hydrogen igniters. The hydrogen generated in the primary system is released into the SG compartments, IRWST and the valve vault room. A detonation to deflagration transition is assumed to occur in the CMT room in the intermediate timeframe, causing containment failure. Containment failure occurs after the majority of the fission products have been released from the RCS, thus time is available for fission product deposition.

Within the containment event tree, global hydrogen deflagrations are modeled as a potential contributor to intermediate containment failure for events in which igniters are failed. However, the containment failure probability from deflagration was judged to be negligible and assigned a value of zero. Quantification was based on combining a probability distribution of the peak adiabatic isochoric complete combustion (AICC) hydrogen burn pressure (developed from separate probability distributions for hydrogen generation and pre-burn containment pressure) with the conditional containment failure probability distribution. Scenarios with no reflooding, early reflooding, and late reflooding of the RPV were separately evaluated and limited sensitivity analyses were performed. In all cases, the containment failure probability from deflagration was determined to be negligible and therefore assigned a value of zero. Deflagrations do not contribute to intermediate containment failure because of the limited quantities of combustible gases produced when core debris is successfully retained in-vessel. (Failure to retain the core debris in-vessel would result in larger amounts of combustible gases, but such sequences are already assumed to result in early containment failure as discussed above.)

Late Containment Failure (CFL)

Late containment failure is defined in the AP600 PRA as a failure occurring later than 24 hours after the onset of core damage. All contributors to late containment failure involve failure of the passive containment cooling system, and containment failure as a result of late

over-pressurization. The total frequency of late containment failure in the baseline PRA is 1.5E-11/y, or less than 0.1 percent of the containment failure frequency.

Westinghouse performed analyses using MAAP and GOTHIC, which indicate that air cooling of the containment alone is sufficient to maintain containment pressure less than 80 psig. Thus, failure to deliver PCS water to the containment shell is not considered a containment failure mode in the PRA. The only late containment failure mode identified and considered in the Level 2 analysis is plugging of the drains in the floor of the annulus around the containment shell. Although not a key failure mode, the availability of the drains will be confirmed every two years in accordance with the technical specifications.

The late containment failure release category is represented in the PRA by a 15.2-cm (6-in.) hot-leg break with failure of IRWST injection, successful cavity flooding and in-vessel retention, and successful operation of hydrogen igniters. No air or water cooling by the PCCS is credited in the analysis. Containment failure was assumed to occur when the containment pressure reaches Westinghouse's Service Level C estimate (90 psig) at about 30 hours. Containment failure occurs after essentially all of the fission products have been released from the RCS, thus significant time is available for fission product deposition.

The following additional late containment failure modes were evaluated in other ALWR PRAs, but were not explicitly modeled in the AP600 PRA for the reasons discussed below:

- containment basemat melt-through
- containment over-pressurization failure due to steaming, non-condensible gas generation, or late hydrogen burn
- containment over-temperature failure

Containment pressurization from steaming would not lead to over-pressure failure since air cooling alone is sufficient to maintain containment pressure below Westinghouse's estimated Service Level C value. Sequences that proceed to RPV failure could lead to over-pressurization from non-condensible gas generation, but are conservatively treated as early containment failures in the AP600 PRA. Hydrogen combustion would have a negligible contribution to late containment failure given the high availability of igniters, the limited amount of hydrogen that can be produced in-vessel, and the likelihood that this hydrogen would be burned in the early and intermediate time frames. Hydrogen combustion was therefore not modeled as contributing to late containment failure. Late containment over-temperature failure would be a viable threat only if the reactor cavity is dry and the containment heat removal is lost. The frequency of such events would be small, given the high probability of a flooded reactor cavity and the high reliability and independent nature of PCS in the AP600 design, and they are conservatively assumed to lead to early containment failure in the PRA. Moreover, as discussed in SSAR Section 3.8.2.4.2.4 and Section 19.2.6 of this report, the gasket material for the equipment hatches and the personnel airlock for AP600 will be similar to EDPM E603, for which the onset of leakage in testing did not occur until temperatures were reached that were well above the severe accident temperature for AP600. The over-temperature challenge would be further reduced by use of the non-safety containment sprays.

Containment Isolation Failure (CI)

Containment isolation failures are events involving failure of the system of valves that close the penetrations between the containment and the environment. The containment isolation analysis in the AP600 PRA consists of a screening of all penetrations to identify those penetrations whose failure would result in a failure of the containment isolation function, and a fault tree analysis on the remaining penetrations to determine the probability of failure to isolate. Penetrations retained in the analysis (i.e., not screened out) are limited to the following lines:

- instrument air in
- RCDT out
- normal containment sump
- containment air filter supply and exhaust

Failure of steam generator isolation following a SGTR, and steamline isolation following a main steamline break event are considered in the Level 1 event tree analysis, but do not contribute to the containment isolation frequency reported in the Level 2 PRA. The frequency of containment isolation failure in the baseline PRA is 3.6E-10/y, or about 2 percent of the containment failure frequency. The probability of a pre-existing opening in containment large enough to constitute an isolation failure (1.2E-04) is included in the Level 1 fault tree model for LOCA, but was inadvertently omitted in the containment isolation fault trees. The inclusion of this contributor would not noticeably impact the containment isolation failure frequency.

The containment isolation failure release category is represented in the PRA by a 6-inch hot-leg break with failure of IRWST injection, successful cavity flooding and in-vessel retention, and successful operation of hydrogen igniters. Containment isolation failure is assumed to involve failure to close the largest containment penetration, an 18-inch diameter purge line, at the onset of the accident. Thus, fission product releases from the RCS can pass from the containment to the environment with reduced potential for attenuation.

19.1.3.2.3 Important Insights from Level 2 PRA and Supporting Sensitivity Analyses

Insights from the Level 2 PRA are summarized below. These are organized in terms of equipment/design features, severe accident phenomena/challenges, and human actions.

Equipment/Design Features

External reactor vessel cooling (ERVC) is effective in the majority of sequences. The AP600 design incorporates several features that enhance ERVC relative to operating plants, including the following:

(1) safety grade systems for RCS depressurization and reactor cavity flooding

(2) a unique RPV thermal insulation system that improves coolant access to the RPV during severe accidents and is not subject to clogging or structural failure by ERVC-related loads

(3) a "clean" lower head that is unobstructed by penetrations

(4) a lower power density core

Credit for ERVC in the Level 2 analysis results in the majority of core melt accidents (~90 percent) being arrested in-vessel in the baseline PRA. As such, containment challenges from ex-vessel FCI and CCI are avoided and the quantity of hydrogen generated is limited in most core melt accidents.

High reliability of RCS depressurization and reactor cavity flooding contribute to the success of ERVC. Credit for ERVC in the PRA is based on a deterministic analysis of ERVC using the Risk Oriented Accident Analysis Methodology (ROAAM), which concludes that thermally-induced failure of an externally flooded AP600-like reactor vessel is "physically unreasonable", and a probabilistic assessment of the likelihood of achieving the necessary conditions for successful ERVC. Requisite conditions are:

(1) depressurization of the RCS to below 150 psi before RCS pressure boundary challenge

(2) flooding of the reactor cavity to an elevation above the hemispherical lower head before relocation of core debris to the lower head, and to an elevation above the maximum debris pool elevation in the long term

Sufficient depressurization (as the result of successful operation of Stages 1-3 of ADS or large LOCA break flow) is achieved in about 93 percent of the core melt sequences. Adequate reactor cavity flooding is achieved in about 96 percent of the sequences. About half of the core damage events require operator actuation of the cavity flooding system to ensure successful cavity flooding, but the remaining half would adequately flood as a direct consequence of the accident progression, even without manual actions. If the operator always fails to manually flood the reactor cavity, the containment failure frequency would increase from 1.8E-08/y to 9.7E-08/y, and the CCFP would increase from 10.8 to 57 percent. Common cause failure of IRWST discharge line strainers is a dominant contributor to failure of reactor cavity flooding and early containment failure in the PRA. IRWST strainer plugging will be controlled by inclusion in D-RAP, and by a technical specification requiring verification that the screens are not restricted by debris.

Reflooding of the RPV through postulated RCS pipe breaks has a significant effect on hydrogen production. If the initiating event is a LOCA in the loop compartment, RPV reflooding occurs after significant core damage and cladding oxidation have already occurred, and does not significantly impact hydrogen production. However, if the initiating event is a DVI line break in the valve vault room and the gravity injection valves in the broken DVI line open, RPV reflooding occurs while cladding oxidation is just beginning, and substantially enhances hydrogen production in the supporting MAAP calculations. Although RPV reflooding is addressed as a separate top event in the CET, the outcome of reflooding has no appreciable impact on containment performance because the igniter system and cavity flooding system function in the majority of sequences to mitigate the effect of additional hydrogen produced by reflood and to retain the core debris in-vessel.

Diversity between injection and recirculation squib valves is important to Level 2 results. An important modeling assumption for 3BE sequences is that the IRWST injection squib valves are

diverse from the containment recirculation squib valves. As such, when IRWST injection is failed as a result of CCF of squib valves in the injection line, credit is taken for diverse squib valves in the recirculation lines used for reactor cavity flooding. Diversity is derived from the difference in operating conditions and design pressures for these valves, and is not considered to be compromised by maintenance errors or environmental/aging effects.

A specific reactor cavity concrete type is not required to meet the Commission's goals regarding large release frequency and conditional containment failure probability. Compared to other ALWRs, the AP600 ex-vessel debris bed is deeper (as a result of the higher ratio of zircaloy to fuel in the AP600 core), and the concrete basemat is thinner. Although these factors tend to increase the severity of basemat erosion, deterministic analyses indicate that in the event of unabated CCI, containment basemat penetration or containment over-pressurization will not occur until after 72 hours, regardless of concrete composition. Based on these results, the AP600 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls. The impact of basemat concrete composition on overall plant risk is not readily apparent from the PRA since all events that lead to reactor vessel breach are assumed to result in early containment failure from other mechanisms. The staff expects the risk contribution from CCI to be small however, since the consequences associated with basemat melt-through or late containment over-pressure at the earliest projected times would be benign relative to other failure modes. Operation of the non-safety-related containment spray system would further reduce the risk from over-pressure failure.

PCS water delivery is not required to assure containment integrity. Failure of PCS water delivery to the containment shell is not considered a containment failure mechanism in the PRA, since containment cooling by air alone is sufficient to limit containment pressure to values below Westinghouse's Service Level C estimate. The only PCS-related failure mode identified and modeled in the PRA is plugging of the drains near the floor of the annulus around the containment shell. Drain plugging can lead to accumulation of PCS water in the annulus, eventually reaching the baffle plate in the annulus and interrupting the air circulation. Drain plugging is conservatively estimated to lead to containment over-pressurization at about 30 hours, but is an insignificant contributor to containment failure frequency because of a low assigned probability of plugging (0.0001). This probability value is based on a weekly surveillance of the PCS annulus to identify and eliminate debris that can potentially plug the drains. Although the AP600 technical specifications permit a much longer surveillance interval (once every 2 years), increasing the PCS failure probability by a factor of 100 increases containment failure frequency and CCFP by only about 8 percent. Thus, failure of PCS would remain a minor contributor to containment failure.

A subset of the containment isolation valves are important in limiting offsite releases during core melt accidents, and are therefore actuated by DAS in addition to PMS. These include the isolation valves in the containment air filter (purge) supply and exhaust lines, the RCDT out line, and the normal containment sump line. The 45.7-cm (18-in.) containment air filter supply and exhaust valves are assumed to be open 12 percent of the time during normal operation in the PRA, and are key release pathways in the event of failure to isolate.

AC power is available in the majority of core melt accidents. Core melt sequences involving loss of offsite power contribute less than 1 percent of the core damage frequency in the

baseline PRA. Thus, ac power would be available in the majority of internally initiated severe accidents. As a result, non-safety-related systems provided specifically to deal with severe accidents, such as containment sprays, can be supplied by normal ac power and still serve their function in the large majority of core melt events.

The non-safety containment spray system provides additional fission product removal. The AP600 design includes a containment spray system for long term accident management, as discussed in Section 19.2.3.3.9 of this report. In the event of a severe accident involving failure or ineffective operation of PCS, containment sprays would reduce containment pressurization and enhance fission product removal. However, the spray system is not needed to meet the Commission's containment performance goals or quantitative health objectives. The containment spray system is not modeled in the PRA, but would not significantly impact the estimated containment failure frequency since containment over-pressurization is not a dominant failure mode in the PRA. The greater impact would be on offsite risk, as discussed in Section 19.1.3.3.3 of this report.

The AP600 design includes a capability to manually vent the containment as a long term accident management measure. The vent provides for a controlled release of fission products in lieu of a catastrophic, over-pressure failure of containment in events involving failure of PCS or unmitigated CCI. However, the vent is not needed in order to meet the Commission's containment performance goals or quantitative health objectives. The vent is not modeled in the PRA, but would not significantly impact the estimated containment failure frequency, since containment over-pressurization is not a dominant failure mode in the PRA. Venting capabilities are discussed further in Section 19.2.3.3.8 of this report.

Phenomena/Challenges

Failure of RCS depressurization or ERVC is conservatively assumed to lead to containment failure. The majority of containment failures in the baseline PRA are a result of conservative treatment of severe accident phenomena associated with events in which the RCS is not successfully depressurized or the reactor cavity is not flooded. High pressure core melts (which could lead to RPV breach and DCH, thermally-induced SGTR, or a more benign creep-rupture failure of RCS piping) are assumed in the PRA to always result in thermally-induced SGTR. Events with failure of cavity flooding (which could lead to early containment failure by ex-vessel FCI, late containment failure by basemat melt-through, or no containment failure) are assumed in the PRA to always result in early containment failure. In contrast, deterministic analyses indicate that DCH and ex-vessel FCI will not result in early containment failure, and that CCI will not lead to containment over-pressure or basemat penetration until after 72 hours. Accordingly, the containment failure frequency and dominant contributors could be substantially different than reported in the PRA if a more realistic, less conservative treatment of these issues were performed.

Eliminating credit for ERVC would increase CCFP, but the large release frequency goal would still be met. For the "final bounding state" core debris configuration that forms the centerpiece of the related ROAAM analysis (DOE/ID-10460), the staff's review of ERVC supports the Westinghouse contention that RPV integrity will be maintained. However, the staff identified two alternative hypothetical debris bed configurations that, if achieved for a sufficient period of time, would lead to thermal loads that could fail the RPV. Uncertainties in the likelihood of forming such debris bed configurations are large because of the inherent limitations in the

modeling of core melt progression/relocation and lower head debris bed behavior. If credit for successful ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption of no credit for ERVC, the containment failure frequency would approach the core melt frequency given the pessimistic characterization of containment response to an RPV breach. Even then, however, the containment failure frequency would remain below the 1E-06/y goal because of the low estimated core damage frequency. The actual containment failure frequency is expected to be much lower based on deterministic analyses that indicate that the containment is capable of sustaining ex-vessel loads.

Diffusion flames represent a unique containment challenge for AP600. Hydrogen combustion is not a significant contributor to containment failure in the baseline PRA. However, hydrogen diffusion flames at the IRWST vent, which represent a unique containment challenge for AP600, are treated optimistically in the PRA. Diffusion flames would occur at the IRWST exit in events with successful operation of ADS stages 1-3 but failure of 4th stage ADS. If the flames remain anchored to the vent, as modeled in the baseline PRA, the resulting radiative and convective heat loads do not challenge the integrity of the containment shell. However, if the flames become attached to the containment shell, which the staff considers a more likely situation, the thermal loads would produce sufficient heating of the containment shell to result in localized creep rupture. Under a bounding assumption that all sequences involving sustained releases through the IRWST (i.e., successful operation of ADS stages 1-3, with failure of stage 4) result in containment failure, the containment failure frequency increases from 1.8E-08/y to 2.6E-08/y, and the CCFP increases from 10.8 to 15.4 percent in the baseline PRA. Although this represents a relatively large increase in both the frequency of early containment failure and the CCFP, the containment failure frequency remains small in absolute terms (because of the low probability of failing the 4th stage ADS). The containment layout has several provisions to minimize the threat of diffusion flames that can challenge the integrity of the containment shell, specifically:

- the openings from the accumulator rooms and CVS compartments that can vent hydrogen to the CMT room are either located away from the containment wall and electrical penetration junction boxes or are covered by a secure hatch and locked close
- IRWST vents near the containment wall are oriented to direct releases away from the containment shell

Hydrogen combustion is not a major contributor to containment failure, concerns regarding diffusion flames notwithstanding. Hydrogen deflagrations do not contribute to containment failure in the baseline PRA because of the following:

- the relatively limited amount of hydrogen that is produced in events that are successfully arrested in-vessel
- the availability of the hydrogen igniter system in the majority of core melt sequences
- the capability of the containment to withstand the AICC peak pressures associated with large deflagrations when igniters are unavailable.

Deflagration-to-detonation transitions (DDT) are the only combustion-related contributor to containment failure in the PRA, but the contribution is small as a result of the high availability of the igniter system. If the igniter system failure probability is increased by a factor of 100, the containment failure frequency increase is small (from 1.8E-08/y to 2.1E-08/y). If the system is assumed to be unavailable in all sequences, the containment failure frequency increases from 1.8E-08/y to 4.3E-08/y and the CCFP increases from 10.8 to 25 percent in the baseline PRA. (These results are not substantially different if diffusion flames are considered to fail the containment in the baseline PRA). This shows that the operation of igniters is important to maintaining a low release frequency, but that system reliability can be reduced and not substantially impact risk.

Human Actions

A limited number of human actions in the Level 2 PRA are risk-important. Westinghouse identified the following operator actions in the Level 2 analysis as important to large release frequency based on sensitivity/importance analyses. These risk-important actions will be taken into account in control room design and the development of implementing procedures and training programs, as discussed in Chapter 18 of this report:

- diagnose and actuate the ADS after core damage to prevent RPV failure or temperature-induced SGTR (LPM-REC01 and ADN-REC01)
- diagnose and actuate the ADS after core damage in SGTR events to terminate releases from containment (PDS6-MANADS)
- open recirculation valves to flood the reactor cavity (REN-MAN03)
- actuate the hydrogen igniter system (VLN-MAN01)

Guidance for certain human actions will be developed as part of accident management. Late RCS depressurization, hydrogen igniter system actuation, and reactor cavity flooding system actuation are credited in the Level 2 analysis and included within the Emergency Operating Procedures. Several other actions not modeled in the Level 2 analysis are also manual, including actuation of the containment spray system and the containment vent system, and energizing the igniter system from either the non-essential diesel generators or the non-Class 1E batteries. Detailed procedures for these latter actions will be developed by the COL applicant as part of COL Action Item 19.2.5-1 regarding accident management.

Operator actions to depressurize the RCS are credited for terminating SGTR. Operator actions to depressurize the RCS and maintain a water level covering the SG tubes are important in mitigating fission product releases from a SGTR accident. In approximately half of the Level 1 SGTR sequences, late RCS depressurization is successful. SGTR sequences with successful late depressurization are not considered to result in containment bypass in the PRA because of low RCS pressure and high water level in the faulted steam generator. Instead, these events are further evaluated in the CET, where they generally result in an intact containment and a benign source term. Eliminating credit for late depressurization during SGTR events increases the frequency of containment failure from 1.8E-08/y to 2.3E-08/y, and the CCFP from 10.8 to 14 percent. This increase could be significant in terms of offsite consequences since the probability of large releases for AP600 is dominated by this release category. The assumption

that the RCS will be depressurized and the steam generator level will be maintained above the break in such sequences will be further assured by inclusion of appropriate guidance on SGTR response within the severe accident management guidance to be developed by the COL applicant, as discussed in Section 19.2.5 of this report.

19.1.3.2.4 Frequency and Conditional Probability of Containment Failure

In assessing the probability of containment failure, the staff considered two alternative definitions of failure:

(1) Loss of containment structural or leak-tight integrity (i.e., the containment integrity definition). Containment failure frequency under this definition is the total frequency of all containment release modes/categories except those in which the containment remains intact, and is equivalent to the "large release frequency" used by Westinghouse.

(2) Releases which result in whole body doses of 25 rem or greater at 0.5 miles from the reactor (i.e., the dose definition). Containment failure frequency under this definition is the total frequency of events which result in a relatively large release at the site boundary. Rather than attempt to define a "large release", the staff used the EPRI criterion of 25 rem at 0.5 miles from the reactor as the dose definition of containment failure.

Based on the AP600 source terms and offsite consequence analysis discussed in Section 19.1.3.3 of this report, the dose definition and containment integrity definition of containment failure are equivalent (i.e., yield approximately the same containment failure frequency) since the conditional probability of exceeding 25 rem at the boundary is close to unity for all release categories (except intact containment). This is true despite Westinghouse's use of source terms based on the MAAP code, and use of a decontamination factor (DF) of 100 on the aerosol release fractions for the containment bypass release category. Discussions below are based on the containment integrity definition of containment failure.

The containment failure frequency for internal events is 1.8E-08/y in the baseline PRA, and 5.5E-07/y in the focussed PRA. These values increase to 2.6E-08/y and 5.9E-07/y in the baseline and focussed PRA if diffusion flames at the IRWST vents are assumed to result in containment failure. The corresponding conditional containment failure probability (CCFP) is approximately 10.8 percent for the baseline PRA, and 15.4 percent if diffusion flames are assumed to result in containment failure. Although the baseline containment failure frequency is similar to the value reported in the DSER, the revised Level 2 analysis is fundamentally different than the original analysis. The updated analysis include the following major features:

- stand-alone assessments of external reactor vessel cooling and in-vessel steam explosions using the ROAAM in lieu of including these issues in the CET

- explicit treatment of reactor cavity flooding, reactor vessel reflooding, and hydrogen combustion challenges within the CET

- simplifications to the CET that provide a bounding treatment of temperature-induced steam generator tube rupture, direct containment heating (DCH), and ex-vessel phenomena associated with reactor vessel melt-through

As discussed in Section 19.1.10 of this report, the staff finds Westinghouse's modeling of these issues in the updated Level 2 PRA to be acceptable for purposes of design certification, but notes that several simplifying assumptions made for the purpose of bounding uncertainties in the underlying phenomena significantly impact the bottom line results for both large release frequency and the dispositioning of this release frequency among the various release categories used in the analysis.

In Westinghouse's analysis, most of the containment failure frequency is associated with early containment failure or containment bypass. This is an artifact of two major simplifying assumptions in the Level 2 PRA as follows:

(1) all accidents that proceed to core damage without successful depressurization are assumed to result in containment bypass due to creep rupture of steam generator tubes

(2) all accidents in which external reactor vessel cooling is unsuccessful are assumed to result in early containment failure as a result of ex-vessel phenomena.

A more detailed assessment of steam generator tube challenges and ex-vessel severe accident phenomena provided in Chapter 37 of WCAP-14745 and Appendix B of the PRA indicates that the RCS/containment pressure boundary could be expected to withstand these early challenges. However, some potential for subsequent hydrogen burns or core concrete interactions that could challenge the containment in the intermediate time frame (within 24 hours of core damage) would remain.

Sensitivity studies reported in Chapter 50 of the PRA provide insights into the importance of various assumptions on the containment failure frequency for the baseline PRA. These studies indicate that for reasonable variations in Level 2 input assumptions and CET split fractions, increases in the containment failure frequency are limited to a factor of 2 to 5, and the containment failure frequency remains below 1E-07/y, even if diffusion flames at the IRWST vents result in containment failure. It is interesting to note that modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency or CCFP since the bulk of the containment failures in the existing analyses are driven by the frequency of events with failure of RCS depressurization or reactor cavity flooding, rather than the frequency at which containment pressure loads exceed the containment pressure capability.

The staff concludes that the AP600 containment design satisfies the Commission's containment performance goal, and is therefore, acceptable. Specifically, the estimated containment failure frequency in the baseline PRA, as well as the focussed PRA, is well below the Commission's large release frequency goal of 1E-06/y. The conditional containment failure probability is at the CCFP goal of 0.1 in the baseline PRA. Although CCFP is exceeded under certain alternative assumptions (e.g., if diffusion flames are assumed to produce containment failure) and in several sensitivity cases, these increases are modest and the corresponding containment failure frequencies remain well below 1E-06/y. In view of the approximate nature of the containment performance goal, the recognition that PRA results contain considerable

uncertainties, and the fact that a large fraction of the containment failures reflected in the calculated CCFP in the baseline PRA would actually involve late basemat melt-throughs (or no containment failures) rather than early releases to the atmosphere, the staff concludes that the AP600 design satisfies the Commission's goals for both large release frequency and CCFP.

19.1.3.3 Results and Insights from the Level 3 PRA (Offsite Consequences)

In the updated AP600 PRA, the end-states of the containment event trees were grouped into 6 individual release categories. For each release category, the timing, energy, isotopic content, and magnitude of release were established based on plant-specific thermal-hydraulic calculations using the MAAP code. The NRC-developed MACCS code was then used to calculate offsite consequences for each of the release categories, specifically, the effective dose equivalent (EDE) whole-body dose complementary cumulative distribution function (CCDF) at 0.5 miles from the reactor site, and the total person-rem exposure over a 50-mile radius from the plant. These analyses were supplemented by sensitivity analyses to assess the impact of uncertainties in key parameters. The staff finds this overall approach and the use of the above codes to be generally consistent with the present state of knowledge regarding severe accident modeling and, therefore, acceptable.

In the sections that follow, results and insights from the Level 3 portion of the PRA are presented. This includes the estimated probability of exceeding selected dose criteria, a breakdown of the total risk in terms of important release classes, and finally, a summary of the risk-significant insights from the Level 3 PRA and supporting sensitivity analyses.

19.1.3.3.1 Risk Results for AP600

Based on the updated PRA, the probability of exceeding a whole-body dose of 25 rem at 0.8 km (0.5 mile) is about 1.8E-08/y for internal events. This value is about a factor of 50 lower than the Commission's large release frequency goal of 1E-06/y and is therefore acceptable. The design also meets the Public Safety Requirement goal established by the Electric Power Research Institute (EPRI) in the Advanced Light Water Reactor Utility Requirements Document (1E-06 probability of exceeding a dose of 25 rem at a distance of 0.5 miles). It should be noted, however, that the EPRI goal applies to both internal and external events, and that the results for AP600 do not include the contribution from seismic and fire events.

Based on the Level 3 PRA, the estimated total risk to the public for AP600 is quite small. Westinghouse's analysis indicates a total dose of about 8E-03 person-rem/y or 0.5 person-rem over a 60-year plant life, based on the use of population and weather data developed by EPRI to bound 80 percent of the reactor sites in the United States (Ref: Revisions 5 and 6 of the URD and a 72 hour mission time). Offsite risk is very low compared to the current generation of operating plants because of a combination of three factors: (1) a very low estimated CDF for AP600, (2) a low conditional containment failure probability, and (3) a relatively benign source term associated with the frequency-dominant release category.

19.1.3.3.2 Leading Contributors to Risk from Level 3 PRA

The contribution to risk from each of the release categories is presented in Table 19.1-5 and Figure 19.1-3. The following can be noted:

- Based on Figure 19.1-3, the probability of exceeding 25 rem at the site boundary is essentially flat and close to unity for all release categories except IC and CFL. Thus, the probability of exceeding 25 rem is equivalent to the probability of containment failure. This is true despite Westinghouse's use of source terms based on the MAAP code, and use of a decontamination factor of 100 on the aerosol release fractions for the containment bypass release category.

- Events in which the containment remains intact (IC) account for nearly 90 percent of core damage events, but are negligible contributors to risk because of the insignificant consequences associated with normal containment leakage.

- Containment bypass events (BP) contribute about 60 percent of the containment failure frequency, but account for only about 6 percent of the risk because of the benign nature of the source term after applying a DF of 100.

- CFE accounts for about 36 percent of the containment failure frequency, but 84 percent of the risk. The larger risk contribution is the result of the large consequences (1E6 person-rem/event) associated with this release.

- Releases from containment isolation failure (CI), although equivalent to CFE in terms of the magnitude of release, account for only 10 percent of the total risk. This is as a result of the low estimated frequency of isolation failure, which is about a factor of 20 lower than the frequency of early containment failure.

19.1.3.3.3 Important Insights from Level 3 PRA and Supporting Sensitivity Analyses

Insights from the Level 3 PRA are summarized below on the basis of the Level 3 PRA results and supporting sensitivity analyses.

- On the basis of the updated PRA, the probability of exceeding a whole-body dose of 25 rem at 0.8 km (0.5 mile) is about 1.8E-08/y, and is equivalent to the containment failure frequency (core damage frequency less the frequency of events with intact containment). The release frequency is a factor of 50 lower than the Commission's large release frequency goal and EPRI's Public Safety Requirement. It should be noted that the EPRI goal applies to both internal and external events, and that the results for AP600 do not include the contribution from seismic and fire events. However, based on the estimated core damage and containment failure frequencies for externally-initiated events and events at shutdown, the large release frequency goals would also be met when these additional contributors are considered.

- The AP600 risk profile is shaped by several major assumptions regarding containment failure modes and release characteristics including the following: (1) conservative assumptions regarding early containment failure from ex-vessel phenomena, (2) optimistic assumptions that external reactor vessel cooling will always prevent reactor

pressure vessel breach, and (3) substantial credit for additional aerosol removal in SGTR events. Their impact on risk results is described below.

In the baseline PRA, risk is dominated by events in which early containment failure is conservatively assumed to occur as a result of ex-vessel phenomena associated with RPV melt-through. However, deterministic calculations performed by Westinghouse subsequent to the PRA update indicate that the containment is likely to withstand these phenomena without loss of integrity. If early containment failure is avoided and reactor pressure vessel breach results instead in a more benign release (e.g., a containment failure in the intermediate time frame), overall risk for internal events would be reduced by about a factor of 2.

In the baseline PRA, successful RCS depressurization and reactor cavity flooding (achieved in over 90 percent of the core damage events) are assumed to always prevent reactor vessel breach and associated ex-vessel phenomena. However, the staff identified three hypothetical debris bed configurations that, if achieved for a sufficient period of time, would lead to thermal loads that could fail the RPV. If credit for ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption that ERVC always fails and leads to early containment failure, the containment failure frequency would approach the core melt frequency and risk would increase by a factor of 20 (to about 0.16 person-rem/y). Even then, however, the containment failure/large release frequency would remain below the Commission's large release frequency goal of 1E-06/y and the absolute level of risk would remain low. The actual containment failure frequency and risk is expected to be much lower based on deterministic analyses that indicate that the containment is capable of sustaining ex-vessel loads, as discussed above.

In the baseline PRA, containment bypass events dominate the frequency of large release, but do not contribute significantly to risk because of a DF of 100 applied to the MAAP-predicted aerosol release fractions for this release category. The DF is intended to account for fission product removal by impaction on steam generator tubes. This removal mechanism is not modeled in either the MAAP calculations on which the AP600 source terms are based or staff codes such as MELCOR or VICTORIA, and credit for this mechanism is unprecedented, although not necessarily unjustified. With this credit for aerosol removal, the risk contribution from containment bypass is minimal (6 percent of the total). Without this credit, overall risk for internal events would increase by a factor of 7 and would be dominated by bypass releases.

- The impact of the containment spray system on fission product releases was not credited in the PRA. Containment sprays could significantly reduce the estimated risk in the baseline PRA (by perhaps a factor of 2) since the sprays would be effective in reducing the source terms in the risk-dominant release categories (i.e., CFE and CI).

- Containment failures in the intermediate and late time frames are insignificant contributors to risk because of the small frequency associated with these release categories.

- Interfacing system LOCAs do not contribute to overall plant risk, primarily because of a piping upgrade that led to a low estimated frequency of these events.

19.1.4 Safety Insights from the Internal Events Risk Analysis for Shutdown Operation

Safety insights from the Level 1 PRA are reported in Sections 19.1.4.1 through 19.1.4.5 while Section 19.1.4.6 reports safety insights from levels 2 and 3 of the PRA.

19.1.4.1 Level 1 Shutdown Internal Events PRA

The staff's review of the AP600 shutdown PRA is founded on the results reported in Attachment 54B of the PRA and additional references from Attachments 54A and 54C and Chapter 54. Attachment 54B is a requantification of the shutdown PRA results using revised success criteria for injection and recirculation during reduced inventory conditions with loss of the normal residual heat removal function. The revised success criteria state the following:

- at least one of the four 4th stage ADS valves must open during reduced inventory conditions for successful gravity injection from the IRWST

- containment sump recirculation is needed for long term cooling following ADS operation during reduced inventory conditions

Attachment 54C documents two success criteria changes for safe/cold shutdown with the RCS intact as follows:

- RCS full depressurization requires 4th stage ADS
- containment recirculation would likely be required following 4th stage ADS operation

Westinghouse estimated the mean CDF from internal events during shutdown for the AP600 design to be 9E-08 per year (about 50 percent of the corresponding CDF for power operation). This estimate assumes that no maintenance activities will be scheduled during reduced inventory conditions on the gravity injection from the IRWST, the 4th stage ADS valves and the containment sump recirculation trains even though such outages are allowed by the AP600 technical specifications (TSs). The shutdown CDF estimate from internal events can increase to 1E-06/year if a COL applicant were to always choose minimal compliance with the AP600 TS. These insights are discussed further in Section 19.1.4.5

The reported CDF from internal events during shutdown operation (9E-08/year) covers safe shutdown operation, cold shutdown operation (including drained RCS conditions) and refueling operations until the refueling cavity is flooded. This shutdown CDF estimate can be directly added to the full power estimate. The AP600 shutdown PRA CDF estimate is determined by the fraction of time per year that the plant is expected to be in safe shutdown operation, cold shutdown operation, and refueling operations until the refueling cavity is flooded. Over 90 percent of AP600 shutdown risk occurs during reduced inventory operations.

Operation in Mode 2 (startup) and Mode 3 (hot standby) were not quantitatively evaluated because the plant response to a loss of core cooling during these conditions is the same as during power operation. Since the safety-related systems (except for the accumulators below 1000 psig) and most actuation signals (both automatic and manual) are required to be operable

by Technical Specifications during Modes 2 and 3, the CDF contribution from events during these Modes is expected to be insignificant compared to at-power conditions (due to the smaller decay heat and the longer times for operator intervention).

In Section 19.1.4.2, Westinghouse presents the dominant accident sequences and the major contributors to the shutdown CDF estimates. The AP600 design features that reduce AP600 shutdown risk compared to operating PWRs are described in Section 19.1.4.3. In Sections 19.1.4.4 and 19.1.4.5, insights drawn from the importance and sensitivity studies are discussed.

19.1.4.2 Dominant Accident Sequences Leading to Core Damage

As discussed above, over 90 percent of AP600 shutdown risk occurs during reduced inventory operations. Reduced inventory operations occur during cold shutdown when the RCS boundary is open (via stages 1,2, and 3 of ADS), and the RCS is drained to reach mid-loop conditions so that nozzle dams can be installed in the hot and cold legs to perform steam generator maintenance. When the RCS boundary is open, emergency core cooling using PRHR is not viable; therefore, gravity injection from the IRWST and 4th stage ADS actuation must be initiated. Given that 4th stage ADS must open during reduced inventory conditions following an extended loss of RNS, containment sump recirculation would be initiated within 72 hours following accident initiation.

The top 9 sequences contributing approximately 90 percent of the risk, as reported by Westinghouse, are described below.

Sequence #1, with a CDF of 3.0E-08 per year and a 33 percent contribution, is initiated by a loss of component cooling water/service water system (CCS/SWS) with the RCS drained. Actuation of the 4th stage ADS squibs is successful. However, gravity injection through either the IRWST injection lines or via the RNS pump suction line fails leading to core damage.

Sequence #2, with a CDF of 1.7E-08 per year and a 19 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Actuation of the 4th stage ADS squibs is successful. Actuation of gravity injection is also successful. However, recirculation from the containment sump fails leading to core damage.

Sequence #3, with a CDF of 1.6E-08 per year and a 17 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Actuation of the 4th stage ADS valves fails leading to core damage.

Sequence #4, with a CDF of 5.8E-09 per year and a 6 percent contribution, is initiated by the loss of RNS with the RCS drained. Actuation of the 4th stage ADS valves is successful. However, gravity injection through either the IRWST injection lines or via the RNS pump suction line fails leading to core damage.

Sequence #5, with a CDF of 3.3E-09 per year and a 4 percent contribution, is initiated by a loss of RNS with the RCS drained. Actuation of the 4th stage ADS squibs is successful. Actuation of gravity injection is also successful. However, recirculation from the containment sump fails leading to core damage.

Sequence #6, with a CDF of 3.0E-09 per year and a 3 percent contribution, is initiated by a loss of RNS with the RCS drained. Actuation of the 4th stage ADS valves fails leading to core damage.

Sequence #7, with a CDF of 2.7E-09 per year and a 3 percent contribution, is initiated by an inadvertent opening of V024 during safe/hot shutdown. Inadvertent opening of V024 causes reactor coolant to drain into the IRWST. The CMTs and ADS successfully actuate. However, gravity injection through the IRWST injection lines fails leading to core damage.

Sequence #8, with a CDF of 2.0E-09 and a 2 percent contribution, is initiated by a loss of offsite power with the RCS drained. Recovery of RNS and recovery of offsite power within 1 hour failed. Actuation of the 4th stage ADS valves succeeds. However, gravity injection through either the IRWST injection lines or via the RNS pump suction line fails leading to core damage.

Sequence #9, with a CDF of 1.9E-09 and a 2 percent contribution, is initiated by overdraining of the RCS during draining operations to reach mid-loop conditions. This initiating event assumes one of three scenarios occurs. In scenario one, both hot-leg level instruments fail, and the operator fails to notice the indication inconsistency between the hot-leg level instruments and the pressurizer wide range level indication. This failure results in the operator overdraining the RCS. In scenario two, the hot-leg level instruments are working. However, the two safety-related AOVs in the RCS drain path fail to isolate. In scenario three, the hot-leg level instruments are working correctly, but the PMS signal to close two safety-related AOVs in the drain path fails, and the operator fails to isolate the drain path. The ADS squib valves successfully actuate. However, gravity injection through either the IRWST injection lines or via the RNS pump suction line fails leading to core damage.

19.1.4.3 Risk-Important Design Features

Listed below are key AP600 design features that significantly reduce the shutdown CDF compared to operating PWR designs. These design features are described below by initiating event category.

Loss of RNS or its Support Systems (CCW/SWS) During Safe Shutdown/Cold Shutdown With the RCS Intact

Unlike current operating PWRs, the AP600 PRHR system provides an additional path of core cooling which is diverse from the RNS as well as ac independent and safety-related (passive). The PRHR does not depend on traditional support systems, such as component cooling water, to operate. In addition, the PRHR is capable of functioning at low pressures and temperatures as long as the RCS is intact. However, manual actuation is required before reactor coolant system pressure increases to cause the normal residual heat removal valve to open.

In current PWRs, operator action is required to restore all interruptions of residual heat removal (RHR). In the AP600 design, should manual actuation of PRHR fail, an alternate core cooling path is automatically established using the CMTs for injection, ADS for depressurization, gravity injection from the IRWST, and long term cooling using containment recirculation.

LOCAs During Safe Shutdown/Cold Shutdown With the RCS Intact

In current PWRs, operator action is required to mitigate all losses of RCS inventory (e.g., operator action is required to actuate injection). In the AP600 design, should a RCS drain path occur that is un-isolable, RCS injection and core cooling are automatically provided using the CMTs, ADS, gravity injection from the IRWST, and containment recirculation (for long term cooling).

LOOP/SBO During Safe Shutdown/Cold Shutdown With the RCS Intact

The AP600 design provides much better protection against LOOP/SBO events compared to current PWRs since the operator is not required to perform many recovery actions. Following a loss of offsite power, the RNS pumps trip, but an automatic restart of the RNS pumps is provided after the diesel generators start and the electrical buses are sequenced. Should the diesel generators fail to start resulting in a loss of ac power and instrument air, PRHR provides core cooling automatically, since the PRHR air operated valves are expected to fail open. Should manual actuation of PRHR fail, an alternate core cooling path is automatically established using the CMTs, ADS, gravity injection and containment recirculation (this requires only dc power).

Loss of RNS due to Inadvertent Overdraining of the RCS to Achieve Mid-loop Conditions

Previous PWR shutdown PRAs have reported that overdraining of the RCS during mid-loop conditions is a dominant contributor to shutdown risk. The AP600 design has many design features, not present in current PWRs, to prevent loss of the RNS pumps as a result of air entrainment and cavitation. These features are discussed further below.

To prevent overdraining, the RCS hot and cold legs are vertically offset. This design permits draining of the steam generators for nozzle dam insertion with a hot-leg level much higher than traditional designs. The RCS must be drained to a level which is sufficient to provide a vent path from the pressurizer to the steam generators (nominally 80 percent level).

To lower the level in the hot leg where vortexing can occur, the AP600 design uses a step nozzle connection between the RCS hot leg and the RHR suction line. To prevent cavitation, the piping elevations and routing and the RNS net positive suction head (NPSH) requirements allow the RNS pumps to be started and operated with saturated conditions in the RCS. Also, there is no need to throttle RNS flow when the RCS is in mid-loop conditions.

If adequate NPSH is lost, recovery of RNS is expected to be quicker compared to operating PWR designs. The RNS pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if a RNS pump is stopped when cavitating due to excessive air entrainment. This self-venting suction line allows the RNS pumps to restart immediately once an adequate level in the hot leg is re-established.

To assist the operator, the AP600 design contains hot-leg level instrumentation with indication in the main control room. Each hot leg contains one hot-leg level channel, totally independent of each other. One level tap is at the bottom of the hot leg, and the other tap is on the top of

the hot leg as close to the steam generator as possible. The AP600 design also provides cold-calibrated wide-range pressurizer level that can measure RCS level down to the bottom of the hot legs. This pressurizer level indication can be used as an alternative way of monitoring level and can be used to identify inconsistencies in the hot-leg level instrumentation.

Should overdraining of the RCS occur, the operator is not required to manually actuate RCS injection as in current PWRs. The safety-related PMS provides automatic isolation of normal CVS letdown on low hot-leg level (one-out-of two basis). On low hot-leg level, two safety-related AOVs close automatically to isolate letdown. On low, low hot-leg level, the PMS provides automatic actuation of IRWST injection (two-out-of-two basis), and automatic actuation of fourth-stage ADS to prevent surge line flooding (two-out-of-two basis). Long term cooling is provided by containment recirculation.

LOOP/SBO During RCS Open Conditions

The AP600 design provides much better protection against LOOP/SBO events compared to current PWRs since the operator is not required to perform many recovery actions. Following a loss of offsite power, the RNS pumps trip, but an automatic restart of the RNS pumps is provided after the diesel generators start and the electrical buses are sequenced. Should the diesel generators fail to start, gravity injection from the IRWST and concurrent 4th stage ADS actuation (to prevent surge line flooding) is automatically provided on low hot-leg level. Gravity Injection and 4th stage ADS require only 1E dc power to operate. Long term cooling is provided by containment sump recirculation.

Loss of RNS (Due to LOCAs or Loss of RNS or its Support Systems) During RCS Open Conditions

The AP600 design provides better protection against losses of RNS compared to current plants since the operator is not required to mitigate the event. Following a loss of RNS, gravity injection from the IRWST and concurrent 4th stage ADS actuation (to prevent surge line flooding) is automatically provided on low hot-leg level from the PMS system. On low IRWST level, automatic containment recirculation provides long term core cooling.

Boron Dilution Events

The RES Surry Shutdown PRA (NUREG-6144 Appendix I) evaluated a potential boron dilution event during reactor startup following an LOOP event, with subsequent startup of the reactor coolant pumps. This scenario was estimated in NUREG-6144 Appendix I as having a CDF of 9E-06 per year. The scenario assumes an occurrence of a loss of offsite power during RCS de-boration during startup. When the charging pumps are restarted by the emergency diesel generators, the pumps drain primary grade water from the volume control tank into the RCS through the cold leg. With none of the RCPs running and virtually no natural circulation present (due to very low decay heat), the boron dilution continues. The primary grade water gradually makes its way to the reactor vessel and settles at the bottom of the vessel. If offsite power is recovered and one of the RCPs is restarted a few moments later, this will send a slug of primary grade water into the core, causing a power excursion.

The AP600 plant design prevents the boron dilution scenario described above from occurring. Once the 1E dc and un-interruptible power supply system (UPS) battery chargers receive low

input voltage, the PMS provides a boron dilution signal that automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related demineralized water supply valves.

Alternatively, should a boron dilution event occur during startup as a result of failure of the plant control system (PLS) and failure of operator control of PLS, the safety-related, boron dilution protection signal would be generated upon any reactor trip signal, source range flux multiplication signal, low input voltage to the Class 1E dc power system battery chargers, or a safety injection signal. As described above, this signal automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related demineralized water supply valves. Boron dilution events during safe shutdown using the "dilute" mode of operation were quantified separately from the shutdown PRA. Westinghouse concludes that these events are a negligible contributor to the AP600 shutdown CDF estimate.

19.1.4.4 Insights from the Risk Importance Studies

As discussed in Section 19.1.3.1.4, the staff used the results of Westinghouse's importance analyses to identify the following: (1) SSCs and/or human actions whose reported reliability contribute most to achieving the low reported shutdown CDF (risk achievement worth) and (2) SSCs and/or human actions which would contribute most to a reduction in shutdown CDF if the reliabilities were improved (risk reduction worth). Since the reported AP600 shutdown CDF is very low (9E-08 per year) and clearly meets the Commission Safety goals and the EPRI ALWR CDF requirements (<10E-05 per year), the staff focused on the results of Westinghouse's shutdown risk achievement analyses. The staff used these results to identify (1) the SSCs for which it is particularly important to maintain the reliability/availability levels assumed in the PRA (e.g., by testing and maintenance) to avoid significant increases in CDF and (2) the human actions which if failed would have the largest impact on the shutdown CDF.

Risk importance analyses were performed at the component/human action level only. In summary, the components, whose reported reliability are most critical to achieving the low shutdown CDF, are those that are required to support gravity injection during reduced inventory operation. The major insights from the risk achievement analysis (from Table 54B-7 in Attachment 54B) are summarized below in order of risk importance.

- Similar to the full power internal events results, common cause software failure among the PMS and PLS logic cards has very high risk significance (basic event CCX-SFTW). If a software fault of this kind existed and manifested itself every time an accident occurred during shutdown, the CDF would increase by four orders of magnitude.

- Inadvertent overdraining of the RCS while reducing inventory to reach mid-loop conditions has very high risk significance (initiating event IEV-RCSOD). This event results in loss of shutdown cooling (i.e., RNS) and requires manual RCS injection and manual 4th stage ADS actuation. For this initiator, Westinghouse did not credit recovery of RNS using non-safety-related CVS to restore RCS level and operator action to vent the RNS pumps.

Three scenarios were postulated which would result in overdraining of the RCS:

- The first scenario starts with failure of either hot-leg level instrument channel. The operator fails to recognize hot-leg instrument failure and thereby fails to stop RCS overdraining.

- The second scenario assumes that the hot-leg level instruments are working correctly, however, the safety-related CVS letdown valves fail to close.

- The third scenario assumes that the hot-leg level instruments are working correctly, however, the signal to close the safety-related CVS letdown valves automatically fails, and the operator fails to respond to the low hot-leg alarm and closes the CVS letdown valves.

Occurrence of either one of these scenarios leads to RCS overdraining and requires manual actuation of gravity injection and 4th stage ADS. If the RCS was always overdrained when reaching mid-loop conditions, the CDF would increase by almost four orders of magnitude.

- Gravity injection is required to mitigate every loss of shutdown cooling event during cold shutdown with the RCS open (except LOOP events where the diesels and automatic restart of RNS are available). Gravity injection is also required to mitigate every loss of shutdown cooling event during safe/cold shutdown with the RCS intact where PRHR is not available (except LOOP events where the diesels and automatic restart of RNS are available). Therefore, events that result in failure of gravity injection have very high risk significance. Specifically, common cause failures of the gravity injection squib valves and failure of RNS V023 (which fails gravity injection through the RNS pump suction line) have very high risk significance (basic event IWX-MV-GO1). Plugging of both IRWST strainers also has very high "risk achievement worth" values (basic event IWX-FL-GP). Plugging of both strainers fails both gravity injection through the IRWST injection lines and the RNS pump suction lines. Assuming that either event always occurs following a shutdown initiator, the CDF would increase by over three orders of magnitude.

- Containment sump recirculation is required to mitigate every loss of shutdown cooling event during cold shutdown with the RCS open (except LOOP events where the diesels and automatic restart of RNS are available). Containment sump recirculation is also required to mitigate every loss of shutdown cooling event during safe/cold shutdown with the RCS intact and PRHR unavailable (except LOOP events where the diesels and automatic restart of RNS are available). Therefore, events that result in failure of containment sump recirculation have very high risk significance. Specifically, plugging of both containment strainers has very high "risk achievement worth" values (basic event REX-FL-GP). Also, common cause failure of the recirculation squib valves (basic event IWX-EV4-SA) has very high risk significance. Assuming that either event always occurs following a shutdown initiator, the CDF would increase by over three orders of magnitude.

- Common cause failure of I&C components that fail automatic gravity injection and/or ADS actuation have very high risk significance, including common cause failure of the

instrument orifices, common cause failure of pressure transmitters, and common cause failure of power interface output boards in the PMS system (basic events CCX-ORY-SPX, CCX-XMTRX, and CCX-EP-SAM). Should any one of these failures occur when demanded, the shutdown CDF would increase by three orders of magnitude.

- Actuation of 4th stage ADS is required to maintain a vent path to mitigate all shutdown events when gravity injection and containment recirculation are required following an extended loss of RNS during safe/cold shutdown with the RCS intact and cold shutdown with the RCS open. Therefore, common cause failure of the 4th stages ADS squib valves to open has very high risk significance (basic event ADX-EV-SA). Should the 4th stages ADS squib valves fail to open when demanded, the shutdown CDF would increase by 3 orders of magnitude.

- Failure of the PMS boron dilution signal to generate on high flux has high risk significance. Boron dilution events during safe shutdown were quantified separately from the PRA. Upon review of the associated event tree, failure of this signal to generate following every dilution event during safe shutdown results in a criticality frequency approximately four orders of magnitude higher than the shutdown core damage frequency. Other boron dilution scenarios were not explicitly quantified. Therefore, the staff believes that all instrumentation associated with the boron dilution signal are important to keeping the core damage risk associated with boron dilution events low.

- Loss of shutdown cooling with the RCS drained (due to RNS failures or its support system failures) have high risk significance (initiating events IEV-CCWD and IEV-RNSD). These initiating events require 4th Stage ADS actuation and gravity injection to maintain core cooling. Long term cooling requires containment sump recirculation. Should either of these events occur each time the plant operates with reduced inventory, the shutdown CDF would increase by three orders of magnitude.

- Inadvertent Opening of RNS Valve V024 by an operator during safe/cold shutdown with the RCS intact causes reactor coolant to drain into the IRWST. This initiating event requires gravity injection from the IRWST, full RCS depressurization, and containment recirculation for long term cooling. Should this event occur each time the plant is at shutdown, the shutdown CDF would increase by three orders of magnitude.

- Inadvertent Opening of RNS Valve V024 by an operator during RCS drained conditions causes reactor coolant to drain into the IRWST. This initiating event requires gravity injection from the IRWST and 4th stage ADS actuation. Long term core cooling requires containment sump recirculation. Should this event occur each time the RCS is drained, the shutdown CDF would increase by three orders of magnitude.

Westinghouse, in performing the Level 1 PRA for internal shutdown events, identified the following risk-important tasks using the risk importance analyses results and threshold values. Westinghouse also examined shutdown initiating events to identify risk important tasks where human error substantially contributes to the frequency of these events. These risk important tasks should be taken into account in the human system interface design, procedure

development, and staffing requirements development. The process for inclusion of these tasks is addressed in Section 18.5 of the SSAR.

- Operator fails to recognize the need for RCS depressurization (LPM-MAN05).
- Operator fails to open the IRWST squib valves for gravity injection(IWN-MAN-00).
- Operator fails to recognize the need to open RNS V023 for gravity injection (RHN-MAN-05).

The following operator actions substantially contribute to the frequency of losing shutdown cooling via RNS. Therefore, Westinghouse considered the following to be risk important tasks:

- Operator inadvertently opens RNS V024 during safe/cold shutdown or during drained conditions in the RCS and fails to terminate the event by reclosing the valve.
- Operator fails to recognize hot-leg-level instrument failure and subsequently fails to close the safety-related air-operated CVS letdown isolation valves (CVS-V045 and CVS-V047).
- Operator fails to detect automatic failure of the CVS letdown isolation valves to close, and subsequently fails to manually close the valves, when low hot-leg level is reached during draining of the RCS to reach mid-loop conditions.

19.1.4.5 Insights from the Sensitivity Studies

Westinghouse performed sensitivity studies to gain insights about the impact of uncertainties on the reported shutdown CDF. Specifically, these studies show how sensitive the shutdown CDF is to potential biases in numerical estimates assigned to initiating event frequencies, equipment unavailabilities, and human error probabilities.

Similar to full power, a separate sensitivity study was performed to investigate the impact of shutdown operation without credit for non-safety-related "defense-in-depth" systems. This study is called the "focused PRA". The results of the "focused PRA" and additional sensitivity studies are described below.

Shutdown CDF Assuming Minimal Compliance with AP600 TS

In the baseline and "focused" shutdown PRA, Westinghouse credits two gravity injection paths to be available (including a small maintenance unavailability). However, the AP600 TSs allow one out of two IRWST injection trains to be out of service during the entire cold shutdown period. (Reduced inventory operation and mid-loop operation are a subset of cold shutdown operation). Westinghouse also credits a third gravity injection path through the RNS pump suction lines. This third path requires RNS valve V-23 to open. RNS valve V-23 is a safety-related, containment isolation valve and can be actuated using the PMS. However, the function of RNS V-23 is to open to provide gravity injection which is not a safety-related function. Therefore, the capability for RNS-V023 to open is not required by AP600 TS during

cold shutdown operation. With respect to RCS venting, Westinghouse credits all four fourth stage ADS valves to be available in the PRA. However, AP600 TS only require two fourth stages ADS valves to be operable. With respect to containment sump recirculation, the AP600 TS only require one out of two containment sump recirculation trains to be available.

In the bases of AP600 TS, there is no discussion that planned maintenance of these three systems should be avoided during cold shutdown. The frequency and duration of IRWST, ADS, and RNS maintenance performed by a future COL applicant has considerable uncertainty. Therefore, the staff asked Westinghouse to perform a sensitivity study assuming minimal compliance with AP600 TS. This sensitivity study provides an upper bound of the shutdown CDF assuming the COL applicant chooses to always perform planned maintenance on one IRWST injection path and recirculation path, two 4th stage ADS valves, and RNS valve V-23 during cold shutdown. The shutdown CDF for this sensitivity study increases to 1.4E-06 per year (a factor of five higher than the full power CDF).

Impact of Operator Error

Based on the results of shutdown PRAs for operating PWRs, the staff recognizes the high risk significance of operator error during shutdown conditions. In current plants, loss of shutdown cooling is often caused by operator error, and all interruptions of shutdown cooling require an operator response to prevent core damage.

As explained in Section 19.1.4.3, the AP600 design provides an automatic mitigation capability for all the initiators quantitatively analyzed in the AP600 shutdown PRA. Therefore, the AP600 dependency on operator action is significantly reduced. Westinghouse performed a sensitivity study setting all human error probabilities associated with event mitigation to .5. The shutdown CDF increases 2.5E-06 which is still quite low compared with operating facilities.

In the sensitivity study discussed above, all operator actions associated with event mitigation and failure of the operator to manually isolate a RNS leak were set to 0.5. The staff performed an additional sensitivity study setting all operator actions to 0.5. The staff took the results of Westinghouse's sensitivity study and set two key human errors associated with preventing overdraining during midloop conditions to 0.5. The first event is failure of the operator to diagnose hot leg instrument failure and stop reactor coolant draining. The second event is failure of the operator to respond to the low hot leg alarm and isolate the drain, given failure of the automatic actuation signal to close the CVS drain valves. By setting these two key actions to 0.5, the CDF increases to at least 4E-5 per year. These results indicate the need for the wide range pressurizer level indication which can be used to identify hot leg level indication problems. These results also point to the risk importance of the hot leg level alarms and the operator recovery actions associated with these alarms.

Risk Impact of Non-Safety-Related Systems

Westinghouse performed a sensitivity study by assuming the AP600 plant was operating at shutdown conditions and *all* of the non-safety-related "defense-in-depth" systems were not available following the occurrence of an initiating event. This sensitivity study is referred to as the "focused" PRA. As described in Section 19.1.3.1.5, this study provides additional insights about the risk importance of the "defense-in-depth" systems. These insights were used to

select non-safety-related systems that require "regulatory treatment" according to the RTNSS process.

Core cooling during Modes 4, 5, and 6 is provided by the non-safety-related RNS system and its non-safety-related support systems. In the "focused" PRA model, the frequency of losing non-safety-related RNS and its support systems (CCW and SWS) remain the same as in the baseline PRA. However, in the "focused PRA", all credit for the non-safety-related systems being able to mitigate a shutdown initiator was removed.

Except for the LOOP trees, no other changes to the event trees were required, since all event mitigation functions are safety-related. In the LOOP event tree, credit was removed for the non-safety-related diesel generators and grid recovery. In the system fault trees, the station blackout fault trees were used for the Class 1E and the UPS systems so that only safety-related power supplies were credited.

The "focused" PRA shutdown CDF was estimated to be 6E-07. The relatively small change occurs for two reasons: 1) the frequency of losing RNS and its support systems was unchanged from the baseline PRA and 2) all event mitigation functions are safety-related. Since the RNS and its support system (CCW and SWS, and ac power) significantly contribute to the likelihood of having a shutdown initiator, these systems are subject to availability controls during Mode 5 and Mode 6 when the RCS is open. During Mode 5 and Mode 6 when the RCS is open, PRHR is not credited for core cooling. The availability controls are discussed in SSAR Section 16.3.

In the "focused" PRA, Westinghouse did credit gravity injection through RNS valve V-023. This valve is a safety-related, containment isolation valve and can be actuated using the PMS. However, the function of RNS V-023 is to open to provide gravity injection, which is not a safety-related function. Therefore, the capability for RNS-V023 to open is not required by AP600 TS during cold shutdown operation. Thus, the staff performed an additional sensitivity study using the results of the "focused PRA" and removing credit for RNS VO23. In this study, the CDF increases to at least 6E-6 per year. Based on this result, the staff concludes that the reliability of the IRWST suction isolation valve (VO23) to open on demand during RCS drained operations is important. The COL applicant will maintain the reliability of this valve as discussed in Section 17.4 of the SSAR.

19.1.4.6 Levels 2 and 3 Shutdown Internal Events PRA

19.1.4.6.1 Level 2 PRA Modeling for Events at Shutdown

Westinghouse's evaluation of containment response during severe accidents initiated during shutdown is documented in Chapter 54B.3 of the PRA. The containment analysis uses Level 1 shutdown PRA results reported in Section 54B.1, which include updates to address staff concerns regarding surge line flooding and long term cooling (recirculation) success criteria. The analysis is limited to quantification of large release frequency for the baseline and focussed shutdown PRA, and does not include an assessment of offsite consequences.

For the purposes of this analysis, the Level 1 PRA results are binned into 6 accident classes based on RCS pressure, the nature of core cooling failure, and whether the containment is bypassed. Each of these accident classes has a corresponding accident class in the at-power

PRA. Four of the shutdown accident classes address events with full or partial RCS depressurization (LP-3BE, LP-3BR, LP-3BL, and LP-3D). A separate containment event tree is developed for each of these classes. The structure of the event tree and the event tree end states are the same as used in the at-power Level 2 PRA and described in Section 19.1.3.2.1 of this report. One accident class (LP-1A) fails depressurization by definition and, consistent with the approach taken in the at-power analysis, is assumed to always induce a steam generator tube rupture. The remaining accident class (LPCBP) bypasses the containment by definition. For these latter two accident classes, no containment event trees are used, and the accident class frequency is added directly to the containment bypass release category frequency (BP).

The CET is quantified separately for each accident class. For system related top events, the split fractions are quantified by linking to the system fault trees for the shutdown PRA (i.e., top events for RCS depressurization, containment isolation, reactor cavity flooding from the IRWST, and hydrogen igniter system). These faults trees were specifically developed to represent shutdown conditions. Special assumptions made for the shutdown modes are documented in Table 54-7 of the PRA. For the balance of the top events, i.e., the nodes used to address severe accident phenomena, the split fractions are assigned scalar values based on a characterization of the underlying processes/phenomena. The scalar values used in the shutdown CETs are taken directly from the at-power CETs for the corresponding accident classes.

The staff has considered the adequacy of Westinghouse's treatment of systems and phenomena in the level 2 shutdown analysis. The staff notes that each of the systems modeled in the CETs are required to be available during shutdown by either technical specifications (RCS depressurization, containment isolation, and reactor cavity flooding) or short term availability controls (hydrogen igniters). The actuation/use of each of these systems is also specifically addressed in the emergency response guidelines. Thus, the failure probability for these systems in the shutdown PRA is small, as in the at-power PRA.

The fault trees for containment isolation do not address situations in which containment hatches, air locks, and spare penetrations are initially open and manual, local actions to close these penetrations are required to achieve containment closure. However, the technical specification concerning containment penetrations (TS 3.6.8) will not permit such penetrations to be open during shutdown unless the penetrations can be closed before steaming into the containment. Also, as described in SSAR Section 3.8.2.1.3 and the technical specification bases, each of the two equipment hatches in the AP600 design can be installed using a dedicated set of hardware, tools, and equipment, and a self-contained power source is provided to drive each hoist while lowering the hatch into position. Accordingly, the likelihood of failure to achieve containment closure is expected to be an insignificant contributor to containment failure.

The bases for TS 3.6.8 require any "equivalent isolation method" or temporary closure devices used in penetrations providing direct access from the containment atmosphere to the outside atmosphere to have a pressure capacity of at least 45 psig. Thus, these temporary closure devices would maintain their integrity in the more likely severe accidents, which typically involve peak containment pressures on the order of 30 psig.

Westinghouse considers use of the at-power split fractions in the shutdown CET conservative, since (1) the decay heat rates for shutdown events are substantially lower than at-power events, and (2) the hydrogen generation and combustion phenomena for shutdown would be similar to or bounded by the at-power case. Although the staff is not convinced that all aspects of events at shutdown are bounded by an equivalent analysis at power, the staff considers these qualitative arguments to be reasonable, and Westinghouse's approach acceptable for the purpose of this analysis, which is scoping in nature.

19.1.4.6.2 Shutdown Level 2 PRA Results

The large release frequency for events at shutdown is 1.5E-08/y, which is comparable to the large release frequency for at-power events (1.8E-08/y). The conditional containment failure probability is approximately 17 percent. In contrast, the large release frequency in the focussed PRA for shutdown is 3.3E-07/y. This is about a factor of 20 higher than the baseline shutdown PRA but still small in absolute terms.

The majority of the release frequency in the shutdown PRA is associated with events involving failure to flood the reactor cavity (68 percent in the baseline and 82 percent in the focussed PRA). Consistent with the treatment in the at-power PRA, failure of reactor cavity flooding is conservatively assumed to lead to containment failure. The dominant contributor to failure of cavity flooding is common cause failure of the IRWST strainers due to plugging. Events involving SGTR and containment isolation failures account for an additional 25 percent and 9 percent of the release frequency in the baseline PRA, respectively.

As discussed in Section 19.2.5 of this report, the COL applicant is expected to develop guidance and procedures for actions that may need to be taken in events during shutdown operations, including actions to flood the reactor cavity. This would reduce the potential for reactor vessel failure and basemat failure, and reduce the overall large release frequency.

19.1.5 Safety Insights from the External Events Risk Analysis

Three external events were analyzed in the AP600 PRA. These are seismic, internal fires and internal floods. In many PRAs performed to date, these external events have had combined CDFs that are the same magnitude as for internal events. It is not unusual to see the combined CDFs for these events in the 1E-04 per year range. The methods used in the AP600 PRA to evaluate external events are acceptable to the NRC because they provide the insights necessary to determine if any design or procedural vulnerabilities exist for these external events and because the methods provide insights needed for design certification requirements, such as ITAACs.

In SECY 93-087, the NRC identified the need for a site-specific probabilistic safety analysis and analysis of external events. Westinghouse did not perform an analysis (PRA or bounding) of the capability of the AP600 design to withstand external flooding, tornados, hurricanes, and other site-specific external events. Westinghouse did submit evaluations of seismic, fires, and internal flood events. The NRC requires, where applicable to the site, that the COL applicant perform a site-specific PRA-based analysis of external flooding, hurricanes, and other external events pertinent to the site to search for site-specific vulnerabilities. This is COL Action Item 19.1.5-1. In addition, the site-specific PRA should update the AP600 PRA to account for the detailed design of the as-built plant, with special emphasis on those areas of the design that

either were not part of the Certified Design or were not detailed in the certification. The site-specific PRA should be submitted at the time of the COL application and updated, as necessary, to account for ongoing first of a kind engineering. As stated previously this is COL Action Item 19.1.1-1.

19.1.5.1 PRA-Based Seismic Margin Analysis (SMA)

The AP600 is designed to withstand a 0.3g safe shutdown earthquake (SSE). Since the analyses used in designing the capability of structures, systems and components (SSCs) to withstand the SSE have significant margin in them, it is expected that a plant built to withstand the SSE actually will be able to withstand a much larger earthquake. A PRA-based margins analysis systematically evaluates the capability of the designed plant to withstand earthquakes without resulting in core damage, but does not estimate the CDF from seismic events. The margins analysis is a method for estimating the "margin" above the SSE, i.e., how much larger than the SSE an earthquake must be before it compromises the safety of the plant.

The capability of a particular SSC to withstand beyond design bases earthquakes is measured by the value of the peak ground acceleration (g-level) at which there is a high confidence that the particular SSC will have a low probability of failure (HCLPF). The HCLPF capacity of a certain SSC corresponds to the earthquake level at which, with high confidence (95 percent), it is unlikely (probability less than 5E-02) that failure of the SSC will occur. A HCLPF value for the entire plant is determined by finding the lowest sequence HCLPF that leads to core damage. It is a measure of the capability of the plant to withstand beyond design basis earthquakes without resulting in core damage. The plant HCLPF value, which is assessed from the SSC HCLPF values, has units of acceleration. The NRC has indicated (SECY-93-087) that a plant designed to withstand a 0.3g SSE should have a plant HCLPF value at least 1.67 times the SSE (i.e., 0.5g). The PRA-based seismic margins analysis shows that the AP600 design meets (and likely exceeds) the 0.5g HCLPF value expectation, and is therefore, acceptable.

No credit is taken in the risk-based SMA for the non-safety-related "defense-in-depth" systems. Since such systems are not seismic Category I, it is conservatively assumed that they become unavailable as a consequence of the seismic initiating event. Since the non-safety-related diesel generators are assumed to be unavailable and the failure with the lowest HCLPF value which would initiate an accident is the loss of offsite power (HCLPF of ceramic insulators is 0.09g), all accident sequences are treated in the SMA as station blackout (SBO) sequences. The potential for adverse interactions between assumed seismically-damaged non-safety-related SSCs and safety-related systems was investigated and accounted for in the analysis. The event and fault trees developed for the internal events PRA were modified to accommodate seismic events. In this way the random failures and human errors modeled in the internal events portion of the PRA are captured in the seismic analysis. The modified event and fault trees were merged and cutsets for all sequences that lead to core damage were generated. These cutsets are of two kinds. One kind contains only seismic failures (i.e., without any random failures or human errors). The other kind contains random failures and/or human errors in addition to seismic failures. In "quantifying" these cutsets, the HCLPF values of the seismic events (instead of mean values of failure probabilities) were used, while the probabilities of random failures and human errors are the same as for the internal events PRA. Most of the HCLPF values for components and structures were obtained using the conservative deterministic failure margin (CDFM) approach or the Probabilistic Fragility Analysis approach or

the Deterministic approach (NUREG/CR-4482, 1986 and EPRI NP-6041, 1988). For electrical equipment, for which documented test results are available, the HCLPF values were obtained by comparing required response spectra to test response spectra for similar types of equipment. Generic fragility data was used when insufficient information was available to determine the HCLPF value by using one of the above mentioned approaches. The min/max approach[2] was used for the sequence and plant level HCLPF calculations. A review of these calculations was conducted by the staff and were found to be acceptable. Additional background information about the seismic margins methodology and its implementation to the AP600 can be found in Appendix 19A.

19.1.5.1.1 Dominant Accident Sequences for Seismic Events

Westinghouse identified "dominant" accident sequences for seismic events. The word dominant appears in quotes to emphasize that the terminology in the context of a seismic margins study is not the same as in a conventional PRA. While these sequences (and associated cut sets) dominate the HCLPF values for the plant, the margins approach does not permit a determination that these are the dominant contributors to seismic risk in a probabilistic sense. If random failures and human errors are ignored (i.e., when cutsets containing seismic failures only are considered), the plant HCLPF was estimated to be at least 0.5g. Since the plant HCLPF can be lower when certain random failures (or human errors) occur simultaneously with the seismic failure of certain SSCs, cutsets containing both seismic and non-seismic failures were examined to find out if there were any cutsets which would lower the plant HCLPF below 0.5g. For earthquakes that generate higher accelerations than the plant HCLPF value, there is no longer the same high degree of confidence that core damage will not occur. However, because a cliff-effect is not likely at or near the plant HCLPF value, the plant will most likely have some seismic margin above the plant HCLPF value (i.e., capability to withstand seismic events that generate higher accelerations than the plant HCLPF value).

The following five "dominant" seismic core damage sequences were identified by the risk-based seismic margins analysis. They have the lowest HCLPFs (when cutsets with seismic only failures are considered) or the lowest combination of HCLPF with random failure/human error (when cutsets with both seismic and non-seismic failures are considered).

Seismic sequence #1, with HCLPF value 0.5g, is a seismically-induced break of the reactor coolant system pressure boundary which results in loss of coolant beyond the capacity of the emergency core cooling system (ECCS) to provide makeup. This leads directly to core damage. Major contributors are fuel failure (HCLPF value 0.5g), steam generator failure (HCLPF value 0.65g) and pressurizer failure (HCLPF value 0.67g). This scenario, which is also assumed to lead to a large fission product release due to loss of containment integrity, determines the HCLPF value for the entire plant with respect to both CDF and LRF (i.e., 0.5g).

Seismic sequence #2, with HCLPF value 0.51g, is a seismically-induced ATWS event and failure of the ADS. The most important cutsets, associated with this sequence, involve failure of

---

[2] In the min/max approach if there is an "ORed" sequence where the failure of any individual SSC would cause core damage, we take the lowest individual SSC HCLPF as the sequence HCLPF. If there is an "ANDed" sequence where the failure of all SSCs would cause core damage, we take the highest individual SSC HCLPF as the sequence HCLPF.

reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value of 0.51g) combined with failure of the Class 1E 120V ac control power (HCLPF value of 0.51g) which causes failure of ADS. The most important contributors to the seismically-induced failure of the Class 1E 125V ac power are (1) failure of the 125V dc distribution panels (0.51g), (2) failure of the 120V ac distribution panels (0.51g), (3) failure of the 125V dc switchboard (0.51g), (4) failure of the transfer switch (0.51g) and (5) failure of the cable tray (0.54g).

Seismic sequence #3, with HCLPF value 0.58g, is a seismically-induced structural collapse of parts of the nuclear island. Major contributors are collapse of (1) shield building wall or roof (0.58g), (2) passive containment cooling water tank (0.58g), (3) an interior (concrete) structure of containment (0.60g), and (4) IRWST structure (0.60g).

Seismic sequence #4, with HCLPF value 0.63g, is a seismically-induced ATWS event with failure of the CMTs. The most important cutset, associated with this sequence, involves failure of reactor internals or core assembly which causes failure of the control rods to insert (0.51g) combined with failure of the CMTs (0.63g).

Seismic sequence #5, is a seismically-induced ATWS event that happens to occur during the "unfavorable exposure time" of the plant (i.e., early in the fuel cycle when an adverse moderator temperature coefficient exists). This is the most important sequence containing both seismic and non-seismic failures. It involves the seismically induced failure of reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value 0.51g) combined with an unfavorable exposure time (probability 0.33).

It should be noted that the analysis did not identify any important sequence containing mixed cutsets (i.e., cutsets made up of both seismic and non-seismic failures) where the HCLPF of the seismic portion is less than the plant HCLPF value (i.e., less than 0.5g). This means that there are no random failures or human errors likely to occur in a seismically-initiated accident sequence that would lower the plant HCLPF below 0.5g.

Westinghouse also performed a bounding analysis, using simplified conservative assumptions, to identify paths by which the containment could be bypassed, fail to isolate, or fail. This analysis assumes that the containment fails when the reactor vessel fails due to failure of the fuel (HCLPF value 0.5g). Thus, the plant HCLPF for large release is assumed to be the same as for core damage. Since the plant HCLPF is at least 0.5g, the plant HCLPF is in accordance with SECY-93-087, and is therefore, acceptable. Westinghouse performed a SMA for plant operation at power only. The staff examined the event tree models used in the internal events PRA for shutdown operation, using the SMA models and results performed for power operation, and concluded that the plant HCLPF value is at least 0.5g even during plant shutdown.

19.1.5.1.2 Risk Important Features and Operator Actions for Seismic Events

The margins approach does not allow a determination of which plant features are most important to risk using importance analyses. The margins approach does allow one to determine which plant features are important to the plant level HCLPF and the redundancy/diversity available in achieving that HCLPF. In order to make this determination, the staff examined each sequence that leads to core damage on the seismic event trees. None of the sequences has a seismic-only HCLPF less than 0.5g. The sequences were examined to

determine if lowering the HCLPF value of a single SSC (to a much lower HCLPF value) or increasing the demand failure rate of a single system (to a much high demand failure rate) would result in a plant HCLPF less than 0.5g.

Important insights about the capability of the AP600 design to withstand earthquakes that were drawn from the examination of the SMA results (accident sequences and associated cutsets) are summarized below.

- The majority of the seismic sequences require multiple failures of SSCs whose HCLPF is greater than 0.5g in order to drive the plant to core damage. A check of the capacity of as-built SSCs to meet the HCLPFs assumed in the AP600 PRA will be provided by a seismic walkdown whose details are to be developed by the COL applicant. This is COL Action Item 19A.2.5-1 (see Section 19A of this report).

- There is a number of important safety-related structures whose seismically-induced failure would lead directly to core damage. These include the fuel in the reactor vessel (0.50g), the shield building wall or roof (0.58g), the passive containment cooling water tank (0.58g), an interior (concrete) structure of containment (0.60g), the IRWST structure (0.60g), the steam generators (0.65g), and the pressurizer (0.67g). The seismic margins analysis assumes that these structures will all have HCLPF values in excess of 0.5g. If any of these structures were built with a HCLPF lower than 0.5g, the plant HCLPF would also be lower than 0.5g.

- There is a number of accident sequences which include cutsets with multiple seismic failures (i.e., two or more seismic failures are required for core damage to occur) but only one of these events has a HCLPF value which is considerably higher than the plant HCLPF value (the other events in the cutset have HCLPF values equal to or just above the plant HCLPF value). If the value of this event is reduced to about 0.5g or below, the plant HCLPF will not change but there will be additional sequences with HCLPF value in the neighborhood of the plant HCLPF. Sequences containing these kind of cutsets are as follows:

  - ATWS sequences which involve failure of the reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value 0.51g) in combination with one other failure whose HCLPF is considerably higher than the plant HCLPF value of 0.5g, such as IRWST injection check valves (0.96g) and squib valves (0.96g)

  - LOCA sequences which involve failure of Class 1E electrical components, such as the 125V dc and the 120V ac distribution panels (0.51g), in addition to the LOCA initiating failure (0.81g)

- The analysis did not identify any important sequence containing mixed cutsets (i.e., cutsets made up of both seismic and non-seismic failures) where the HCLPF of the seismic portion is less than the plant HCLPF value (i.e., less than 0.5g). The only sequences containing seismic/random combinations (mixed cutsets) which would lower the plant HCLPF below 0.5g, when certain non-seismic (random) failures occur, are loss of offsite power sequences which are initiated by failure of the ceramic insulators (HCLPF value 0.09g). However, the probability of such random failures occurring is

extremely remote (in the range of 1E-07 or less). This means that it is highly unlikely that random failures or human errors would occur in a seismically-initiated accident sequence and would lower the plant HCLPF below 0.5g.

- The same human error rates and random failure rates that were used in the AP600 internal events analysis were also used in the SMA. The PRA-based SMA did not identify any human reliability insights that were not already identified in the internal events analyses. An examination of the top mixed cutsets shows that human errors are not significant contributors to non-seismic failure probabilities.

The following is a list of important design features which contribute to the capability of AP600 to withstand earthquakes.

- There are no safety-related SSCs with HCLPF values less than 0.50g.

- The reliance on passive safety-related systems and dc power for accident mitigation, minimizes the impact of non-seismic (random or human) failures on the plant HCLPF value.

- "Defense-in-depth" with respect to seismically induced failures. The only single seismically-induced failures that would lead directly to core damage involve gross collapse of structures in the nuclear island, such as failure of the fuel in the reactor vessel (0.50g) or collapse of the auxiliary building roof (0.58g). Such failures control the plant level HCLPF.

- No safety-related equipment is located outside the nuclear island.

- No interaction between the nuclear island and any other structures has a detrimental impact on nuclear island structures. A potential indirect seismic interaction is possible between the turbine building (designed to the Uniform Building Code requirements) and the auxiliary building (a seismic Category I structure). An access bay protects important safety-related I&C equipment as well as the main control room and the remote shutdown panel, located in the north end of the auxiliary building, from potential debris produced by a postulated seismically-induced structural collapse of the adjacent turbine building.

- The fragility of valve rooms labeled 11206/11207 where the passive core cooling system valves are concentrated is an important factor in the AP600 capability to withstand earthquakes. A check of the capacity of as-built SSCs to meet the HCLPFs assumed in the AP600 PRA will be provided by a seismic walkdown and whose details are to be developed by the COL applicant. As stated previously this is COL Action Item 19A.2.5-1.

19.1.5.1.3 Insights from Uncertainty, Importance, and Sensitivity Analyses for Seismic Events

One of the reasons for performing an uncertainty analysis is to display the range of values within which the results of an analysis could reasonably be expected to fall. The use of a PRA-based seismic margins analysis inherently makes use of the breadth of information being

considered. This is because HCLPF values can be thought of as the g-level at which one has 95 percent confidence that less that 5 percent of the time the equipment will fail (i.e., the tails of the curves). It was not found necessary to combine (use convolution) a seismic hazards analysis with equipment fragilities, since hazard curves have a large uncertainty which reduces their value in helping to make judgements about the seismic risk. From seismic PRA analyses, it is clear that uncertainties in the hazard curves would dominate the uncertainties in equipment/structure fragilities. For the AP600 PRA-based SMA, no uncertainty analyses was performed because uncertainty is directly reflected in the margins method. Also, since the margins method does not quantify risk (e.g., in terms of core damage frequency), importance analyses were not performed. Westinghouse did, however, perform sensitivity analyses to evaluate the effects of changes in certain assumptions used in the SMA. The most important insights from the sensitivity studies are listed below.

- A decrease in the "generic" HCLPF values assumed in the SMA for several SSCs, such as ADS MOVs (0.81g) and pipe supports (0.81g), will not impact the plant HCLPF as assessed in the SMA. However, decreasing such "generic" HCLPF values will impact the results. This is not surprising since they affect large numbers of components. There are always one or more sequences whose HCLPF is controlled by one or more of the components with "generic" HCLPFs, so it is necessary to assure that these HCLPFs are not inappropriately low in the as-built plant (this will be confirmed by the COL applicant during a seismic walkdown of the as-built plant. This process is part of COL Action Item 19.1.5-2.

- Increasing the fuel and core assembly HCLPF values (from 0.5g to any value above 0.58g), the plant HCLPF will increase to 0.58g and will be dominated by structural failures in the auxiliary and shield buildings (HCLPF value 0.58g).

- Increasing the fuel HCLPF value from 0.5g to any value above 0.51g (but keeping the core assembly HCLPF at 0.5g), the plant HCLPF will increase to 0.51g and will be dominated by the failure of the Class 1E 125V ac power (HCLPF value 0.51g).

- Since the HCLPF associated with equipment needed to support an operator action is 0.51g (driven by failure of the dc power), increasing the dc power HCLPF value would allow more recovery actions following earthquakes that generate acceleration levels above the plant HCLPF.

- The plant HCLPF or the SMA insights about the AP600 design are not impacted by potential, but unlikely, seismic interactions between the turbine building and the auxiliary building.

- Since no credit is taken in the SMA for the non-safety-related "defense-in-depth" systems to mitigate seismic events and the SMA has shown that the plant HCLPF is at least two-thirds the ground motion acceleration of the design-basis SSE (SECY-93-087), the results of the SMA do not impact the probabilistic criteria (see Section 19.1.7 of this report) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

19.1.5.2 Internal Fires Risk Analysis

Westinghouse performed a fire risk analysis, for both at-power and shutdown conditions, to search for potential design vulnerabilities and identify important safety insights about the AP600 design needed to support certification requirements, such as ITAACs. The analysis uses 1) available plant-specific design information, including the locations of major equipment and cables, of rated fire barriers, and automatic detection and suppression equipment; 2) industry fire safety data, including the frequency of fires in different compartments, the reliability of automatic and manual suppression, the reliability of fire barriers; and 3) the plant internal events PRA model (without credit for the "defense-in-depth" non-safety-related systems) to assess the CDF associated with internal fire. The approach used is a modified Fire Induced Vulnerability Evaluation (FIVE) methodology (EPRI TR-100370, 1992) and is generally consistent with fire risk assessment methods used to evaluate conventional plants (e.g., NUREG/CR-2300, 1983 and NUREG/CR-4840, 1989).

In general, the fire PRA is performed largely as a screening level analysis and employs a number of conservative assumptions. Somewhat less conservative assumptions are employed for two fire areas[3], i.e., the containment and the main control room (MCR). Key features of the fire PRA are as follows.

- For most fire areas, the analysis assumes that, given a fire in the area, all of the equipment in the area is lost. Thus, the analysis does not take credit for the possibility of fire self-extinguishment or suppression before the loss of equipment within the affected area. This treatment is likely to be quite conservative for most plant areas. However, it may only be slightly conservative for plant areas housing sensitive electronic components, since these are more susceptible to the effects of heat, humidity, and smoke.

- For the containment and the MCR, the analysis is more detailed. Based on the separation of equipment within each area, fire scenarios involving subsets of equipment are identified and analyzed. In the case of the MCR, the analysis accounts for the possibility that MCR fires are extinguished before they cause equipment damage or MCR evacuation.

- The analysis allows for the possibility of fire growth into a second fire area when the barrier between two areas contains any type of penetration. The likelihood of automatic suppression system failure (if such a system is installed) and the likelihood of barrier failure are used in determining the likelihood of fire growth. If growth occurs, it is assumed that all equipment in both areas is lost. The analysis considers only the possibility of fire growth to one adjacent fire area (i.e., it is assumed that the likelihood of growth to multiple areas is negligible).

---

[3]The AP600 fire areas are defined in the SSAR. They are separated from each other by fire barriers with ratings of 2 hours or more. A fire area can be separated into "fire zones" which are defined for analytical convenience and need not be separated by barriers.

- The analysis explicitly treats the possibility of fire-induced spurious actuations of ADS squib valves. Fire-induced hot shorts in relevant safety- and DAS-related cables and cabinets are treated as leading to medium LOCA (MLOCA) or large LOCA (LLOCA) scenarios when the reactor is at power. Fire-induced MLOCA scenarios are also treated when the reactor is shutdown (but not in mid-loop). Credit is not taken for the potential use of fiber optics cabling and digitally encoded signals in portions of the control system.

- The analysis employs the "focused" PRA model to determine the conditional core damage probability, given the loss of a set of equipment due to fire. Such model does not take credit for the performance of the non-safety-related "defense-in-depth" systems.

- The analysis treats the possibility of operator recovery actions. These actions involve the manual actuation of equipment from the MCR or the remote shutdown workstation (RSW) as backup to automatic actuation (actions by local equipment operators are not credited). Consequently, the human error probabilities used in the recovery analysis are not modified to reflect fire-specific impacts on operator performance. The analysis relies on two important assumptions. First, a large fire in the MCR or RSW will not affect the automatic actuation of equipment. Second, ex-MCR or RSW activities, e.g., coordination of fire-fighting activities and plant response, will not place any significant additional burden on the MCR operators.

- The hot/cold shutdown (HCSD) and mid-loop (ML) analyses are performed in a manner very similar to that used for the at-power analysis. The primary difference is in the containment fire frequencies (transient fires not considered in the at-power analysis are included in the HCSD and ML analyses).

The AP600 fire PRA reflects the generally strong separation between the four safety-related power and control divisions. The only plant fire areas containing all four divisions are the MCR, the RSW area, and the containment. The MCR is continuously manned and the RSW area is not normally enabled. Additionally, because of the AP600's digital I&C design, fires within these areas are not expected to inhibit the automatic actuation of safe-shutdown equipment. Within the containment, redundant divisions are generally separated by continuous structural or fire barriers without penetrations and by labyrinth passageways (in a few cases, the divisions are separated by large open spaces without intervening combustibles). Because of the general divisional separation and the I&C design, a single fire in the plant is not expected to damage enough equipment to cause core damage; additional (non-fire caused) failures are required for this to occur.

19.1.5.2.1 Dominant Accident Sequences Leading to Core Damage for Internal Fires

Westinghouse quantified the CDF associated with internal fires, for both at power operation and during shutdown, by using applicable event and fault tree models from the internal events PRA. The fire-induced CDF was assessed to be about 6.5E-07/year for fires occurring during power operation and about 5E-07/year for fires occurring during shutdown. Westinghouse considers the above mentioned CDF estimates to be conservative upper bounds (based on conservative bounding assumptions made in the analysis). The staff believes that such a conclusion is not possible without a detailed PRA. The staff's review did not concentrate on bottom-line numbers

but rather on important modeling assumptions and the relative insights that the internal fires analysis provides about the design. Based on this information, the staff was able to conclude that the AP600 design is capable of withstanding severe accident challenges from internal fires in a manner superior to most, if not all, operating plant designs. The internal fires PRA has provided useful safety insights for inclusion in ITAAC, COL Action Items, and RAP. Since detailed PRA-based internal fires analyses at some operating plants have shown that fires-induced sequences can be leading contributors to CDF, the COL applicant should provide an updated internal fires PRA that takes into account design details (e.g., cable routing, door and equipment locations and fire detection and suppression system locations) to search for internal fire vulnerabilities in the detailed design. This is COL Action Item 19.1.5-3.

Operation at power

The top six internal fire scenarios, contributing about 90 percent of the total CDF from internal fires at power operation, are summarized below.

Fire scenario #1, contributing about 47 percent, is initiated by a fire inside the containment (fire area 1000 AF 01). The dominant contributing area is the operating deck (1100 AF 11500 fire zone). Additional significant contributors are fires in the maintenance floor above platform (1100 AF 11300C fire zone) and in the ADS lower and upper valve areas (fire zones 1100 AF 11303A & 11303B). A fire in any of these areas is assumed to fail or degrade the actuation of all in-containment safety-related equipment supported by cabling passing through that area. In addition, it was assumed that "hot shorts" could occur that would spuriously open a certain number of ADS valves causing a medium or large LOCA (a single "hot short" causes a medium LOCA while a multiple "hot short" causes a large LOCA).

- A fire in the operating deck (1100 AF 11500 fire zone) is assumed to fail all in-containment safety-related equipment supported by divisions A and C (cabling from these two divisions passes through this area). In addition, it was assumed that "hot shorts" could occur in cables that would spuriously open ADS valves (supported by divisions A & C) causing a LOCA. The fire scenario that dominates the CDF associated with fires in the operating deck is a fire-induced single "hot short" which causes a medium LOCA and at the same time fails or degrades the reliability of all equipment supported by divisions A & C of power and control, such as the affected ADS valves and train B of IRWST injection/containment recirculation systems.

- A fire in the maintenance floor above platform (1100 AF 11300C fire zone) is assumed to fail or degrade the reliability of all in-containment safety-related equipment supported by division A (cabling from this division passes through this area). In addition, it was assumed that "hot shorts" could occur in cables that would spuriously open ADS valves (supported by division A) causing a LOCA. The fire scenario that dominates the CDF associated with fires in the maintenance floor (above platform) is a fire-induced single "hot short" which causes a medium LOCA and at the same time fails all equipment supported by division A of power and control, such as one CMT.

- A fire in the ADS lower and upper valve areas (fire zones 1100 AF 11303A & 11303B) is assumed to fail or degrade all in-containment safety-related equipment supported by two divisions (B&D for the upper valve area, A&C for the lower valve area). In addition,

it was assumed that "hot shorts" could occur in cables that would spuriously open ADS valves. The fire scenario that dominates the CDF associated with fires in the ADS upper and lower valve areas is a fire-induced single "hot short" which causes a medium LOCA and at the same time fails or degrades all equipment supported by two divisions of power and control, such as the affected ADS valves and one train of IRWST injection and containment recirculation systems.

Fire scenario #2, contributing about 14 percent, is initiated by a fire in the division C of class 1E electrical and I&C equipment area (fire area 1202 AF 03). The dominant contributor to this scenario is a fire-induced single "hot short" causing a medium LOCA with division C of power and control unavailable.

Fire scenario #3, contributing about 9 percent, is initiated by a fire in the division D of class 1E electrical and I&C equipment area (fire area 1201 AF 03). The dominant contributor to this scenario is a fire-induced single "hot short" causing a medium LOCA with division D of power and control unavailable.

Fire scenario #4, contributing about 9 percent, is initiated by a fire in the division A of class 1E electrical and I&C equipment area (fire area 1202 AF 04). The dominant contributor to this scenario is a fire-induced single "hot short" causing a medium LOCA with division A of power and control unavailable.

Fire scenario #5, contributing about 6 percent, is initiated by a fire in the division B of class 1E electrical and I&C equipment area (fire area 1201 AF 02). The dominant contributor to this scenario is a fire-induced single "hot short" causing a medium LOCA with division B of power and control unavailable.

Fire scenario #6, contributing about 4 percent, is initiated by a fire in the non-class 1E electrical equipment/penetration room (fire area 1200 AF 04). The dominant contributor to this scenario is a fire-induced single "hot short" (in DAS cables) causing a medium LOCA with loss of reactor trip signals from electrical divisions B and D.

The AP600 PRA predicts the at-power fire risk to be dominated by fire-induced medium LOCAs. They account for 85 percent of the fire-induced CDF. Most of the remaining CDF (11 percent) is attributed two fire-induced large LOCAs postulated as a result of multiple "hot shorts" causing spurious actuation of two ADS stage #4 squib valves. The final 4 percent contribution to the fire-induced CDF is attributed to loss of offsite power and transients. With respect to fire areas (or zones), the AP600 PRA predicts that about half (47 percent) of the fire-induced CDF during power operation is associated with fires inside the containment and that most of the remaining contribution is associated with fires in the electrical areas of the auxiliary building. The PRA predicts an almost insignificant contribution to CDF from fires in the MCR. Due to differences in the level of conservatism employed in the analysis for the various areas of the plant (e.g., the analysis for postulated fires in the MCR is more detailed and less conservative than the analysis for the auxiliary building), a comparison of contributions to risk from the various plant areas will not yield useful results. The staff, however, finds that this analysis is adequate for the purpose of identifying potential vulnerabilities and for gaining insights about the design which can be used to support design certification requirements, such as ITAACs.

An examination of the dominant cutsets (Table 57-12 of the AP600 PRA) shows that none of the identified internal fire events leads to core damage unless additional random (i.e., non-fire related) failures occur. However, about 40 percent of the dominant cutsets involve a single non-fire basic event. For example, the top ranked cutset involves a fire-induced MLOCA (due to hot short actuation of 1 ADS Stage 4 valve) and loss of one division of power and control (including failure of one of the two IRWST injection lines), combined with a random failure of the output logic group 1 input/output board. Most of the random failures involve common cause failure (CCF) of electrical, mechanical, or I&C equipment and software. However, a number of these failures involve single component failures. Thus, the AP600 fire PRA predicts that there may be scenarios (although of low probability) where a single fire has the capability of bringing the plant within one failure of core damage. This conclusion, however, may be biased because of the conservatism used in the analysis. For example, a further examination of cutsets involving a single random failure which is a single component failure, shows that they would not lead to core damage (i.e., they would not be cutsets) had non-safety-related "defense-in-depth" systems, such as DAS and RNS, been credited in the fire risk analysis. Availability control of such "defense-in-depth" systems, according to the RTNSS process, averts potential situations where a single fire has the capability of bringing the plant within one failure of core damage.

Low Power and Shutdown Operation

The PRA predicts the fire-induced CDF during shutdown (about 5E-07/year) to be dominated by fires occurring while the plant is in the ML mode of operation (about 95 percent contribution). The dominant fire scenarios, contributing over 80 percent of the total CDF from internal fires at low power and shutdown operation are summarized below. (All take place while the plant is in the mid-loop mode of operation.)

Fire scenario #1, contributing about 18 percent, is initiated by a fire in the Yard/Outlying Building (fire area 0000 AF 00) while the plant is in the ML mode of operation. Such a fire is assumed to cause a non-recoverable loss of offsite power. This causes failure of decay heat removal by the normal residual heat removal system (RNS) since no credit for on-site ac power is taken in the fire PRA. Subsequent random failure to remove decay heat by IRWST injection leads to core damage.

Fire scenario #2, contributing about 17 percent, is initiated by a fire inside the containment (fire area 1000 AF 01) while the plant is in the ML mode of operation. The dominant contributing areas are the operating deck (fire zone 1100 AF 11500) and the main control room emergency habitability system (VES) air storage/operating deck staging area (fire zone 1250 AF 12555). Additional significant contributors are fires in the maintenance floor (1100 AF 11300B & 11300C fire zones). A fire in any of these areas is assumed to fail one or two safety-related divisions of power and control. Such failures combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection lead to core damage.

Fire scenario #3, contributing about 10 percent, is initiated by a postulated fire in the division C of class 1E electrical and I&C equipment area (fire area 1202 AF 03) while the plant is in the ML mode of operation. Such a fire is assumed to disable division C of safety-related power and control. This combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection leads to core damage.

Fire scenario #4, contributing about 10 percent, is initiated by a postulated fire in non-class 1E electrical switchgear room #1 (fire area 4042 AF 01) while the plant is in the ML mode of operation. Such a fire is assumed to disable one non-class 1E electrical and DAS. Such failures combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection lead to core damage.

Fire scenario #5, contributing about 6 percent, is initiated by a postulated fire in division B RCP trip switchgear area (fire area 1220 AF 01) while the plant is in the ML mode of operation. Such a fire is assumed to disable division B of safety-related power and control. This combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection leads to core damage.

Fire scenario #6, contributing about 6 percent, is initiated by a postulated fire in the Generator Panel room of the turbine building (2053 AF 01 fire area) while the plant is in the ML mode of operation. Such a fire is assumed to cause the loss of offsite power. This, in turn, causes failure of decay heat removal by RNS since no credit for on-site ac power is taken in the fire PRA. Subsequent random failure to remove decay heat by IRWST injection leads to core damage.

Fire scenarios #7 and #8, each contributing about 5 percent, are initiated by a postulated fire in the divisions A and D of class 1E electrical and I&C equipment, respectively (fire areas 1202 AF 04 and 1201 AF 03, respectively) while the plant is in the ML mode of operation. Such a fire is assumed to disable one division of safety-related power and control. This combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection leads to core damage.

Fire scenarios #9, contributing about 3 percent, is initiated by a postulated fire in the division B of class 1E electrical and I&C equipment (fire area 1201 AF 02) while the plant is in the ML mode of operation. Such a fire is assumed to disable division B of safety-related power and control. This combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection leads to core damage.

Fire scenario #10, contributing about 2 percent, is initiated by a postulated fire in non-class 1E electrical switchgear room #2 (fire area 4042 AF 02) while the plant is in the ML mode of operation. Such a fire is assumed to disable one division of the non-class 1E electrical system and DAS. Such failures combined with random failure or unavailability of decay heat removal by RNS or by IRWST injection leads to core damage.

Fire scenario #11, contributing about 2 percent, is initiated by a fire in the radiologically control area (RCA) of the auxiliary building (1200 AF 01 fire area) while the plant is in the ML mode of operation. Such a fire is assumed to cause failure of the RNS system. Subsequent random failure to remove decay heat by IRWST injection leads to core damage.

None of the identified internal fire events during shutdown operation leads to core damage unless additional random failures occur. An examination of the dominant fire scenarios show that (1) the fire-induced CDF during shutdown is dominated by events (fires) occurring during the mid-loop mode of operation, (2) there are no dominant contributing fire areas to the fire-induced CDF during shutdown (contributions are distributed over the entire plant although some areas are more important contributors than others), and (3) no additional insights were

identified in the fire PRA regarding random failures that were not already identified in the internal events analyses.

19.1.5.2.2 Risk Important Design Features and Operator Actions for Internal Fires

The following is a list of important design features which contribute to the reduced fire risk associated with the AP600 design as compared to operating reactors.

- Separation of divisions. In most areas of the plant, the 4 safety-related electrical divisions (Divisions A through D) are in separate fire areas, i.e., they are separated barriers of at least 2-hour fire rating or equivalent. In particular, the major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms) are separated by 3-hour rated fire walls without openings. There are no doors, dampers, or seals in these walls. The rooms are served by separate ventilation subsystems. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).

- Separation of automatic actuation systems from main control room (MCR) and remote shutdown workstation (RSW). The MCR and the RSW are the only two plant areas where all 4 divisions can be affected by a single fire with significant likelihood. For fires in these areas, the plant is designed to have an independent, automatic means to reach safe shutdown. (In fact, operator actions from the MCR and RSW are not required according to the design; these actions are treated as backups to the automatic response.)

- Separation of safety divisions within containment. The containment is the third fire area containing all 4 divisions. Redundant divisions are generally separated by "continuous structural or fire barriers without penetrations and by labyrinth passageways." In a few situations, the divisions are separated by large open spaces without intervening combustibles.

- There is no cable spreading room in the AP600 design.

- No safety-related equipment is located in the turbine building. There is a 3-hour fire barrier wall between the turbine building and the safety-related areas of the nuclear island.

- The vast majority of cables in the MCR are low voltage; this is expected to reduce the likelihood of self-ignited fires.

- If control room evacuation is necessary, the RSW provides complete redundancy in terms of control for all safe shutdown functions.

- Digital I&C and fiber optics cabling (not credited in the PRA). These features are believed to greatly reduce the likelihood of spurious fire-induced I&C signals for the following reasons:

  - fire induced failures of fiber optic cabling are expected to cause an interruption of optical signals and not spurious signals

  - even where conventional wires and cables are employed, fire induced faults are not expected to result in meaningful commands (the commands are digitally encoded)

  - the I&C system employs error checking routines to identify and deal with faulty signals

A fire can, of course, still affect the analog portions of the I&C system. It should be noted that the use of digital I&C is expected to increase the likelihood of fire-induced loss of function in the I&C equipment (cabinet) rooms, due to the sensitivity of the I&C electronic components to heat, smoke, and humidity (from suppression activities). The AP600 fire PRA accounts for this sensitivity by conservatively assuming the loss of all equipment in a fire area if a fire occurs. However, the degree of conservatism of this assumption is believed to be relatively small for the I&C rooms (as compared to other areas of the plant which contain more rugged components).

- The same human error rates and random failure rates that were used in the AP600 internal events analysis were also used in the internal fires analysis. The fire PRA did not identify any human reliability insights that were not already identified in the internal events analyses. The AP600 design is significantly less dependent on human actions to mitigate internal fires than operating reactors.

19.1.5.2.3 Insights from Uncertainty, Importance, and Sensitivity Analyses for Internal Fires

No uncertainty and importance analyses were performed by Westinghouse for internal fires. Due to the conservatism in the approach taken in performing the AP600 internal fire PRA, Westinghouse judged that uncertainty and importance analyses would result in biased insights. Since no credit was taken for the non-safety-related "defense-in-depth" systems, the results and insights of the fire risk analysis can be used directly in the criteria for selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process. The fire-induced CDF estimate (for both at power and during shutdown operation) is based on conservative assumptions and still is about an order of magnitude smaller than the CDF estimate for internal events obtained with the "focused" PRA model (i.e., when no credit is taken for the non-safety-related "defense-in-depth" systems). This means that the fire PRA results do not have a significant impact on the probabilistic criteria (reported in Section 19.1.7) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

The AP600 fire PRA predicts the at-power fire risk to be dominated by fire-induced spurious actuation of ADS valves leading to medium size LOCA events (85 percent contribution). A sensitivity study was performed by the staff, using Westinghouse's PRA models and results, to gain insights about the impact of uncertainties in modeling spurious actuation of ADS valves on plant fire risk. Hot shorts, especially in I&C copper cables from the protection logic cabinets

(PLCs) to the squib valve operators, could cause detonation of the squib valves. The AP600 PRA uses a "hot short" probability on the basis of a distribution provided in NUREG/CR-2258, 1981. Changes in the probabilities of single and double hot shorts will directly affect the medium, and to a lesser extent the large, LOCA contributions which dominate the fire CDF. For example, increasing the single "hot short" probability by about a factor of three (to the 95th percentile of the distribution presented in NUREG/CR-2258, 1981) without changing the relative uncertainty in the hot short probability causes the fire CDF to increase by about a factor of 6 (from 6.5E-07/year to 3.7E-06/year). This issue is of special concern because the technical basis for the AP600 estimates of "hot short" probabilities (both single and multiple) is not strong (the distribution, reported in NUREG/CR-2258, was developed from a subjective consideration of information available at the time (1981)). In addition, it is not clear if this distribution is directly applicable to the AP600 cables or whether it is conservatively or optimistically biased for the AP600 application. The significant uncertainty in the hot short probability underlines the importance of cable routing and the incorporation of features and requirements in the detailed design of ADS cabling which will minimize the probability of hot shorts actuating an ADS squib valve. Such features/requirements include using a squib valve controller circuit which requires multiple hot shorts for actuation, physical separation of potential hot short locations (e.g., routing of ADS cables in low voltage cable trays and use of redundant series controllers located in separate cabinets), and provisions for operator action to remove power from the fire zone.

19.1.5.3 Internal Flooding Risk Analysis

Due to the lack of detailed design information needed to identify exactly the potential flood sources and flood levels, such as pipe routings, drain capacities and locations, and other flood mitigating devices like sloped floors or curbs, Westinghouse chose not to perform a detailed PRA to assess the risk from internal flooding associated with the AP600 design. Instead, Westinghouse performed an internal flooding PRA which is commensurate with the level of detail available and making conservative assumptions, where detailed information was not available, to bound the flooding analysis. The staff finds that this analysis is adequate for the purpose of identifying potential vulnerabilities and for gaining insights about the design which can be used to support design certification requirements, such as ITAACs.

The performance of the internal flooding PRA included four stages. During the first stage, information required to perform the flooding analysis was collected, such as identifying areas that contain potential flooding sources and/or equipment required for plant operation and safe shutdown of the plant. During the second stage, an initial screening of the areas identified during the first stage was accomplished, using conservative assumptions (e.g., total immersion and failure of equipment in affected areas) and taking into account the potential for propagation to other areas, to identify areas where flooding could cause a reactor trip or affect safe shutdown. During the third phase, a detailed screening of the areas identified in the second stage was accomplished (e.g., by determining maximum expected flood height, evaluating the potential for spray of safe-shutdown equipment and the potential for propagation into other areas), to identify plant areas where flooding could have an impact on safe-shutdown equipment modeled in the internal events PRA. During the forth stage, the risk from flooding in the areas which were not screened out during the second and third stages was quantified using models, with appropriate assumptions, from the internal events analysis.

In performing the AP600 internal flooding PRA, Westinghouse considered all of the buildings and locations in the screening phase of the study. Buildings in which an internal flood could result in a reactor trip or affect safe shutdown are the nuclear island (Containment Building and auxiliary building), the annex building, the turbine building, the Diesel Generator Building, and the Circulating Water Pumphouse. The second (initial screening) and third (detailed screening) stages of the study resulted in eight potential internal flooding locations for quantification. Quantification of these eight scenarios resulted in a total core damage frequency (CDF), from internal floods that occur when the plant is operating at power, of about 2E-10 per year.

The risk analysis for internal flooding during shutdown operation was performed in a manner similar to the analysis for power operation. The screening of areas performed as part of the at-power analysis was reviewed for applicability to shutdown operation based only on safe-shutdown equipment required during shutdown operation. This screening resulted in eight flooding scenarios. Quantification of these eight scenarios resulted in a total CDF, from internal floods that occur during shutdown operation, of about 2E-09 per year.

Westinghouse considers the above mentioned CDF estimates to be conservative upper bounds (based on conservative bounding assumptions made in the analysis). Although such a conclusion is not possible without a detailed PRA, the staff finds Westinghouse's analysis acceptable. The staff's review did not concentrate on bottom-line numbers but rather on the relative insights that the internal flood analysis provides. The staff believes that the AP600 design is capable of withstanding severe accident challenges from internal floods in a manner superior to operating plants and that the conclusions from the internal flood risk analysis performed by Westinghouse complement this belief. The internal flood risk analysis has provided useful safety insights for inclusion in ITAAC, COL Action Items, and RAP. Since detailed PRA-based internal flood analyses at some operating plants have shown that flood-induced sequences can be leading contributors to CDF, the COL applicant should provide an updated internal flood PRA that takes into account design details (e.g., pipe routing, door locations, and flood barriers) to search for internal flooding vulnerabilities in the detailed design. This is COL Action Item 19.1.5-4.

19.1.5.3.1 Dominant Accident Sequences for Internal Floods

Westinghouse quantified the CDF associated with internal floods, for both at power operation and during shutdown, by using applicable event and fault tree models from the internal events PRA.

Operation at Power

The top three flooding scenarios, contributing about 94 percent of the total CDF from internal flooding at power operation, are summarized below.

Flooding scenario #1, contributing about 37 percent, is initiated by flow from a rupture of condensate, main or startup feedwater, or fire protection piping located in a room of the turbine building Elevation 135'-3" general area. From there it propagates under the doors to other rooms at the same level as well as to lower level areas (turbine building Elevation 117'-6" and 100'-0" general areas) via floor grating. It is assumed that the flooding and spraying damages all equipment contained in these areas, such as main and startup feedwater, condensate, component cooling and service water, portion of the non-Class 1E ac power system and

compressed air. This leads to a "loss of main feedwater to both steam generators" accident initiating event with several non-safety-related and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The two dominant ones are as follows:

(1) stuck-open main steamline safety valve or PORV and consequential steam generator tube rupture followed by failure of either the IRWST gravity injection or the recirculation from the containment sump

(2) failure of PRHR followed by failure of either the IRWST gravity injection or the recirculation from the containment sump

Flooding scenario #2, contributing about 33 percent, is initiated by flow from a rupture of the condensate, main or startup feedwater, or fire protection piping located in the turbine building Elevation 117'-6" general area. From there it propagates via floor grating to the 100'-0" level areas. It is assumed that the flooding and spraying damages all equipment contained in these areas, such as main and startup feedwater, condensate, component cooling water, service water and portion of the non-Class 1E ac power system. This leads to a "loss of main feedwater to both steam generators" accident initiating event with several non-safety-related and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The two dominant ones are as follows:

(1) stuck-open main steamline safety valve or PORV and consequential steam generator tube rupture followed by failure of either the IRWST gravity injection or the recirculation from the containment sump

(2) failure of PRHR followed by failure of either the IRWST gravity injection or the recirculation from the containment sump

Flooding scenario #3, contributing about 24 percent, is initiated by flow from a rupture of an expansion joint in the circulating water system located in the turbine building Elevation 100'-0" general area. It is assumed that the flooding and spraying damages all equipment contained in this area, such as main and startup feedwater, condensate, component cooling water, service water and portion of the non-Class 1E ac power system. This leads to a "loss of main feedwater to both steam generators" accident initiating event with several non-safety-related support and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The two dominant ones are as follows:

(1) stuck-open main steamline safety valve or PORV and consequential steam generator tube rupture followed by failure of either the IRWST gravity injection or the recirculation from the containment sump

(2) failure of PRHR followed by failure of either the IRWST gravity injection or the recirculation from the containment sump.

None of the identified internal flooding events during operation at power leads to core damage unless additional random failures occur.

Low Power and Shutdown Operation

The top two flooding scenarios, contributing about 95 percent of the total CDF from internal flooding during shutdown operation, are summarized below.

Shutdown flooding scenario #1, contributing about 48 percent, is initiated by flow from a rupture of the component cooling water, service water or fire protection system piping in the turbine building during mid-loop operation (RCS drained condition). It is assumed that this break, and the subsequent flooding and spraying, damages all equipment contained in the turbine building. This causes a loss of decay heat removal accident initiating event due to the loss of component cooling/service water. Subsequent random failure to inject by either one of the two IRWST gravity injection lines leads to core damage.

Shutdown flooding scenario #2, contributing about 47 percent, is initiated by flow from a rupture of the chemical and volume control or fire protection system piping in the auxiliary building radiologically controlled area (RCA) during mid-loop operation (RCS drained condition). It is assumed that the flooding and spraying damages the RNS contained in the auxiliary building RCA area and causes a loss of decay heat removal accident initiating event. Subsequent random failure to inject by either one of the two IRWST gravity injection lines leads to core damage.

None of the identified internal flooding events during shutdown operation leads to core damage unless additional random failures occur.

19.1.5.3.2 Risk-Important Design Features and Operator Actions for Internal Floods

The following is a list of important design features which contribute to the small impact of internal floods in the AP600:

- Connections to sources of large quantity of water are outside the nuclear island (Containment and auxiliary building) and the annex building.
- There is no safety-related equipment located in the turbine and annex buildings.
- Flow from any postulated ruptures above grade level (Elevation 100'-0") in the turbine building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the auxiliary building via flow under the doors.
- The bounding flooding source for the turbine building is a break in the circulating water piping at grade level. Flow from this break runs out from the building to the yard through a relief panel in the turbine building west wall and limits the maximum flood level to less than 6 inches. Flooding propagation to areas of the adjacent auxiliary and annex

buildings, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.

- Propagation to the auxiliary building valve/piping penetration room at grade level (the only auxiliary building area that interfaces with the turbine building) – because of the presence of water tight walls and floor combined with drains and access doors to outside, the maximum flood height in the valve/piping penetration room is 36 inches and the flooding does not propagate beyond this area.

- Propagation to the annex building – flow is directed by the sloped floor to drains and to the yard area through the door of the annex building.

- Flow from any postulated ruptures above grade level (elevation 100'-0") in the annex building is directed by floor drains to the annex building sump which discharges to the turbine building drain tank. Alternate paths include flows to the turbine building via flow under access doors and down to grade level via stairwells and elevator shaft.

- The floors of the annex building are sloped away from the access doors to the auxiliary building in the vicinity of the access doors to prevent migration of flood water to the non-radiologically controlled areas of the nuclear island where all safety-related equipment, except for some containment isolation valves, is located.

- To prevent flooding in a RCA in the auxiliary building from propagating to non-RCAs (where all safety-related equipment except for some containment isolation valves is located), the non-RCAs are separated from the RCAs by 2 and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the auxiliary building are located above the maximum flood level.

- Physical separation of safety-related equipment and systems performing redundant functions provides defense-in-depth against internal floods.

- The few penetrations through flood protection walls in the nuclear island that are below the maximum flood level are watertight.

- There are no watertight doors used for flood protection.

- The two 72-hour Class 1E division B and C batteries are located above the maximum flood height in the auxiliary building considering all possible flooding sources (including propagation from sources located outside the auxiliary building).

- The mechanical and electrical equipment in the auxiliary building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E electrical and Class 1E I&C equipment rooms.

- There are two compartments inside containment (PXS-A and PXS-B) containing safe-shutdown equipment other than containment isolation valves that are floodable (i.e., below the maximum flood height of Elevation 108'-2"). Each of these two

compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line and one containment recirculation line). These two compartments are physically separated so that a flood in one compartment cannot propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.

- Containment isolation valves located below the maximum flood height inside containment or in the auxiliary building are normally closed and would not fail open when submerged. Also, there is a redundant, normally closed, containment isolation valve located outside containment in series with each of these valves.

- Plugging of the drain headers is prevented by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible. Drain headers are at least 10.2 cm (4 in.) in diameter and include features, such as check valves and siphon breaks, that prevent backflow.

- The walls, floors and penetrations are designed to withstand the maximum anticipated hydrodynamic loads.

- The two diesel generators are housed in separate compartments in the Diesel Generator Building with no water propagation paths between the compartments.

- Doors in the Circulating Water Pumphouse prevent flooding the circulating water pumps.

- The main feature of the AP600 design that contributes to the low CDF associated with internal flooding during shutdown operation is the IRWST. It provides a reliable means of removing decay heat which is not affected by the internal flooding scenarios.

The operator actions modeled in the internal flooding PRA are those used in the internal events PRA plus four additional operator actions to diagnose and isolate a flooding in the north air handling equipment area (Elevation 135'-3") of the annex building (due to the postulated rupture of the 20.3-cm (8-in.) main fire extension) from propagating to the level 66'-6" area of the auxiliary building where the 24-hour Class 1E batteries are located. This scenario would become a dominant internal flooding scenario if all of the human actions were assumed to fail. However, the CDF of this scenario would still be several orders of magnitude lower than the CDF from internal events. Therefore, no additional significant insights are gained from the internal flooding PRA regarding human errors.

#### 19.1.5.3.3 Insights from the Uncertainty, Sensitivity and Importance Analyses (Internal Flooding)

No uncertainty analysis was performed for internal floods. Because of the conservatism in the approach taken in performing the AP600 internal flood analysis, an uncertainty analysis would result in biased insights. Westinghouse performed a few sensitivity and importance studies to gain insights about the impact of uncertainties on PRA results and the importance of the non-safety-related "defense-in-depth" systems during shutdown operation. These studies provided additional insights about the risk importance of the several "defense-in-depth" systems

which were taken into account in selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process. Insights from the sensitivity and importance studies are summarized below.

- The AP600 design is significantly less dependent on human actions to mitigate internal floods than operating reactors.

- If no credit is taken by the non-safety-related "defense-in-depth" systems to mitigate the flooding events occurring during power operation of the plant, the CDF due to internal flooding would increase by about one order of magnitude (to about 2E-09/yr). This result does not change significantly when the uncertainties associated with failure probabilities, reported in Section 19.1.3.1.5 of this report for internal events, are taken into account. This increase in CDF is very small and does not impact the criteria (reported in Section 19.1.7) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

- If no credit is taken by the non-safety-related "defense-in-depth" systems to mitigate floods occurring during shutdown operation, the CDF due to internal flooding would increase by about a factor of two (to about 4E-09/yr). The CDF increases to about 4E-08/yr when the uncertainties associated with failure probabilities, reported in Section 19.1.3.1.5 of this report for internal events, are taken into account. This increase in CDF is very small and does not impact the probabilistic criteria (reported in Section 19.1.7) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

### 19.1.6 Use of PRA in the Design Process

Westinghouse used PRA in the design process to achieve the following three objectives:

(1) identify vulnerabilities in operating reactor designs and introduce features and requirements that reduce or eliminate these vulnerabilities

(2) quantify the effect of new design features and operational strategies on plant risk to confirm the risk reduction credit for such improvements

(3) select among alternate features, operational strategies or design options

Westinghouse used PRA results and insights from operating reactor experience, as well as from the advanced pressurized water reactor (APWR) SP-90 and Sizewell designs, to identify and evaluate potential vulnerabilities in operating reactor designs. This information was used to introduce the special "advanced" design features described in Section 19.1.2 of this chapter, and make the transition from the operating PWR and APWR designs to the AP600 design. Once these features were introduced, PRA was used to quantify their effect on risk and confirm acceptable reduction or elimination of vulnerabilities, including compliance with the Commission's safety goals. Examples are the CDF reduction estimates (by accident-initiating event category) and associated AP600 features which contribute to such reduction, reported in Section 19.1.3.1.2 of this chapter.

The following are examples of ways in which Westinghouse enhanced the AP600 design by adding or modifying design features or operational requirements based on the AP600 PRA and its evaluation by the staff:

- The diverse actuation system was added as an important alternative to ensure automatic or manual actuation of passive heat removal and containment cooling systems and safety-related functions for reactor protection, automatic depressurization and containment isolation.

- The RNS was designed with at least three containment isolation valves for each containment penetration to reduce the probability of interfacing systems LOCAs that bypass containment.

- Protection system logic modifications were adapted to preclude steam generator overfilling during a SGTR event to reduce the need for full reactor depressurization, and therefore, the frequency of core damage for SGTR events that bypass containment.

- The core makeup tank actuation logic design was changed to allow actuation on low steam generator level and high hot-leg temperature to reduce the importance of operator actions to initiate passive feed and bleed.

- The scope of the diverse actuation symptom was expanded to include control rod insertion. The diverse actuation system was also modified to include an actuation signal to the IRWST MOVs during mid-loop operations, to reduce the dependence upon operator actions to open the valves in the event of an accident during mid-loop operations.

The following are specific examples of confirmatory use of PRA in the design process:

- The IRWST system initially consisted of one line containing a normally closed motor-operated valve and two series check valves. To improve the reliability of the injection phase of the system, a second parallel path of two check valves in series was added to the existing line. Additionally, the motor-operated valve is now normally open, thus the system does not require the opening of a motor-operated valve, which would require an open signal, to initiate injection.

- To improve the reliability of the sump recirculation function, redundant and diverse recirculation valves were incorporated into the design. The AP600 conceptual design consisted of two parallel check valves from the sump. Diversity was modeled into the design by changing one of the check valves to a motor-operated valve; redundancy was incorporated by making each line contain two valves in series.

- Alarms were provided in the main control room to inform the operator of mispositioned isolation valves of the passive core cooling system (PXS) that have remote manual control capability. This reduces the probability of valve mispositioning.

- The PRA was used by Westinghouse to improve the reliability of the final design of the reactor cavity flooding system. This included (1) replacement of motor operated valves in the flooding lines with squib valves to improve system reliability, (2) complete

redesign of the RPV thermal insulation design to enhance coolant access to the RPV, and (3) relocating operator instructions regarding reactor cavity flooding from the Severe Accident Management Guidelines to the Emergency Operating Procedures to provide for earlier flooding.

- Analyses of hydrogen combustion behavior revealed that diffusion flames at the IRWST vents could produce sufficient heating of the containment shell to result in localized creep rupture if the flame becomes attached to the containment shell. In recognition of this threat, Westinghouse incorporated several changes to the design to minimize the threat posed by diffusion flames. These changes are as follows: (1) the openings from the accumulator rooms and CVS compartments that can vent hydrogen to the CMT room will be either located away from the containment wall and electrical penetration junction boxes or covered by a secure hatch, and (2) IRWST vents near the containment wall will be oriented to direct releases away from the containment shell.

The following are some specific examples of use of PRA that resulted in an alternate design:

- Originally the depressurization system consisted of three stages, each stage contained two lines with two normally closed motor-operated valves. An alternate design was then analyzed and selected to include a fourth depressurization stage off the hot leg with valve types diverse from the first three stages.

- Onsite power supplies were increased to provide for two non-safety-related diesel generators.

Operational changes were also made based on the PRA. The normal residual heat removal system and automatic depressurization system provide some examples of operational changes.

- Initiation of the normal residual heat removal system initially required the operators to first decide if it was appropriate to actuate normal residual heat removal system following depressurization. To reduce the operator's burden as to when it was appropriate to actuate normal residual heat removal, an operation change was made so that the operator initiates the system whenever automatic depressurization system is actuated, with the exception of cases when radiation could leak out of containment. Additionally, the system can now be manually actuated from the main control room instead of using local manual actuation.

- As an outcome of scoping PRA studies, the ADS stage 1, 2, and 3 valve configuration was initially changed from two normally-closed valves to one valve open and one valve closed in each line to allow for testing during refueling. Further evaluation of this configuration showed that the potential for spurious actuation of the automatic depressurization system had increased. Thus, the automatic depressurization system valve configuration was changed to two closed valves with quarterly testing.

Finally, PRA was used to identify non-safety-related "defense-in-depth" SSCs that require regulatory oversight (according to the RTNSS process) and to evaluate several severe accident mitigation design alternatives (SAMDAs) by examining the benefits associated with each of these design alternatives.

### 19.1.7 PRA Input to the "Regulatory Treatment of Non-Safety-Related Systems" (RTNSS) Process

The NRC and the ALWR Steering Committee reached consensus on a process for resolving the RTNSS issue (SECY-94-084). This process included the use of both probabilistic and deterministic criteria to achieve the following objectives: (1) determine whether regulatory oversight for certain non-safety-related systems was needed, (2) identify risk important SSCs for regulatory oversight (if it were determined that regulatory oversight was needed), and (3) decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance. The following two probabilistic criteria are used to achieve such objectives:

(1) The AP600 design should meet the Commission's safety goal guideline for CDF of less than 1E-04/yr with no credit for the performance of any non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.

(2) The AP600 design should meet the Commission's safety goal guideline for large release frequency (LRF) of less than 1E-06/yr with no credit for the performance of the non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.

In applying these criteria, the RTNSS process stresses the importance of accounting for uncertainties and also taking into consideration the risk importance of SSCs contributing to initiating event frequencies. Specifically, the RTNSS process provides that the following two items must be addressed:

(1) Uncertainties, such as in the assumed reliability values for passive system components.

(2) Non-Safety-related SSCs contributing to initiating event frequencies could be subject to regulatory oversight which is commensurate with their reliability/availability missions.

Westinghouse used its AP600 "focused" PRA model, which does not credit non-safety-related systems for accident mitigation (except for the RPV thermal insulation system), and assessed CDF and LRF values which meet both probabilistic criteria. In addition, Westinghouse provided probabilistic arguments showing that no additional regulatory oversight is needed for SSCs contributing to initiating event frequencies, except for the RNS during cold shutdown and refueling. Westinghouse placed availability controls on RNS and its support systems (SWS, CCS, and ac power) when RCS level is not visible in the pressurizer until the refueling cavity is half full and the upper internals are removed. The staff's review found that this additional regulatory oversight for RNS and its support systems (CCW, SSW and ac power) must be extended to Mode 5 operation when the RCS is open (see Section 19.1.4.5 of this report). Westinghouse agreed to require additional regulatory oversight for RNS and its support systems (CCW, SSW and onsite ac power) for the whole period of Mode 5 when the RCS is open, as discussed in Section 16.3 of the SSAR.

Furthermore, the staff review found that the issue of uncertainties (e.g., those associated with the assumed reliability values for passive system components) had not been addressed. Staff sensitivity studies have shown that the "focused" PRA results (e.g., CDF and LRF) are sensitive

to the reliability values used in the PRA for certain passive system components which have significant uncertainties associated with them. The results of such sensitivity studies have shown that when more bounding data are used in the PRA in order to address uncertainties, both probabilistic criteria are met only when credit is taken for some additional non-safety-related "defense-in-depth" systems. Therefore, the need for regulatory oversight of certain SSCs has been determined and is discussed below and in Chapter 22 of this report.

The results of the uncertainty and importance analyses were used to select SSCs for sensitivity studies. These analyses indicated that the following SSCs have the largest impact on PRA results, such as CDF and LRF, used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process:

- reactor trip components, such as circuit breakers
- engineered safety features (ESF) actuation components, such as software
- passive system check valves and explosive (squib) valves

A series of sensitivity studies were performed by the staff to investigate the impact of uncertainties in the performance of these SSCs on PRA results, under the assumption of plant operation without credit for one or more non-safety-related "defense-in-depth" systems. These studies provided additional insights about the risk importance of the various "defense-in-depth" systems which were taken into account in selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process (detailed results and insights related to CDF are reported in Section 19.1.3.1.5 while insights related to LRF and CCFP are reported in Section 19.1.3.2 of this report). The most important insights from such sensitivity studies, as they relate to the RTNSS process, are summarized below.

- Availability control of the reactor trip (RT) function of DAS provides an efficient means for minimizing the impact of uncertainties in reactor trip components, such as circuit breakers, on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process. Such availability control should include the two motor-generator set circuit breakers (CBs) because the RT function of DAS requires the availability (to open) of both these CBs.

- Availability control of the ESF actuation function of DAS provides an efficient means for minimizing the impact of uncertainties associated with ESF actuation components, such as digital I&C system software, on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process.

- Availability control of the RNS (including its support systems) provides an efficient means for minimizing the impact of uncertainties associated with passive system check valves and explosive (squib) valves on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process.

- Criterion #1 (i.e., CDF less than 1E-04/y) is fully satisfied when an unavailability of 0.25 or less is assumed in the PRA for DAS (for both the reactor trip and ESF actuation functions) and for RNS. This requires an "average" yearly availability of at least 75 percent for such systems.

- Criterion #2 (i.e., LRF less than 1E-06/y) is fully satisfied when an unavailability of 0.1 or less is assumed in the PRA for each of the automatic and manual portions of DAS (for both the reactor trip and ESF actuation functions) and for RNS. This requires an "average" yearly availability of at least 90 percent for such systems or subsystems.

An additional criterion for assessing containment performance is the degree to which the design comports with the Commission's probabilistic containment performance goal of 0.1 conditional containment failure probability (CCFP) when no credit is provided for the performance of the non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight. The CCFP is a containment performance measure that provides perspectives on the degree to which the design has achieved a balance between core damage prevention and core damage mitigation. CCFP was used in a qualitative manner to confirm that the design, combined with the regulatory oversight for identified SSCs, has maintained an acceptable balance between core damage prevention and mitigation, but was not used as a criterion for establishing the availability requirements for non-safety-related "defense-in-depth" systems.

Based on sensitivity analyses performed by the staff, the CCFP is approximately 0.1 and is not dramatically changed as availability is increased (CCFP is about 0.16 for 90 percent availability, 0.12 for 95 percent availability and 0.08 for 99 percent availability of DAS). The staff concludes that an appropriate balance between prevention and mitigation is maintained for any of these availability values.

In meeting criterion #2 and the CCFP goal, credit was taken for external reactor vessel cooling (ERVC) as a strategy for retaining molten core debris in-vessel. This results in the majority of core melt accidents (~90 percent) being arrested in-vessel, thereby avoiding RPV failure and associated containment challenges from ex-vessel phenomena. Successful RCS depressurization and reactor cavity flooding are prerequisites for ERVC, and credit for these aspects of ERVC in the focussed PRA is appropriate since both functions are fulfilled by safety-related systems. However, the non-safety-related RPV thermal insulation system is also required for successful ERVC. The thermal insulation system limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents. Attributes of the system include specific RPV/insulation clearances and water/steam flow areas based on scaled tests, water inlets and steam vents which change position during flood-up of the reactor cavity, and insulation panel and support members designed to withstand the hydrodynamic loads associated with ERVC.

In view of the reliance on ERVC to meet the Commission's large release frequency and containment performance goals, Westinghouse has committed to regulatory oversight of the RPV thermal insulation system according to the RTNSS process. Specifically, the system is included as a risk-significant SSC in the reliability assurance program, the design description and functional requirements for the RPV insulation are included in the SSAR, and important criteria associated with the insulation design is included in the ITAAC. This oversight provides reasonable assurance that the as-built insulation system conforms with design specifications contained in Chapter 39 of the PRA, and that the operability of the system is confirmed through periodic surveillance.

19.1.8 PRA Input to the Design Certification Process

PRA was used in the design certification process to achieve the following objectives: (1) develop an in-depth understanding of design robustness and tolerance of severe accidents initiated by either internal or external events; (2) develop a good appreciation of the risk significance of human errors associated with the design, and characterize the key errors in preparation for better training and refined procedures; and (3) identify important safety insights related to design features and assumptions made in the PRA to support certification requirements, such as ITAACs, design RAP (D-RAP) requirements, Technical Specifications, as well as COL and interface requirements.

The first two objectives were achieved by identifying the dominant accident sequences as well as the risk-important design features and human actions (see Sections 19.1.3 to 19.1.5). The third objective was achieved by using PRA insights and assumptions to develop the following list of design certification requirements. These requirements will be incorporated, as appropriate, into the Design Control Document (DCD) to ensure that any future plant which references the AP600 design will be built and operated in a manner that is consistent with important assumptions made in the AP600 design certification PRA.

General & Plant-wide Requirements

(1) The D-RAP (SSAR Section 17.4) provides a list of risk important SSCs.

(2) The COL applicant referencing the AP600 certified design will perform a seismic walkdown to confirm that the as-built plant conforms to the design used as the basis for the seismic margins evaluation and that seismic spatial systems interactions do not exist. The COL applicant will develop details of the seismic walkdown. This is COL Action Item 19A.2.5-1 (see section 19A of this report).

(3) The COL applicant referencing the AP600 certified design will compare the as-built SSC HCLPFs to those assumed in the AP600 seismic margins evaluation. The COL applicant will evaluate deviations from the HCLPF values or assumptions in the seismic margins evaluation to determine if vulnerabilities have been introduced. This was previously identified as part of COL Action Item 19.1.5-2.

(4) The COL applicant will maintain an operation reliability assurance process founded on the system reliability information derived from the PRA and other sources. The COL applicant will incorporate the list of risk-important SSCs, as presented in the SSAR section on D-RAP, in its D-RAP and operation reliability assurance process. This was previously identified as COL Action Item 19.1.3.1-1.

(5) The COL applicant will use information regarding risk-important operator actions from the PRA, as presented in Chapter 18 of the SSAR on human factors engineering, in developing and implementing procedures, training, and other human reliability related programs. This was previously identified as COL Action Item 19.1.3.1-2.

(6) As deemed necessary, during the detailed design phase, the COL applicant will update the PRA, including the fire and flood analyses for both at-power and shutdown

operation. Using the final design information and site-specific information, the COL applicant will also re-evaluate the qualitative screening of external events. The updated PRA will include any site specific susceptibilities found, and the applicable external events. These above COL Action Items were previously identified as part of COL Action Items 19.1.1-1, 19.1.5-3, and 19.1.5-4.

(7) There is no safety-related equipment located outside the nuclear island.

(8) A combination of multiple isolation valves, valve interlocking, increase in the piping pressure limits and pressure relief capability protects the AP600 low pressure systems which interface with the RCS against interfacing systems LOCA (ISLOCA).

(9) The AP600 safety-related I&C system will use solid state switching devices and electro-mechanical relays resistant to relay chatter. Use of these devices and relays minimizes the mechanical discontinuities associated with similar devices at operating reactors.

(10) The AP600 design does not use watertight doors for flood protection.

(11) The AP600 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. The design enables all flood barriers (e.g., walls, floors and penetrations) to withstand the maximum anticipated hydrodynamic loads.

(12) The design of the drain headers minimizes plugging by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible. Drain headers are at least 10.2 cm (4 in.) in diameter.

(13) There is no cable spreading room in the AP600 design.

(14) Separation or protection of equipment and cabling among the divisions of safety-related equipment and separation of safety-related from non-safety-related equipment, minimizes the probability that a fire or flood would affect more than one safety-related system or train except in some areas inside containment where equipment will be capable of achieving safe shutdown before damage.

(15) The following minimize the probability for fire or flood propagation from one area to another and help limit risk from internal fires and floods:

- Fire barriers are sealed (doors sealed to the extent possible) and flood barriers are watertight.

- Each fire door is alarmed in the control room.

- Requirements for fire and flood barrier and maintenance will be implemented in COL Applicant programs. The purpose of these requirements is to ensure the reliable performance of fire barriers (e.g., through appropriate inspection and maintenance of doors, dampers, and penetration seals) and of flood barriers

(e.g., through appropriate maintenance of all water tight penetrations during power operation to prevent the propagation of water from one area to the next). This is COL Action Item 19.1.8-1.

- It is necessary to take appropriate compensatory measures to minimize risk when a fire door, fire barrier penetration, or flood barrier penetration must be open to allow specific maintenance (e.g., during plant shutdown). Appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration minimize risk during shutdown. In particular, configuration control of fire/flood barriers will be required to ensure the integrity of fire and flood barriers between areas containing equipment performing redundant safe shutdown functions. This is COL Action Item 19.1.8-2.

- Drains include features, such as check valves and siphon breaks, that prevent backflow.

(16) The design provides fire detection and suppression capability. The design also provides flooding control features and sump level indication. Compensatory measures are expected to be taken in order to maintain the detection and suppression capability to allow specific maintenance activities.

(17) In addition to the MCR which has its own dedicated ventilation system, there are separate ventilation systems for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). Furthermore, the plant ventilation systems include features to prevent propagation of smoke from a non-safety-related area to a safety-related area or between safety-related areas supported by two different divisions. The COL applicant must ensure the reliable performance of such smoke propagation prevention features.

(18) The COL applicant will implement the maintenance guidelines as described in the Shutdown Evaluation Report (WCAP-14837). This is COL Action Item 19.1.8-3.

(19) The COL applicant will control transient combustibles. This is particularly important during shutdown operation with ongoing maintenance activities. This is COL Action Item 19.1.8-4.

Main Control Room (MCR) and Remote Shutdown Workstation (RSW)

(1) A fire in either the MCR or the RSW does not affect the automatic function of the AP600 actuation systems (i.e., PMS and DAS). This ensures an independent, automatic means, to reach safe shutdown even when a fire occurs in the MCR or the RSW (there is no need for manual actuation unless the automatic actuation fails). Also, even though a fire in the MCR may defeat manual actuation of equipment from the MCR, it will not affect the manual operation from the RSW. This is because of the location of the I&C cabinets in fire areas outside the MCR and the RSW.

(2) The MCR provides, within itself, redundancy in MCR operations, in terms of both monitoring and manual control of safe-shutdown equipment. This provides an

alternative means for mitigating certain MCR fires before deciding to evacuate the MCR and use the RSW.

(3) The RSW provides sufficient instrumentation and control to bring the plant to safe-shutdown conditions in case of control room evacuation. There are no differences between MCR and RSW controls and monitoring that would be expected to affect safety system redundancy and reliability.

(4) The MCR has its own dedicated ventilation system and is pressurized. This prevents smoke, hot gases, and fire suppressants, originated in areas outside the MCR, to migrate via the ventilation system to the control room.

(5) The MCR and the RSW are in separate fire and flood areas. They have separate and independent ventilation systems.

(6) AP600 MCR fire ignition frequency is limited as a result of the use of low-voltage, low-current equipment and fiber optic cables.

Containment/Shield Building

(1) Redundant containment isolation valves in each line protect containment isolation functions from the impact of internal fires and floods. The location of these valves is in separate fire and flood areas. Different power and control divisions serve these valves, if powered. The location of one isolation component in a given line is always inside containment, while the location of the other is outside containment, and the containment wall is a fire/flood barrier.

(2) Although the containment is a single fire area, adequate design features exist to ensure the plant can achieve safe-shutdown conditions. Such features include separation (structural or space), suppression, lack of combustibles and operator actions.

(3) There are two compartments inside containment (PXS-A and PXS-B) containing safe-shutdown equipment other than containment isolation valves that are floodable (i.e., below the maximum flood height). Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line and one containment recirculation line). A structural wall physically separates these two compartments to ensure that a flood in one compartment does not propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.

(4) Containment isolation valves located below the maximum flood height inside containment or in the auxiliary building are normally closed and are designed to fail closed.

(5) The passive containment cooling system (PCS) cooling water not evaporated from the vessel wall flows down to the bottom of the inner containment annulus. Screens prevent clogging (e.g., by the entry of small animals into the drains) of two 100 percent drain

openings, located in the side wall of the shield building. These drains are always open. The annulus drains will have the same (or higher) HCLPF value as the shield building so that the drain system will not fail at lower acceleration levels causing water blocking of the PCS air baffle.

(6) The ability to close containment hatches and penetrations following an accident during Modes 5 and 6, before steam is released into the containment, is important. The COL applicant is responsible for developing procedures and training to address this issue. This is COL Action Item 19.1.8-5.

(7) The COL applicant should provide administrative controls to control foreign debris from being introduced into the containment during maintenance and inspection operations, to prevent plugging of the containment sump screens. This is COL Action Item 19.1.8-6.

Auxiliary Building

(1) The design provides separate ventilation systems for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). This prevents smoke, hot gases, and fire suppressants originating in divisions A or C from propagating to divisions B and D.

(2) 3-hour rated fire walls without openings separate the major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms). There are no doors, dampers, or seals in these walls. Separate ventilation subsystems serve the rooms. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).

(3) An access bay protects important safety-related I&C equipment as well as the main control room and the remote shutdown panel, located in the north end of the auxiliary building, from potential debris produced by a postulated seismically-induced structural collapse of the adjacent turbine building.

(4) There are no normally open connections to sources of "unlimited" quantity of water in the auxiliary building.

(5) Separation of the non-RCAs from the RCAs by 2 and 3-foot walls and floor slabs prevent flooding in a RCA in the auxiliary building from propagating to non-RCAs. In addition, the location of electrical penetrations between RCAs and non-RCAs in the auxiliary building are above the maximum flood level.

(6) The location of the two 72-hour rated Class 1E division B and C batteries are above the maximum flood height in the auxiliary building considering all possible flooding sources (including propagation from sources located outside the auxiliary building).

(7) Flood water propagated from the turbine building to the auxiliary building valve/piping penetration room at grade level (the only auxiliary building area that interfaces with the

turbine building) is directed to drains and to the outside through access doors. This, combined with the presence of water tight walls and floor of the valve/penetration room, limits the maximum flood height in the valve/piping penetration room (to about 36 inches) and prevents flooding from propagating beyond this area.

(8) The mechanical and electrical equipment in the auxiliary building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E electrical and Class 1E I&C equipment rooms.

Turbine Building

(1) The turbine building contains no safety-related equipment. There is a 3-hour fire barrier wall between the turbine building and the safety-related areas of the nuclear island.

(2) The location of the connections to sources of "large" quantity of water are in the turbine building. They are the service water system (SWS) which interfaces with the component cooling water system (CCS) and the circulating water system (CWS) which interfaces with the turbine building closed cooling system (TCS) and the condenser. Features that minimize flood propagation to other buildings are:

- Flow from any postulated ruptures above grade level (Elevation 100'-0") in the turbine building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the auxiliary building via flow under the doors.

- A relief panel in the turbine building west wall at grade level directs the water outside the building to the yard and limits the maximum flood level in the turbine building to less than 15.2 cm (6 in.). Flooding propagation to areas of the adjacent auxiliary building, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.

Annex Building

(1) There is no safety-related equipment located in the annex building.

(2) The sloped floor directs flood water in the annex building grade level to drains and to the yard area through the door of the annex building.

(3) Floor drains to the annex building sump that discharges to the turbine building drain tank directs flow from postulated ruptures above grade level in the annex building. Alternate paths include flows to the turbine building via flow under access doors and down to grade level via stairwells and elevator shaft.

(4) The floors of the annex building slope away from the access doors to the auxiliary building in the vicinity of the access doors to prevent migration of flood water to the non-radiologically controlled areas of the nuclear island, the location of all safety-related equipment except for some containment isolation valves.

(5) There are no connections to sources of "unlimited" quantity of water (i.e., open connections) in the annex building.

Reactor Coolant System

(1) To prevent overdraining, the RCS hot and cold legs are vertically offset which permits draining of the steam generators for nozzle dam insertion with a hot-leg level much higher than traditional designs. This level is nominally 80 percent level in the hot leg.

(2) Use of a step nozzle connection between the RCS hot leg and the RHR suction line lowers the level in the hot leg at which vortexing can occur. The step nozzle is a 20 inch schedule 140 pipe, approximately 0.61 m (2 ft) long.

(3) Should vortexing occur, the maximum air entrainment into the pump suction was shown experimentally to be no greater than 5 percent.

(4) There are two safety-related RCS hot-leg level channels, one located in each hot leg. These level instruments are independent and do not share instrument lines. These level indicators are in place primarily to monitor RCS level during mid-loop operations. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg as close to the steam generator as possible.

(5) Wide range pressurizer level indication (cold calibrated) provides measurement of RCS level to the bottom of the hot legs. The upper level tap connects to an ADS valve inlet header above the top of the pressurizer. The lower level tap connects to the bottom of the hot leg. This non-safety-related pressurizer level indication can serve as an alternative way of monitoring level and as a means to identify inconsistencies in the safety-related hot-leg level instrumentation.

(6) The RNS pump suction line slopes continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if an RNS pump is stopped when cavitating as a result of excessive air entrainment. This self-venting suction line allows the RNS pumps to immediately restart once re-establishment of an adequate level in the hot leg occurs.

(7) The COL applicant should have procedures and policies to maximize the availability of the non-safety-related wide range pressurizer level indication (cold calibrated) during RCS draining operations during cold shutdown. Training should be given to the operators on how to use this indication to identify inconsistencies in the safety-related hot-leg level instrumentation to prevent RCS overdraining. This is COL Action Item 19.1.8-7.

Passive Core Cooling Systems (PXS)

The passive core cooling system (PXS) is composed of (1) the accumulator subsystem, (2) the CMTs subsystem, (3) the IRWST subsystem, and (4) the passive residual heat removal

(PRHR) subsystem. In addition, the ADS, which is part of the RCS, also supports passive core cooling functions.

Accumulators

The accumulators provide a safety-related means of safety injection of borated water to the RCS. The following are some important aspects of the accumulator subsystem as represented in the PRA:

- There are two accumulators, each with an injection line to the reactor vessel/direct vessel injection (DVI) nozzle. Each injection line has two check valves in series.
- The reliability of the accumulator subsystem is important. The COL will maintain the reliability of the accumulator subsystem.
- Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.

Core Makeup Tanks

The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS. The following are some important aspects of CMT subsystem as represented in the PRA:

- There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle. Each CMT has a normally open pressure balance line from an RCS cold leg. A parallel set of air-operated valves (AOVs) which open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS isolates each injection line. The injection line for each CMT also has two normally open check valves in series.
- Actuation of the CMT AOVs from PMS and DAS is automatic and manual. Indication of their positions and alarms are in the control room.
- CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.
- The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty. The COL will maintain the reliability of the CMT subsystem. These AOVs are stroke-tested quarterly.
- The Technical Specifications require the CMTs to be available from power conditions down through cold shutdown with RCS pressure boundary intact.

In-Containment Refueling Water Storage Tank

The IRWST subsystem provides a safety-related means of performing (1) low-pressure safety injection following ADS actuation, (2) long-term core cooling via containment recirculation,

and (3) reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment. Some important aspects of the IRWST subsystem as represented in the PRA are shown below.

- The IRWST subsystem has the following flowpaths:
  - Two (redundant) injection lines from IRWST to reactor vessel DVI nozzle. A parallel set of valves isolates each line; each set with a check valve in series with a squib valve.
  - Two (redundant) recirculation lines from the containment to the IRWST injection line. Each recirculation line has two paths: one path contains a squib valve and an MOV, the other path contains a squib valve and a check valve.
  - The two MOV/squib valve lines also provide the capability to flood the reactor cavity.
- There are screens for each IRWST injection line and recirculation line which prevents clogging by debris or other materials generated in the IRWST or containment sump. The COL Applicant will maintain the reliability of the IRWST subsystem, including the IRWST and containment recirculation screens.
- Explosive (squib) valves provide the pressure boundary and protect the check valves from any potential adverse impact of high differential pressures.
- Class 1E dc is the power source for the Squib valves and MOVs. Indication of their positions and alarms are in the control room.
- Actuation of the squib valves and MOVs for injection and recirculation via PMS is automatic and manual. Actuation via DAS is manual.
- Actuation of the squib valves and MOVs for reactor cavity flooding is manual via PMS and DAS from the control room.
- Diversity of the squib valves in the injection lines and recirculation lines minimizes the potential for common cause failure between injection and recirculation/reactor cavity flooding.
- PMS low hot-leg level logic provides automatic IRWST injection at shutdown conditions.
- Exercising of the IRWST injection and recirculation check valves occurs at each refueling. Testing of IRWST injection and recirculation squib valve actuators occurs every 2 years for 20 percent of the valves. Stroke testing of IRWST recirculation MOVs occurs quarterly.
- The reliability of the IRWST subsystem is important. The COL will maintain the reliability of the IRWST subsystem.

- Technical specifications require IRWST injection and recirculation to be available from power conditions to refueling without the cavity flooded.

The IRWST provides a safety-related long term source of water during shutdown conditions. The following are some additional important aspects of the IRWST subsystem as represented in the shutdown PRA.

- The COL applicant should provide administrative controls to control foreign debris from being introduced in the IRWST tank during maintenance and inspection operations, to prevent plugging of the IRWST screens. This is COL Action Item 19.1.8-8.

- On low hot-leg level, the PMS actuates the squib valves to open allowing gravity injection from the IRWST.

Passive Residual Heat Removal System

The PRHR provides a safety-related means of performing the following functions: (1) removes core decay heat during accidents, (2) allows adequate plant performance during transient (non-LOCA and non-ATWS) accidents without ADS, (3) allows automatic termination of RCS leak during a SGTR accident without ADS, and (4) allows plant to ride out an ATWS event without rod insertion.

The PRA models incorporate the following important aspects of the PRHR design and operation features:

- Opening redundant parallel AOVs actuates PRHR. These AOVs are designed to fail open on loss of Class 1E power, loss of air, or loss of signal from the PMS.

- Two redundant and diverse I&C systems automatically actuate the PRHR AOVs: (1) the safety-related PMS and (2) the non-safety-related DAS. Manual actuation of the PRHR can also be done from the control room using either PMS or DAS.

- Diversity of the PRHR AOVs from the AOVs in the CMTs minimizes the probability for common cause failure of both PRHR and CMT AOVs.

- Indications of the positions of the inlet and outlet PRHR valves, including alarms, are in the MCR.

- Tests of the PRHR AOVs occur quarterly. The PRHR HX is subject to flow testing.

- The PRHR heat exchanger (HX), in conjunction with the PCS, can provide core cooling for an indefinite period of time. After the IRWST water reaches its saturation temperature, the process of steaming to the containment initiates. Condensation occurs on the steel containment vessel, and the condensate is collected in a safety-related gutter arrangement that returns the condensate to the IRWST. The gutter normally drains to the containment sump, but when the PRHR HX actuates, safety-related isolation valves in the gutter drain line shut and the gutter overflow returns directly to the

IRWST. The following design features provide proper re-alignment of the gutter system valves to direct water to the IRWST:

- the IRWST gutter and its isolation valves are safety-related
- On loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal the valves that re-direct the flow will, by design, fail-closed.
- PMS and DAS automatically actuate the isolation valves.

- Use of the PRHR HX for long-term cooling will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST via the gutter system. If the condensate does not return to the IRWST, the IRWST volume is sufficient for at least 72 hours of PRHR operation. Connections to the IRWST from the spent fuel system (SFS) and chemical and volume control system (CVS) exist to extend PRHR operation. A safety-related makeup connection is also in place from outside the containment through the RNS to the IRWST.

- Technical Specifications require the PRHR to be available, with RCS boundary intact, from power conditions down through cold shutdown.

- Capability exists and guidance is provided for the control room operator to identify a leak in the PRHR HX before it reaches a "critical" size which would cause it to degrade to a tube rupture under normal operation or design-basis accident conditions (i.e., under the stress conditions likely to occur during design-basis accidents requiring PRHR operation).

- The PRHR provides a safety-related means of removing decay heat following loss of RNS cooling during safe/cold shutdown with the RCS intact.

Automatic Depressurization System

ADS provides a safety-related means of depressurizing the RCS. The following are some important aspects of ADS as represented in the PRA:

- ADS has four stages. Two separate groups of valves and lines comprise each stage. Stages 1,2, and 3 discharge from the top of the pressurizer to the IRWST. Stage 4 discharges from the hot leg to the RCS loop compartment.

- Each stage 1, 2, and 3 line contains two MOVs in series. Each stage 4 line contains an MOV valve and a squib valve in series.

- The valve arrangement and positioning for each stage, by design, reduces spurious actuation of ADS.
  - Stage 1, 2, and 3 MOVs are normally closed and have separate controls.
  - Each stage 4 squib valve has redundant, series controllers.
  - Stage 4 is blocked from opening at high RCS pressures.

- Actuation of the ADS valves via the PMS is automatic and manual. Via the DAS, actuation is manual.

- Class 1E dc is the ADS valves power source. The control room contains their position indication as well as alarms.

- Stroke-testing of stage 1, 2, and 3 valves occurs during every cold shutdown. Testing of stage 4 squib valve actuators occurs every 2 years for 20 percent of the valves.

- The reliability of the ADS is important. The COL will maintain the reliability of the ADS.

- Technical specifications require ADS to be available from power conditions until the refueling cavity is flooded.

- Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events. Procedures will be provided for use of the ADS for depressurization of the RCS after core uncovery.

- The AP600 design includes features that prevent fire-induced detonation of a squib valve. The use of a squib valve controller circuit which requires multiple hot shorts for actuation, physical separation of potential hot short locations (e.g., by routing ADS cables in low voltage cable trays and by using redundant series controllers located in separate cabinets) and provisions for operator action to remove power from the fire zone, prevents spurious actuation of squib valves.

- The first, second, and third-stage valves, connected to the top of the pressurizer, provide a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost.

- On low-low hot-leg level (empty hot leg), the PMS signals the ADS 4th stage squibs to open.

- Following an extended loss of RNS during safe/cold shutdown with the RCS intact and PRHR unavailable, it is essential to establish and maintain a venting capability with ADS stage 4 for gravity injection and containment recirculation.

- Because of the potential for counter current flow limitation in the surgeline and pressurizer, it is essential to establish and maintain a venting capability with ADS stage 4 for gravity injection and containment sump recirculation, following an extended loss of RNS when the RCS is open during shutdown operations. With the opening of ADS 4th stage, the RCS depressurzies within 24 hours, requiring the containment sump recirculation function.

Normal Residual Heat Removal System

The RNS provides the following non-safety-related means of core cooling during accidents: (1) RCS recirculation at shutdown conditions, (2) low pressure pumped injection from the IRWST, and (3) long-term pumped recirculation from the containment sump. Such RNS

functions provide defense-in-depth in mitigating accidents, in addition to that provided by the passive safety-related systems.

The following are some important aspects of RNS as represented in the PRA:

- The RNS has redundant pumps (separate non-Class 1E buses with backup connections from the diesel generators power these pumps) and redundant heat exchangers.

- The RNS provides safety-related means for (1) containment isolation at the penetration of the RNS lines, (2) RCS isolation at the RNS suction and discharge lines, and (3) IRWST and containment sump inventory makeup.

- Operators in the control room can manually align the RNS to perform its core cooling functions. Emergency response guidelines (ERGs) provide guidance for aligning the RNS from the control room for RCS injection and recirculation.

- Actuation of recirculation from the containment sump is automatically (i.e., IRWST recirculation valves open automatically) induced by a low IRWST level signal or manually from the control room, if automatic actuation fails following accidents at full power and at shutdown with the RCS open.

- For long-term recirculation operation, the RNS pumps obtain suction from only one of the two sump recirculation lines. Unrestricted flow through both parallel paths (one containing an MOV and a squib valve in series, the other containing a check valve and a squib valve in series) is essential for success of the sump recirculation function when both RNS pumps are running. If one of the two parallel paths fails to open, operator action (in the control room through PMS) is required to manually throttle the RNS discharge MOV (V011) to prevent pump cavitation.

- With the RNS pumps aligned either to the IRWST or the containment sump, the pumps' NPSH is adequate to prevent pump cavitation and failure even when saturation of the IRWST or sump inventory occurs.

- The RNS containment isolation and RCS pressure boundary valves are safety-related. Class 1E dc is the power source for the MOVs.

- The containment isolation valves in the RNS piping close automatically via PMS with a high radiation signal. The established actuation setpoint is consistent with a DBA non-mechanistic source term associated with a large LOCA. The expectation is that the containment radiation level for other accidents is below the point that would cause the RNS MOVs to automatically close.

- The following AP600 design features contribute to the low likelihood of interfacing system LOCAs through the RNS system:

  - The portion of the RNS outside containment is capable of withstanding the operating pressure of the RCS.

- A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure.

- At least three valves isolate each RNS line.

- The pressure in the RNS pump suction line is continuously indicated and alarmed in the main control room.

- Interlocking of the pump suction isolation valves connecting the RNS pumps to the RCS hot leg with RCS pressure prevents opening of the valves until the RCS pressure is less than 450 psig. This prevents overpressurization of the RCS when the RNS is aligned for shutdown cooling.

- The two remotely operated MOVs connecting the suction and discharge headers, respectively, to the IRWST are interlocked with the isolation valves connecting the RNS pumps to the hot leg. This prevents inadvertent opening of any of these two MOVs when the RNS is aligned for shutdown cooling and potential diversion and draining of reactor coolant system.

- During normal power operation administrative blockage of the power to the four isolation MOVs connecting the RNS pumps to the RCS hot leg at their motor control centers is present.

- Testing of the operability of the RNS occurs, via connections to the IRWST, immediately before its alignment to the RCS hot leg, for shutdown cooling, to ensure that there are no any open manual valves in the drain lines.

- The IRWST suction isolation valve (V023) and the RCS pressure boundary isolation valves (V001A, V001B, V002A and V002B) are environmentally qualified to perform their safety functions.

- The reliability of the IRWST suction isolation valve (V023) to open on demand (for RNS injection during power operation and for IRWST gravity injection via the RNS hot leg connection during shutdown operation) is important. The COL will maintain the reliability of this valve.

- During cold shutdown and refueling conditions with the RCS open, RNS V-023 provides an alternative gravity injection path. The COL applicant will have policies that maximize the availability of this valve and procedures to open this valve during cold shutdown and refueling operations when the RCS is open and PRHR cannot be used for core cooling. This is COL Action Item 19.1.8-9.

- Performance of planned maintenance affecting the RNS cooling function and its support systems will occur in Modes 1, 2, and 3 when the RNS is not normally operating.

- Since inadvertent opening of RNS valve V024 results in a draindown of RCS inventory to the IRWST and requires gravity injection from the IRWST, the COL applicant will have administrative controls to ensure that inadvertent opening of this valve is unlikely.

This is COL Action Item 19.1.8-10. This error will be taken into account in the control room design. This is COL Action Item 19.1.8-11.

- The RNS is an important "defense-in-depth" system for accidents initiated while the plant is at power. During shutdown operations with the RCS open and the refueling cavity not flooded, reliable RNS operation is critical to reducing the probability of an initiating event as a result of loss of RNS cooling. The availability of the RNS and its support systems (CCW, SWS and diesel generators) will be controlled during power operation, as well as during shutdown operation with the RCS open, as described in SSAR Chapter 16.3 on RTNSS.

Startup Feedwater System

The SFW system pumps provide feedwater to the steam generators (SGs). This capability provides an alternate core cooling mechanism to the PRHR heat exchanger for non-LOCA or SGTR accidents which minimizes the PRHR challenge rate. The COL applicant will maintain the reliability of the SFW system.

Instrumentation and Control (I&C)

The following three I&C systems are credited in the PRA for providing monitoring and control functions during accidents: (1) the safety-related PMS, (2) the non-safety-related DAS, and (3) the non-safety-related PLS.

The PMS provides a safety-related means of performing the following functions:

- automatic and manual reactor trip
- automatic and manual actuation of ESF
- monitor the safety-related functions during and following an accident as provided by RG 1.97

The DAS provides a non-safety-related means of performing the following functions:

- automatic and manual reactor trip
- automatic and manual actuation of selected engineered safety features
- provide control room indication for monitoring of selected safety-related functions

The PLS provides a non-safety-related means of performing the following functions:

- automatic and manual control of non-safety-related functions, including "defense-in-depth" systems (e.g., RNS)
- provide control room indication for monitoring overall plant and non-safety-related system performance

The following are some important aspects of PMS as represented in the PRA:

- The PMS has four (redundant) divisions of reactor trip and ESF actuation and automatically produces a reactor trip or ESF initiation upon an attempt to bypass more than two channels of a function that uses 2-out-of-4 logic.
- The PMS has redundant divisions of safety-related post-accident parameter display.
- Each PMS division receives power from its respective Class 1E dc division.
- The PMS provides fixed position controls in the control room.
- Redundancy and functional diversity within each division ensures the reliability of the PMS:
  - The reactor trip functions are divided into two functionally diverse subsystems.
  - Two microprocessor-based subsystems that are functionally identical in both hardware and software process the ESF functions.
- Separate input channels are provided for the reactor trip and the ESF actuation functions, with the exception of sensors that may be shared.
- Sensor redundancy and diversity contribute to the reliability of PMS. Four sensors normally monitor variables used for an ESF actuation. Also, functional diversity provides protection against common cause failures.
- Provisions are in place for continuous automatic PMS system monitoring and failure detection/alarm.
- PMS equipment accommodates, by design, a loss of the normal heating, ventilation, and air conditioning (HVAC). The passive heat sinks protect PMS equipment on failure or degradation of the active HVAC.
- The reliability of the PMS is important. The COL will maintain the reliability of the PMS.
- The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with standards reported in Chapter 7 of the SSAR, such as IEEE 7-4.3.2 (1993) that has been endorsed by RG 1.152. Elements that contribute to a reliable software design include:
  - A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, Section 5.3, "Quality")
  - A verification and validation program prepared to confirm that the design implemented would function as required (IEEE standard, Section 5.3.4, "Verification and Validation")

- Equipment qualification testing performed to demonstrate that the system will function as required in the environment for which it is intended to be installed (IEEE standard, Section 5.4, "Equipment Qualification")

- Design for system integrity (performing its intended safety function) when subjected to all conditions, external or internal, that have significant potential for defeating the safety function (abnormal conditions and events) (IEEE standard, Section 5.5, "System Integrity")

- Software configuration management process (IEEE standard, Section 5.3.5, "Software Configuration Management").

The following are some important aspects of DAS as represented in the PRA:

- The PRA assumes diversity that eliminates the potential for common cause failures between PMS and DAS. Generation of the DAS automatic actuation signals is in a manner functionally diverse from the PMS signals. The use of different architecture, different hardware implementations, and different software achieves diversity between the DAS and PMS .

- DAS provides control room displays and fixed position controls to allow the operators to take manual actions.

- DAS actuates using 2-out-of-2 logic. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual 2-out-of-2 redundancy, reduces the probability of inadvertent actuation.

- The actuation devices of DAS and PMS are capable of independent operation unaffected by the operation of the other. The DAS will, by design, actuate components only in a manner that initiates the safety function.

- DAS provides capability for on-line testing and calibration of the DAS channels, including sensors.

- Implementation of the DAS manual initiation functions bypasses the signal processing equipment of the DAS automatic logic. This eliminates the potential for common cause failures between automatic and manual DAS functions.

- Implementation of the DAS reactor trip function is through a trip of the control rods via the motor-generator (M-G) set which is separate and diverse from the reactor trip breakers. The COL will maintain the reliability of the M-G set breakers.

- DAS is an important "defense-in-depth" system. The availability of DAS, with respect to both its reactor trip and ESF actuation functions, will be controlled. The COL will maintain its reliability.

The following are some important aspects of PLS as represented in the PRA:

- PLS has redundancy to minimize plant transients.
- PLS provides capability for both automatic control and manual control.
- Redundant signal selectors provide PLS with the ability to obtain inputs from the integrated protection cabinets in the PMS. The signal selector function maintains the independence of the PLS and PMS. The signal selectors select those protection system signals that represent the actual status of the plant and reject erroneous signals.
- Distribution of PLS control functions are across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers.

Onsite Power

The onsite power system consists of the main ac power system and the dc power system. The main ac power system is a non-Class 1E system. The dc power system consists of two independent systems: the Class 1E dc system and the non-Class 1E dc system.

The main ac power system is a non-Class 1E system comprised of a normal, preferred, and standby power system. It distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.

The Class 1E dc and uninterruptible power supply (UPS) system (IDS) provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant.

The non-Class 1E dc and UPS system (EDS) consists of the electric power supply and distribution equipment that provide dc and uninterruptible ac power to non-safety-related loads.

The following are some important aspects of the main ac power system as represented in the PRA:

- The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.
- During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. During plant startup, shutdown, and maintenance, the preferred power supply from the high-voltage switchyard provides the main ac power. The onsite standby power system, powered by the two onsite standby diesel generators, supplies power to selected loads in the event of loss of normal and preferred ac power supplies.
- Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant non-safety-related ac loads.

- On loss of power to a 4160 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers open, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses.

The following are some important aspects of the Class 1E dc and UPS system (IDS) as represented in the PRA:

- There are four independent, Class 1E 125 V dc divisions. Divisions A and D each consist of one battery bank, one switchboard, and one battery charger. Divisions B and C each consist of two battery banks, two switchboards, and two battery chargers. The first battery bank in the four divisions is the 24-hour battery bank. The second battery bank in Divisions B and C is the 72-hour battery bank.

- The 24-hour battery banks provide power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a design-basis accident. The 72-hour battery banks provide power to those loads requiring power for 72 hours following the same event.

- Battery chargers are connected to dc switchboard buses. The input ac power for the Class 1E dc battery chargers is supplied from non-Class 1E 480 V ac diesel-generator-backed motor control centers.

- The 24-hour and 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.

- Electrical isolation and physical separation of each of the four divisions of dc systems prevent an event from causing the loss of more than one division.

- Reliability of the Class 1E batteries is important. The COL will maintain the reliability of the equipment.

The following are some important aspects of the non-Class 1E dc and UPS system as represented in the PRA:

- The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.

- EDS load groups 1, 2, and 3 provide 125 V dc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.

- The onsite standby diesel-generator-backed 480 V ac distribution system provides the normal ac power to the battery chargers.

- The size of the batteries is sufficient to supply the system loads for a period of at least two hours after loss of all ac power sources.

Component Cooling Water System

The CCS is a non-safety-related system that removes heat from various components and transfers the heat to the service water system. The following are some important aspects of the CCS as represented in the PRA:

- The CCS is arranged into two trains. Each train includes one pump and one heat exchanger.
- During normal operation, one CCS pump is operating. The standby pump alignment will create an automatic start in case of a failure of the operating CCS pump.
- Loading of the CCS pumps on the standby diesel generator is automatic in the event of a loss of normal ac power. The CCS, therefore, continues to provide cooling of required components if normal ac power is lost.

Service Water System

The SWS is a non-safety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere. The following are some important aspects of the SWS as represented in the PRA:

- The SWS is arranged into two trains. Each train includes one pump, one strainer, and one cooling tower cell.
- During normal operation, one SWS train of equipment is operating. The alignment of the standby train ensures automatic start in case of a failure of the operating SWS pump.
- Loading of the SWS pumps and cooling tower fans onto their associated diesel bus is automatic in the event of a loss of normal ac power. Both pumps and cooling tower fans automatically start after power from the diesel generator is available.

Chemical and Volume Control System

The CVS provides a safety-related means to accomplish the following tasks: (1) terminate an inadvertent RCS boron dilution and (2) isolate normal CVS letdown during shutdown operation on low hot-leg level. In addition, the CVS provides a non-safety-related means to perform the following functions: (1) provide makeup water to the RCS during normal plant operation, (2) provide boration following a failure of reactor trip, and (3) provide coolant to the pressurizer auxiliary spray line.

The following are some important aspects of CVS as represented in the PRA:

- The CVS has two makeup pumps and each pump is capable of providing normal makeup.
- The configuration is such that one CVS pump operates on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically.

- On low hot-leg level, the safety-related PMS signals two safety-related CVS AOVs to close automatically to isolate letdown during Mode 4 (when RNS is in operation), Mode 5, and Mode 6 (with the upper internals in place and the refueling cavity less than half full) as required by AP600 TS.

- The safety-related PMS boron dilution signal automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related CVS demineralized water supply valves. This signal actuates on upon any reactor trip signal, source range flux multiplication signal, low input voltage to the Class 1E dc power system battery chargers, or a safety injection signal.

- The COL applicant will maintain procedures to respond to low hot-leg level alarms. This is COL Action Item 19.1.8-12.

Passive Containment Cooling System

Flooding of the PCS annulus because of plugging of the upper annulus drains is the only PRA-postulated mechanism for the failure of PCS cooling. The probability of plugging is minimized in the design by including the following: (1) two 100 percent drains in the side wall of the shield building, with protective screens to prevent entry of small animals into the drains, and (2) a technical specification requirement to perform surveillance of the annulus floor and drains every two years to identify and to eliminate debris that can potentially plug the drains.

Containment Isolation System

DAS, in addition to PMS, controls containment isolation valves in lines that represent risk-significant release paths to further limit offsite releases following core melt accidents. These lines are: containment air filter supply and exhaust, and normal containment sump. D-RAP includes the containment isolation valves controlled by DAS as risk-significant SSCs. Short term availability controls for DAS address the operability of DAS actuation of these isolation valves .

Reactor Cavity Flooding System

The AP600 design includes a safety-related reactor cavity flooding system to prevent reactor vessel breach and ex-vessel phenomena in the event of a severe accident. The following design features comprise the system:

- two 15.2-cm (6-in.) diameter recirculation lines that provide a path for gravity draining the IRWST to the reactor cavity,

- a squib valve and a motor operated valve in each recirculation line, each powered from the Class 1E dc power supply, and actuated from the control room, and

- a reactor vessel thermal insulation system designed specifically to enhance RPV cooling, as described in Section 19.2.3.3.1 of this report.

Included as risk-significant SSCs within D-RAP are the containment recirculation squib valves and isolation MOVs, and containment recirculation screens.

In-Service Inspection and Testing Programs provide surveillance and maintenance requirements on the related piping and valves.

Specific guidelines are given for the operator action to flood the reactor cavity. Emergency Response Guideline FR.C-1 instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission product releases as determined by a core damage assessment guideline.

Key aspects of the reactor cavity flooding system will be confirmed by ITAAC.

RPV Thermal Insulation System

The AP600 design includes a reflective reactor vessel insulation system that provides an engineered flow path to allow the ingression of water and venting of steam for externally cooling the vessel in the event of a severe accident involving core relocation to the lower plenum. Key attributes of the insulation system are:

- RPV/insulation panel clearances, water entrance and steam exit flow areas, and loss coefficients resulting from scale tests in the ULPU facility,

- the entrance and exit of the insulation boundary incorporate water inlets and steam vents that open because of buoyant forces during cavity flood-up, and

- insulation panels and support members designed to withstand the pressure differential loading as a result of the ERVC boiling phenomena.

There are no applications of coatings to the outside surface of the reactor vessel that will inhibit the wettability of the surface.

A metal grating covers the opening between the vertical access tunnel and the RCDT room that will prevent any large pieces of debris from entering the reactor cavity.

The doorway between the reactor cavity compartment and the RCDT room includes a normally-closed damper. The design of this damper enables it to open passively during containment flood-up to permit flooding of the reactor cavity from the RCDT room, and continued water flow through the opening.

The reactor vessel insulation system and the damper between the reactor cavity and the RCDT room are included as risk-significant SSCs in the reliability assurance program, and key aspects of the as-built system will be confirmed by ITAAC.

Reactor Cavity Design for Direct Containment Heating

The reactor cavity and RPV arrangement provide no direct flow path for the transport of particulated molten debris from the reactor cavity to the upper containment regions.

Reactor Cavity Design for Ex-Vessel Fuel-Coolant Interactions

The design can withstand a best-estimate ex-vessel steam explosion without loss of containment integrity.

Reactor Cavity Design for Core Concrete Interactions

The AP600 is designed for in-vessel retention of molten core debris, however, the reactor cavity design incorporates features that extend the time to basemat melt-through in the event of RPV failure. The cavity design includes:

- a minimum floor area of 48 $m^2$ available for spreading of the molten core debris
- a minimum thickness of concrete above the embedded containment liner of 2.8 ft (0.85 m)
- there is no buried piping in the concrete beneath the reactor cavity, and no enclosed sump drain lines in either the reactor cavity floor or reactor cavity sump concrete. Thus, there is no direct pathway from the reactor cavity to outside the containment in the event of core concrete interactions
- the openings between the reactor cavity and cavity sump are small diameter openings in which core debris will solidify. Thus, there is no direct pathway for core debris to enter the sump except in the case where it might spill over the sump curb.
- The specifications do not include a specific type of concrete for use in the basemat.

Hydrogen Igniter System

The AP600 design includes a hydrogen igniter system to limit the concentration of hydrogen in the containment during severe accidents. The features of the system are:

- 64 glow plug igniters distributed throughout the containment
- powered from the non-safety-related onsite ac power system, but also capable of being powered by offsite ac power, onsite non-essential diesel generators, or non Class 1E batteries via dc-to-ac inverters.
- manually actuated from the control room when core exit temperature exceeds 1200F, as the first step in ERG FR.C-1 to ensure that the igniter activation occurs before rapid cladding oxidation.

The igniter system is non-safety-related but is subject to investment protection short-term availability controls.

The AP600 design also includes four passive autocatalytic recombiners (PARs) strategically located within the containment. The primary function of the PARs is to cope with hydrogen

production during design-basis accidents, but the expectation is that they will function to reduce combustible gas concentrations during severe accidents as well.

Protection of Containment from Diffusion Flames

The containment layout prevents the formation of diffusion flames that can challenge the integrity of the containment shell. Specifically:

- the openings from the accumulator rooms and CVS compartments that can vent hydrogen to the CMT room are either away from the containment wall and electrical penetration junction boxes, or covered by a secure hatch, and
- the orientation of IRWST vents near the containment wall direct releases away from the containment shell.

These provisions will be confirmed by ITAAC.

Operation of ADS stage 4 provides a vent path for the severe accident hydrogen to the steam generator compartments, bypassing the IRWST, and mitigating the conditions required to produce a diffusion flame near the containment wall.

Non-safety Containment Spray

The AP600 design includes a non-safety grade containment spray system with the capability to supply water to the containment spray header from an external source in the event of a severe accident. Loss of ac power does not contribute significantly to the core damage frequency, therefore, non-safety-related containment spray does not need to be ac independent. The COL applicant will develop and implement guidance and procedures for use of the non-safety containment spray system as part of COL Action Item 19.2.5-1 regarding the accident management program.

Containment Vent

In the event of a severe accident that results in gradual containment pressurization, it is possible to vent the AP600 containment to the spent fuel pool via the residual heat removal suction lines. The vent process would be initiated by opening the manual valve from the spent fuel pool to the RNS pump suction and then remotely operating the RNS hot-leg suction isolation valves.

The COL applicant, as part of COL Action Item 19.2.5-1 regarding accident management, will develop detailed procedures for use of the containment vent system.

Accident Management

The COL applicant will develop and implement severe accident management guidance and procedures using the framework provided in WCAP-13914, Revision 3 (see COL Action Item 19.2.5-1).

Containment Closure During Shutdown Operations

The technical specification concerning containment penetrations (TS 3.6.8) will not permit containment hatches, air locks, or spare penetrations to be open during shutdown unless the penetrations can be closed before steaming into the containment. Also, SSAR Section 3.8.2.1.3 and the technical specification bases, indicate that each of the two equipment hatches in the AP600 design can be installed using a dedicated set of hardware, tools, and equipment, and that a self-contained power source is provided to drive each hoist while lowering the hatch into position. Accordingly, the expectation is that the likelihood of failure to achieve containment closure is an insignificant contributor to containment failure.

19.1.9 Conclusions and Findings

The NRC has evaluated the AP600 design PRA quality and its use in the design and certification processes. The NRC concludes that the quality and completeness of the AP600 PRA is adequate for its intended purposes, such as supporting the design and certification processes. The approaches used by the applicant for both the core damage and containment analyses are logical and sufficient to achieve the desired goals of describing and quantifying potential core damage scenarios and containment performance during severe accidents. The NRC concludes that the use of PRA in the AP600 design process helped improve the unique passive features of the design by better understanding plant response, including potential system interactions, during postulated beyond-design-basis accidents. Such features contributed to the reduced CDF and CCFP estimates of the AP600 design when compared with operating PWRs. PRA results and insights were used to identify areas where it is particularly important to implement the certification and operational requirements assumed during the design and certification processes (e.g., ITAACs, RTNSS requirements, D-RAP, COL Action Items and Technical Specifications). On the basis of this review the NRC believes that the AP600 design meets NRC's safety goals and represents an improvement in safety over operating PWRs in the United States.

19.1.10 Resolution of DSER Open Items

The staff reviewed the quality of the PRA submittal by evaluating the models, techniques, methodologies, assumptions, data, and calculational tools that were used by Westinghouse as discussed in Section 19.1.1.2 of this report. A summary of the resolution of the DSER Open Items is discussed below.

Open Item 19.1.3.1-1: The staff requested Westinghouse to justify assumptions and data used in calculating pipe break initiating event frequencies. Westinghouse assessed the pipe break contribution to the LOCA frequency by performing a pipe break analysis to identify pipe sizes and sections (pipe segments between major discontinuities, such as valves) and assuming an hourly failure rate of 4.25E-10 events per hour for each pipe section (independently of the size of the pipe). The staff found that Westinghouse had not provided adequate justification of (1) the assumed failure rate (4.25E-10/hr per pipe section for all pipe sizes except for the PRHR tubes), (2) the assumption that the PRHR tube rupture frequency (5.0E-04/year) is approximately an order of magnitude lower than the frequency of a SGTR event, and (3) the basis for the assumed apportioning of this failure rate among small, medium and large LOCAs. Westinghouse justified the assumed failure rate (4.25E-10/hr) per pipe section using the

"leak-before-break" argument and data from EPRI's "Utility Requirements Document" (URD). With respect to the assumed failure rate for the PRHR tubes, Westinghouse listed a number of factors that are expected to reduce the failure rate of PRHR tubes as compared to SG tubes (e.g., fewer and shorter tubes and less adverse operating conditions). Westinghouse also explained that the assumed apportionment of the pipe failure rate among small, medium and large LOCAs was based on AP600 tube sizes. In addition to the above information, Westinghouse provided the results of sensitivity studies which show that PRA results and insights are not impacted significantly by reasonable changes in parameters defining the issues mentioned in this DSER open item. Based on Westinghouse's "leak-before-break" argument, data from EPRI's URD, the factors that are expected to reduce the failure rate of the PRHR tubes as compared to SG tubes, and the results of the sensitivity studies the staff finds this acceptable. This open item is resolved.

Open Item 19.1.3.1-2: The staff requested Westinghouse to provide documentation supporting the assumed contribution to LOCA initiating event frequencies attributable to non-break failures, such as spurious opening (and stuck open) of pressurizer safety valves (medium LOCA), spurious actuation (opening) of one line of an ADS stage (medium LOCA), and spurious opening of more than one line of ADS (large LOCA). In its response, Westinghouse provided an explanation of how I&C logic failures, mechanical failures and operator actions could cause spurious actuations and contribute to the LOCA initiating event frequencies. Also, Westinghouse's response documented the methodology that was used and the assumptions that were made in calculating these contributions. The information provided by Westinghouse adequately supported the assumed contribution to LOCA, and is therefore, acceptable. This open item is resolved.

Open Item 19.1.3.1-3: Westinghouse was asked to provide better justification and documentation for the success criteria for passive systems and operator actions assumed in the AP600 PRA models. This issue is of particular importance to AP600 design because of the presence of passive safety-related systems. The AP600 PRA models assume perfect reliability for the passive systems following actuation (i.e., once they start-up) and does not take into account uncertainties in thermohydraulic (T-H) parameters (e.g., heat transfer coefficients and friction factors which, given the small heat rates and driving forces associated with passive systems, could be significant for the AP600 design), in T-H phenomena modeling (e.g., modeling ADS blowdown) or uncertainties as a result of code deficiencies (e.g., due to using the code outside the range of its applicability). Such uncertainties could affect: (1) the system success criteria (e.g., the number of CMTs required to operate within a certain time window to avoid core damage), in general sequence dependent; (2) the timing of events in a sequence (e.g., time available to the operator to depressurize the RCS for short-term cooling by gravity injection); and (3) the event tree models (e.g., by underestimating pressures which would cause some safety relief valves to open and stick open). The staff asked Westinghouse to account for T-H uncertainties in establishing success criteria for passive systems and operator actions. The staff's evaluation of the T-H uncertainties can be found in sections 22.5.4.1 and 22.5.4.4 of this report. On the basis of the evaluation contained in these sections the information provided by Westinghouse is acceptable and this open item is resolved.

Open Item 19.1.3.1-4: This DSER open item involves LOCA sequences with impaired containment. These sequences were not quantified in the PRA. The staff requested Westinghouse to either modify the event trees by modeling recovery actions or count these sequences as leading to core damage with open containment. Westinghouse responded that

these sequences are not significant risk contributors because (1) analyses show that sufficient water for long-term recirculation cooling of the core is available for at least 2.7 days when containment isolation fails and (2) successful recovery actions are very likely (e.g., provide inventory makeup through the safety-related makeup connection from outside the containment to the IRWST or by repairing and using the plant pumped systems). The staff's review found Westinghouse's response, including related analyses, acceptable. This open item is resolved.

Open Item 19.1.3.1-5: The staff asked Westinghouse to address inconsistencies in several sequence transfers between event trees, such as success and failure of the same system in the same accident sequence. Westinghouse addressed this issue in the revised PRA by providing adequate explanation of transfers between event trees and adding a list in the PRA identifying consequential failure events. This is acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.1-6: This DSER open item involves long-term cooling, beyond 24 hours, in sequences where the reactor is initially maintained at high pressure with containment isolation successful (Westinghouse assumes a mission time of 24 hours for long-term cooling independently of plant condition). The staff asked Westinghouse to justify this assumption (e.g., by showing, through a bounding analysis, that the residual risk is not significant) or extend the PRA models beyond 24 hours (to a point in time where it can be argued that the residual risk is not significant). Sequences of most concern involved transients with loss of main feedwater where the use of the PRHR HX for long-term cooling causes the IRWST water to heat up, resulting in inventory loss through evaporation. To ensure successful long-term cooling by the PRHR HX (i.e., without depressurizing the RCS), the evaporated IRWST inventory must return to the IRWST after condensed on the containment liner and collected in the IRWST gutter system. Westinghouse responded by changing the design of the gutter system from non-safety-related to safety-related and by incorporated features which ensure that the gutter system valves direct water to the IRWST during accidents (e.g., the valves that re-direct the flow are actuated automatically by PMS and DAS and fail-safe on loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal). For sequences other than transients with loss of main feedwater, Westinghouse provided information showing that the residual risk associated with long-term cooling (beyond 24 hours) is not risk significant. Based on the above mentioned design changes and the results of the assessment of residual risk associated with long term cooling, the staff finds this acceptable. This open item is resolved.

Open Item 19.1.3.1-7: The staff asked Westinghouse to correct several inconsistencies and provide better documentation of support system PRA models (e.g., using same event name for different failure modes). The revised PRA removed such inconsistencies and provided much better documentation of support system PRA models, and is therefore, acceptable. This open item is resolved.

Open Item 19.1.3.1-8: The pre-DSER AP600 PRA included a large number of modularized fault trees that used the same name for different failure modes. To avoid confusion in interpreting PRA results, the staff asked Westinghouse to rename some of these modules. These modules were renamed in the revised PRA, and are therefore, acceptable. This open item is resolved.

Open Item 19.1.3.1-9: The pre-DSER AP600 PRA contained descriptions of design changes that have been made and not included in the PRA. This documentation in all cases indicated that the design changes had no effect on PRA results and insights. The staff asked Westinghouse to justify these statements and verify that the PRA models are representative of the AP600 design. Westinghouse provided documentation in the revised PRA verifying that the PRA models are representative of the AP600 design. This is acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.1-10: Westinghouse used generic failure data in the AP600 PRA that are representative of components used in previous PRAs for operating reactors. The staff asked Westinghouse to justify the applicability of some of these data to the AP600 environment and operating conditions. An example is the failure rate used for the check valves (CVs) in the IRWST injection lines. Such CVs will have to open under very low differential pressures (created by the gravity driving head only) after long periods of being held closed (testing every two years at refueling) in the presence of stagnant borated water. This issue was addressed by (1) design changes (e.g., some check valves in the IRWST injection lines have been replaced by squib valves, thus eliminating the high differential pressure normal operating environment that the check valves would experience in the original design) and (2) by analyses showing that certain categories of failures that appear in data for operating reactors are not applicable in the AP600 design. In addition, uncertainties associated with assumed failure rates for some highly risk important components (such as IRWST injection check valves) were addressed by requiring availability control of non-safety-related systems performing "defense-in-depth" functions (e.g., injection by the RNS pumps is redundant to IRWST gravity injection) according to the RTNSS process. Based on the above mentioned design changes, analyses, and availability controls, the staff finds this acceptable. This open item is resolved.

Open Item 19.1.3.1-11: Westinghouse was asked to justify and document the logic and instrumentation failure data for the microprocessor-based components used in the PRA. This information was made available to the staff and found to be acceptable. This open item is resolved.

Open Item 19.1.3.1-12: Westinghouse was asked to provide a description and a complete listing of the error factors associated with random (and other) failure rates. The pre-DSER uncertainty analysis documented only a few of the error factors, and it was not clear what error factors, if any, had been used for some events in the uncertainty analysis. Westinghouse provided this information with a completely revised uncertainty analysis. The staff reviewed this revised uncertainty analysis and found it acceptable. This open item is resolved.

Open Item 19.1.3.1-13: The staff asked Westinghouse to justify the common-cause failure probability for IRWST injection check valves (CVs). This issue involved CCF histories at operating reactors and their applicability to AP600 CVs. The CCF probabilities of CVs, assumed in the AP600 PRA, are on the basis of information provided in the last revision (Revision 6) of EPRI's URD. The information on CCF of check valves, as revised in the last revision of EPRI's URD, leads to a decrease by about an order of magnitude in the value of CCF probability recommended in previous URD revisions which was used in previous PRAs for evolutionary designs and operating reactors. According to Westinghouse this is the result of better understanding of individual events involving failure of check valves at nuclear power plants and that "EPRI found no common cause failures to open of check valves (other than failure modes unique to testable check valves)." An NRC-sponsored evaluation of LER and

NPRDS events (see Common-Cause Failure data Collection and Analysis System, INEL-94/0064, December 1995), which occurred between 1980 and 1993 at operating nuclear power plants, has found about twenty events involving common cause failure of check valves. Although it can be argued that only a portion of such events are applicable to the AP600 design, the staff believes that there is still significant uncertainty in the data used to calculate CCF probabilities of CVs in the AP600 PRA. This uncertainty was addressed by requiring availability control of non-safety-related systems performing "defense-in-depth" functions (e.g., injection by the RNS pumps is redundant to IRWST gravity injection) according to the RTNSS process. The staff finds this to be acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.1-14: Westinghouse was asked to justify and document common-cause failure probabilities for I&C hardware components used in the PRA. This information was made available to the staff and was found acceptable. This open item is resolved.

Open Item 19.1.3.1-15: Westinghouse was asked to justify and document the I&C software failure probabilities used in the AP600 PRA. Digital I&C systems are designed as complex combinations of hardware and software (i.e., computer programs) components. Although computer software does not wear out, as hardware does, it fails as a consequence of the excitation of residual design errors when a particular combination of inputs occurs. If one could eliminate all the design errors before a software product is put in operation, it would work perfectly for ever. However, it is impossible to be certain that a software product is error free. On the contrary, experience shows that there are always residual faults that do not show up, and thus they do not cause a software failure, unless the program is exposed to an environment for which it was not designed or tested. Exposure to such an environment is possible because, due to the large number of possible states and inputs in most software programs, it is extremely difficult to perfectly comprehend program requirements and implementation and virtually impossible to test more than a small subset of all possible input combinations during development. Thus, software reliability is essentially a measure of the confidence one has in the design of the software and its ability to function properly in its expected environment. Quantification of software reliability may be too difficult, especially for software which must meet high reliability requirements such as those used in the AP600 design. This is the result of the random nature of a large number of possible inputs, the unknown mechanisms of human failure which create errors during the development process and the randomness of the testing process used to detect errors. However, regardless of whether the reliability of software can be accurately quantified, the design goal must be to minimize the number of residual errors, their frequency of occurrence, and their effect on system performance. This can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program. For these reasons, each software product is unique and extrapolation of statistical data for other products is meaningless. From the basic properties of software it follows that commonly used hardware redundancy techniques do not improve software reliability. The several defense mechanisms against hardware CCFs that are incorporated in the design (such as redundancy, separation, operational testing, maintenance, and immediate detectability of failure provided by the on-line diagnostics) cannot be relied on to prevent software CCFs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a common mode software failure in all channels (or divisions) at the same time (i.e., it would be a CCF of redundant channels or divisions). Thus, a highly reliable software product is needed whenever the same program is executed in two or more channels (or divisions) in parallel. Since the

reliability of a software product is basically determined during development and testing, the importance of the software development process in achieving high reliability cannot be overestimated. Although it is not easy to quantify software reliability, it is generally accepted that high reliability can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program in accordance with IEEE standards. The AP600 design PRA assumes high reliability for all software used in the digital I&C systems. Westinghouse expects to develop highly reliable software for the AP600 I&C systems by setting reliability goals and design requirements and by incorporating features in the software design which act as "defenses" against CCF. Westinghouse has agreed to follow IEEE standards as discussed in Chapter 7 of the SSAR. The uncertainty in the software failure probability used in the AP600 PRA was further addressed by requiring availability control of non-safety-related systems performing "defense-in-depth" functions (i.e., the ESF actuation portion of DAS which is redundant and diverse to the ESF actuation portion of the safety-related PMS) according to the RTNSS process. The above mentioned IEEE standards and availability controls on DAS justify the I&C software probabilities assumed in the PRA, and are therefore, acceptable. This open item is resolved.

Open Item 19.1.3.1-16: The staff asked Westinghouse to provide additional documentation and justification of (1) the assumptions made in the PRA regarding the frequency of unscheduled maintenance, (2) the assumed and allowed (if applicable) outage times, and (3) the assumed error factors (or distribution parameters) for maintenance duration and component unavailability as a result of maintenance that were used in the uncertainty analysis. In particular, it was not clear whether the frequency of unscheduled maintenance that could affect the unavailability of safety-related "passive" systems was modeled in the PRA. For example, it was mentioned that the normally closed air-operated valves in the CMTs are exercise-tested every three months. Although failure unavailabilities were on the basis of quarterly testing, which implies that faulty valve repair will occur upon detection, the PRA did not model the valve unavailability as a result of such unscheduled maintenance (neither was a justification for not modeling it provided). This seemed true, also, for several other systems, such as the PRHR and the ADS. The revised PRA provides this information, and the staff review found it to be acceptable. This open item is resolved.

Open Item 19.1.3.1-17: Westinghouse was asked to revise the Human Reliability Analysis (HRA) to follow acceptable HRA modeling techniques and procedures. The staff identified substantial quality problems in the implementation of the HRA which had the potential of impacting several risk important human error probability (HEP) estimates as well as the plant CDF estimate. For example, in many cases, Westinghouse did not follow proper HRA modeling practices in modifying failure rates to account for dependency, stress level, time available and recovery. Westinghouse performed a major revision of the HRA and addressed the staff's concerns by either following acceptable HRA modeling techniques and procedures, or by performing sensitivity studies and showing that the impact of such HRA modeling techniques and procedures on PRA results and insights is not significant. The staff's review found this to be acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.1-18: The staff asked Westinghouse to document assumptions made in the HRA about the control room design and the emergency operating procedures. The revised HRA provides this information. The staff finds this acceptable. This open item is resolved.

Open Item 19.1.3.1-19: Westinghouse was asked to address crew response during common-cause failure of several I&C components. The concern was that same credit was taken in the PRA for operator actions irrespective of the number of I&C failed components. Westinghouse responded by listing the information expected to be available to the operator during several risk important scenarios involving common-cause I&C failures. Westinghouse's response has shown that adequate indications are available to the operator during risk-important accident scenarios even when common-cause I&C failures occur. Therefore, this is acceptable and this open item is resolved.

Open Item 19.1.3.1-20: Westinghouse was asked to take into account the high operator stress level in estimating HEPs for operator actions occurring during an ATWS accident. Westinghouse re-calculated these HEPs as suggested by the staff. The staff reviewed these revised HEPs and found them acceptable. This open item is resolved.

Open Item 19.1.3.1-21: The staff asked Westinghouse to document the dominant cutsets by accident sequence for all the top accident sequences which cumulatively contribute at least 90 percent to the total CDF from internal events. In addition, the staff asked Westinghouse to include some important cutsets that were missing in the pre-DSER PRA. Westinghouse provided the requested information, and the staff found it acceptable. This open item is resolved.

Open Item 19.1.3.1-22: Westinghouse was asked to verify that the dominant cutsets do not contain correlated events. The potential for the dominant cutsets to contain correlated events was not fully reviewed and assessed by Westinghouse in the pre-DSER PRA. The staff's review of the pre-DSER dominant cut sets indicated a close review and assessment of the sequences that are dominated by common cause failure of the I&C systems should had been included in the correlated event analysis. In the revised PRA, Westinghouse provided the requested information, and the staff found it to be acceptable. This open item is resolved.

Open Item 19.1.3.1-23: Westinghouse was asked to perform an uncertainty analysis and identify the major contributors to the uncertainty associated with the CDF estimates. Westinghouse included an uncertainty analysis in the revised PRA, and the staff found it acceptable. This open item is resolved.

Open Item 19.1.3.1-24: Westinghouse was asked to expand its risk importance analysis and provide proper interpretation of results. The pre-DSER importance analysis was not complete. Although all basic events modeled in the PRA (SSCs, initiators and human actions) had been ranked according to their risk importance, no proper interpretation of the importance analysis results had been made and no dominant contributors had been selected. In the revised PRA, Westinghouse provided the requested information, and the staff's review found it to be acceptable. This open item is resolved.

Open Item 19.1.3.1-25: Westinghouse submitted sensitivity studies as part of the RAI process in the original (pre-DSER) PRA submittal. These sensitivity studies investigated the impact of changes in the numerical values of several basic events on core damage frequency. The staff asked Westinghouse to perform additional sensitivity studies, as necessary, to determine (1) the sensitivity of the estimated CDF to potential biases in numerical values, (2) the impact of potential lack of modeling details on the estimated CDF, and (3) the sensitivity of the estimated

CDF to previously raised issues. In the revised PRA, Westinghouse used the results of sensitivity studies extensively to determine the risk significance of various issues raised by the staff and to gain insights about the design. The staff's review found this to be acceptable. This open item is resolved.

Open Item 19.1.3.1-26: The staff asked Westinghouse to use insights from the sensitivity, uncertainty and importance analyses in an integrated fashion, in conjunction with key assumptions from the entire PRA (i.e., all three PRA levels for both internal and external events and for all modes of operation) to identify design certification and operational requirements (such as ITAACs, RAP, Technical Specifications, administrative controls, procedures) as well as COL and interface requirements. Westinghouse provided the requested information, and the staff's review found it to be acceptable. This open item is resolved.

Open Item 19.1.3.1-27: The staff identified technical and documentation concerns during the review of the original Level 2 PRA (Revision 0) and the supporting technical evaluations provided in WCAP-13388. Westinghouse modified the Level 2 and 3 portions of the PRA to address these concerns, but did not submit the revised analyses in sufficient time for the staff to complete its review before the DSER. Accordingly, the review of the Level 2 and 3 PRA was identified as Open Item 19.1.3.1-27.

Revised Level 2 and 3 analyses were submitted in Revision 1 of the PRA (July 1994). The analyses were subsequently requantified in Revision 3 of the PRA (February 1995) to reflect changes in the Level 1 analysis, but this requantification did not involve any changes in the Level 2 and 3 models or assumptions. The revised Level 2 and 3 analyses included the following:

- modified containment event trees (CETs) with expanded treatment of severe accident challenges and late containment failure modes
- decomposition event trees (DETs) to represent the impact of key severe accident phenomena and underlying parameters and processes
- incorporation of a containment fragility curve for assessing the likelihood of containment failure at pressures less than the ultimate capacity
- an expanded set of fission product release categories to provide better resolution in classifying/grouping CET end-states
- revised accident progression analyses dependent on an updated version of the MAAP code
- additional MAAP sensitivity analyses
- revised source term estimates for each release class on the basis of revised MAAP analyses
- modified input assumptions for decontamination factors
- revised offsite consequence (MACCS) calculations

In its review of the revised Level 2 and 3 analyses, the staff identified a need for additional information/justification regarding the model changes, including: (1) documentation of the interface between the Level 1 and Level 2 analyses, (2) justification for the structure and quantification of each of the DETs, and the impact of uncertainties on the DETs, (3) bases for omitting certain containment failure modes in the revised CET, (4) sensitivity and importance analyses for containment performance, and (5) justification and documentation of the process for binning accident sequences into release categories, and assigning source terms to these categories. The staff requested additional information to address these concerns in a January 20, 1995 letter to Westinghouse. In response to staff concerns, Westinghouse substantially modified the PRA and submitted the revised analyses as Revision 8 to the PRA (September 1996). The PRA modifications and staff views on the revised analyses are summarized below.

Documentation of the Level 2 analysis and the interfaces with the Level 1 and 3 analyses was substantially improved. The documentation includes the following:

- details regarding the analyses supporting the Level 2 models and assumptions
- additional information regarding the binning processes and interfaces with the Level 1 and 3 analyses
- listings of the dominant sequences and cutsets contributing to each accident class, each release category, and the large release frequency

The revised PRA documentation is comprehensive and provides a coherent description of the interfaces between the various portions of the PRA, the underlying details of the level 2 analyses, and the risk results. The documentation represents a significant improvement over the original documentation and resolves previous staff concerns in this area.

Contentious DETs were replaced with either more detailed technical analyses or bounding treatment of the related issues in the CET. The DETs for in-vessel retention of core debris and in-vessel steam explosion were replaced with detailed, peer-reviewed evaluations of these issues using the ROAAM approach. Sections 19.2.3.3.1 and 19.2.3.3.5.1 of this report, respectively, provide the staff's review of these evaluations. The staff considers that these evaluations provide a technically sound assessment of the issues and are of sufficient rigor and quality to support the related PRA models.

A bounding assumption that high pressure core melt accidents would always result in thermally-induced SGTR replaced the DET for thermally-induced failures of the RCS pressure boundary. Similarly, a bounding assumption that RPV failure and debris relocation into the reactor cavity will always result in early containment failure replaced the DETs for ex-vessel steam explosion and ex-vessel debris coolability. Although these assumptions bias risk results, as discussed in Sections 19.1.3.2.3 and 19.1.3.3.3 of this report, they conservatively bound uncertainties in related severe accident phenomena. The staff considers the simplified PRA treatment, in conjunction with supporting sensitivity analyses, adequate for design certification.

A more detailed assessment of hydrogen mixing and combustion provided in Chapter 41 of the PRA replaced the DET for hydrogen combustion. The threat from deflagrations,

deflagration-to-detonation transition, and diffusion flames was evaluated for different time periods and hydrogen release locations, with explicit treatment of the effects of RPV reflood on hydrogen generation and distribution. The assessment of deflagration pressure loads included development of probability distributions for the quantity of hydrogen generated and the baseline containment pressure, and comparison of peak pressure distributions with the containment failure probability distribution. Using the Sherman-Berman methodology that was developed under NRC-sponsorship, the potential for deflagration-to-detonation transition was evaluated for the early timeframe (during hydrogen release to containment) and the intermediate timeframe (when hydrogen is mixed in the containment atmosphere). An expanded set of MAAP analyses for AP600 substantiated the characterization of hydrogen combustion threat and the quantification of the revised event trees. Sections 6.2.5 and 19.1.3.2.3 of this report describe the staff's review of hydrogen combustion. Notwithstanding a concern regarding optimistic treatment of diffusion flames in the baseline PRA, the staff considers the PRA treatment of hydrogen combustion to be comprehensive, and in conjunction with supporting sensitivity analyses, adequate for design certification.

The analysis incorporated a containment fragility curve to quantify the likelihood of containment over-pressure failure. As described in Section 19.2.6 of this report, the staff finds Westinghouse's overall containment failure probability distribution acceptable on the basis of independent staff calculations. The application of this distribution within the Level 2 analysis, e.g., for assessing the probability of containment failure from hydrogen deflagrations, is consistent with PRA practice, and is therefore, acceptable. This resolves previous staff concerns in this area.

As part of the staff's review of the PRA quantification process, data and information for the Level 1 and 2 portions of the AP600 PRA model for internally-initiated events were loaded into the NRC's library of plant databases for use with the staff's Safety Analysis Program for Hands-on Integrated Reliability Evaluations (SAPHIRE) code (on the basis of Revision 0 through Revision 8 of the PRA). A comparison of Westinghouse and SAPHIRE results for the Level 2 analysis shows good overall agreement in terms of the dominant containment event tree sequences and their frequencies, and provides limited confirmation that the binning and event tree quantification in the Westinghouse analysis were properly carried out.

Westinghouse performed additional MAAP analyses to more fully investigate and substantiate the treatment of accident progression and related issues in the Level 2 analysis. In Chapters 34 and 41 of the PRA, Westinghouse documents MAAP analyses performed for a spectrum of accident sequences. In general, Westinghouse performed a separate MAAP analysis for the frequency-dominant accident sequence in each accident class. Additional cases were run as sensitivity analyses to explore the impact of different system availability assumptions, initiating events, and containment failure modes on event progression. Where MAAP results were recognized as sensitive to these parameters, Westinghouse tended to adopt the more conservative cases for subsequent analyses. Each of the major CET sequences contributing to large release frequency are represented by a MAAP run, with the exception of ATWS sequences for which accident response was determined using the LOFTRAN code.

MAAP results include the chronology of major events in the accident progression, RCS and containment pressure and temperature response, water levels and hydrogen/air/steam concentrations within major subcompartments, and source term releases to the containment

and the environment. Westinghouse used this information to substantiate the treatment of containment failure modes, hydrogen generation and combustion, reactor cavity flooding and RPV reflooding, and assignment of source terms in the Level 2 analysis. The staff performed confirmatory calculations for a limited number of sequences using the MELCOR code at two different stages of the AP600 design evolution. Although these calculations revealed some significant differences in predicted behavior, the code comparisons confirm the order and approximate timing of major events in the accident progression, and the overall thermal hydraulic behavior during the accidents analyzed. In view of this confirmation, and the generally conservative approach used by Westinghouse for selecting sequences for further analyses, the staff concludes that use of the MAAP results provides an acceptable basis for characterizing accident progression in the Level 2 analysis.

In Chapter 45 of the PRA, Westinghouse documents a systematic process used to assign source terms to each release category. For each release category Westinghouse identified a representative source term by comparing source terms for the various accident classes and sequences binned within the release category, and selecting the one that bounds all accident classes for that release category in terms of noble gas, volatile and non-volatile releases. Westinghouse performed a limited sensitivity studies to assess the impact of fission product release and removal models on the source term results, and to show that the default values used in the MAAP calculations provide conservative results. Comparisons of AP600 source terms with NUREG-1150 results (for the closest corresponding release scenario) were also made, and show reasonable agreement. The staff concludes that the process for assigning source terms is acceptable and resolves previous concerns in this area.

Westinghouse and NRC performed sensitivity and importance analyses to address key Level 2 and 3 issues. This included an assessment of the importance of the various CET top events to containment performance, and the sensitivity of containment performance and risk to changes in system failure rates, human error probabilities, and other modeling assumptions. Chapter 50 of the PRA and Sections 19.1.3.2.3 and 19.1.3.3.3 of this report provide insights from the sensitivity and importance analyses.

The staff concludes that all issues related to the Level 2 and 3 PRA have been adequately addressed. This resolves DSER Open Item 19.1.3.1-27.

Open Item 19.1.3.2-1: The staff did not include an evaluation of the risk-based seismic margins analysis (SMA) in the DSER because Westinghouse submitted this analysis at about the same time the DSER was due. The staff subsequently reviewed the SMA, requested additional information by Westinghouse and received satisfactory responses. The staff finds the SMA acceptable. This open item is resolved.

Open Item 19.1.3.2-2: The staff requested that Westinghouse improve the documentation of the fire risk study to support the review. The modeling approach, key assumptions, intermediate results, and final results are now clearly presented. The staff's review found it to be acceptable. This open item is resolved.

Open Item 19.1.3.2-3: The staff requested that Westinghouse clarify whether postulated fire scenarios involve fire areas or fire zones, referring to the fire areas/zones identified in the SSAR. The staff also requested that Westinghouse identify fire areas having two or more

safety-related divisions. The fire PRA now clearly indicates where the analysis is performed on a fire area basis (most of the fire scenarios) and where it is performed on a fire zone basis (the containment fire scenarios). On the basis of the PRA documentation, identification of areas/zones containing two or more safety-related divisions is possible, and is therefore, acceptable. This open item is resolved.

Open Item 19.1.3.2-4: The staff requested that Westinghouse redo the analysis without taking credit for fire barriers with less than a 3-hour rating. The fire PRA now does not take credit for barriers between fire zones for most areas of the plant; fires are assumed to cause damage of all equipment within a fire area. The lone exception is the containment. In its response to RAI 720.334, Westinghouse justifies the neglect of fire propagation between zones resulting from the use of fire or structural barriers without penetrations, labyrinth passageways, or open space. As a general principle, the staff does not accept neglect of cross-zone fire propagation without a detailed analysis of possible fires and their effects. However, in the case of the AP600 containment fire analysis, the staff believes that no significant impact to the study's risk insights will occur if cross-zone scenarios are treated because (1) the containment scenarios already dominate the fire risk, (2) the fire risk analysis does not take credit for non-safety equipment outside of containment, and (3) the likelihood of extremely severe containment fires is low, on the basis of past experience with operating reactors and on the AP600's use of sealed-can reactor coolant pumps. The staff finds the above justification for crediting less that 3-hour fire barriers inside the containment acceptable. This open item is resolved.

Open Item 19.1.3.2-5: The staff requested that Westinghouse analyze MCR fires. The fire PRA now includes analyses of several MCR fire scenarios. The staff does not concur with the analyses' detailed assumptions concerning fire frequency, the probability of large fires involving the mimic panel, and the probability of hot shorts. However, staff-performed sensitivity analyses addressing these issues indicate that the potential impact on CDF is not large and that the MCR is not a dominant contributor to risk. Therefore, this is acceptable and this open item is resolved.

Open Item 19.1.3.2-6: The staff requested that Westinghouse analyze fires during shutdown conditions. The fire PRA now addresses this issue with an analysis comparable in detail to that for at-power conditions. The staff finds the shutdown fire risk analysis to be acceptable. This open item is resolved.

Open Item 19.1.3.2-7: The staff requested that Westinghouse analyze fire-induced opening of the ADS valves. The fire PRA now treats medium and large LOCA events as a result of this issue. Fire-induced LOCA scenarios now constitute 96 percent of the total fire CDF. The staff found Westinghouse's analysis to acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.2-8: The staff requested that Westinghouse analyze lube oil fires in the PRA. This has been done implicitly; the PRA now assumes that fires in the turbine building cause the loss of all equipment in the turbine building. The analysis now also accounts for the possibility of fire spread from the turbine building to the auxiliary building (including Fire Area 1201 AF 05, which is at grade level), and is therefore, acceptable. This open item is resolved.

Open Item 19.1.3.2-9: The staff requested that Westinghouse analyze fire-induced LOOP events. The fire PRA now includes these events which the staff has reviewed and found to be acceptable. They constitute about 2 percent of the total fire CDF. This open item is resolved.

Open Item 19.1.3.2-10: The staff requested that Westinghouse list all operator actions credited in the fire analysis. The current fire PRA does not credit local operator actions or recovery actions. The PRA does indicate operator actions taken at the remote shutdown workstation in the event of a severe MCR fire. The PRA also includes sensitivity studies that show that the risk impact is minimal if no credit is taken for any operator actions. This open item is resolved.

Open Item 19.1.3.2-11: The staff requested that Westinghouse identify the risk dominant fire minimal cutsets. Table 57-12 of the PRA now lists the top 200 fire minimal cutsets, which contribute about 92 percent to the total fire CDF. This open item is resolved.

Open Item 19.1.3.2-12: The staff requested that Westinghouse recalculate the CDF assuming that all of the non-safety-related systems are failed. This has been done; all of the conditional core damage probabilities, given fire damage, are calculated in the fire PRA using the "focused" PRA model for internal events, and is therefore, acceptable. This open item is resolved.

Open Item 19.1.3.2-13: The staff requested that Westinghouse perform sensitivity and importance analyses to assist the staff in identifying leading contributors to fire risk. Westinghouse has performed a number of sensitivity studies in the MCR analysis to show the impact of different human error probability assumptions. Westinghouse also performed a sensitivity study investigating the impact of containment fire-induced hot shorts during shutdown. Westinghouse has not performed importance analyses; the fire PRA states that the results of such an analysis will be misleading because the PRA employs numerous conservatisms. The staff does not concur with this argument. However, sufficient information is now provided by the current PRA (see Open Item 19.1.3.2-2) that the staff can identify the important fire risk contributors (by area and by initiator). This open item is resolved.

Open Item 19.1.3.2-14: In the pre-DSER fire PRA, Westinghouse made references to the SSAR without providing specific page, table or figure numbers. Westinghouse was asked to include in the revised PRA specific references to information in the SSAR and complete layout drawings of the plant. The revised PRA includes this information and references to the SSAR are clear. This is acceptable; therefore, this open item is resolved.

Open Item 19.1.3.2-15: Westinghouse was asked to provide better documentation to identify each flooding area and flooding boundary credited in the flooding PRA. Westinghouse provided this information in the revised PRA and the identification of flooding areas and boundaries is now clear. This is acceptable; therefore, this open item is resolved.

Open Item 19.1.3.2-16: Westinghouse was asked to consider all flooding areas that contain safe-shutdown equipment in the flooding PRA. This was done in the revised flooding PRA and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-17: In the pre-DSER PRA, Westinghouse had reported a flood-induced initiating events frequency for each flooding area without proper explanation of how such frequencies where estimated. The staff asked Westinghouse to document in the PRA how the flooding initiating event frequencies for each flooding area were estimated. Westinghouse provided this information in the revised PRA and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-18: Westinghouse was asked to list all human actions that were credited in the flooding PRA. This information was included in the revised PRA and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-19: Westinghouse was asked to include a list of the dominant flood-induced minimal cutsets in the PRA. The revised PRA includes this information and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-20: Westinghouse was asked to provide more detailed information regarding the risk dominant flooding scenarios identified by the PRA. The revised PRA included this information and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-21: Westinghouse was asked to assess the flood-induced CDF assuming all non-safety systems have failed (focused PRA). The revised PRA included this information and the staff's review found it acceptable. This open item is resolved.

Open Item 19.1.3.2-22: Westinghouse was asked to perform sensitivity, uncertainty, and importance analyses, as appropriate, in order to identify leading contributors to flooding risk and gain insights about the capability of the AP600 design to mitigate flood-induced accidents. Westinghouse included these analyses in the revised PRA and the staff's review found them acceptable. This open item is resolved.

Open Item 19.1.3.3-1 The staff requested Westinghouse to justify the low human error rate for inadvertent draining of the reactor coolant system through the Normal RHR system. In response, Westinghouse documented in the SSAR (Section 5.4.7.1) the many design features that reduce the probability of overdraining the RCS resulting in a loss of RNS. Section 54.2.6 of the AP600 Shutdown PRA and the "Shutdown Evaluation Report" (WCAP-14837) also discuss these features. Westinghouse also evaluated potential RCS drain paths in section 54.2.4 of the Shutdown PRA. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3-2 The staff requested Westinghouse to quantitatively evaluate safe shutdown operations when the RCS temperature is greater than 350F and RNS is not in service (a subset of Mode 4 operation). Westinghouse responded that the plant response to a loss of core cooling event (including LOCAs) is the same as during power operation, since the safety-related and non-safety-related systems and actuation signals, both automatic and manual are required to be operable by AP600 TS (except Accumulators that are isolated when RCS pressure < 1000 psig). Westinghouse expects the CDF contribution from events during these safe shutdowns, when RNS is not in service, to be insignificant compared with at-power conditions, for the following three reasons: Compared with at power conditions, (1) decay heat is less, (2) there is additional time for operator intervention, and (3) this cooldown period is expected to be very short. Westinghouse also provided a table in the shutdown PRA documenting the TS requirement for the safety-related systems in all modes of operation. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3.-3 The staff requested Westinghouse to quantitatively assess overdraining events occurring during mid-loop/vessel flange operation using a separate event tree to illustrate systems and human interactions. In response, Westinghouse evaluated overdraining of the RCS during mid-loop/vessel flange operations in a separate event tree and incorporated

the results in the shutdown CDF estimate. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3-4 The staff requested Westinghouse to document in the PRA the functions of PMS, DAS, and DIS during safe shutdown, cold shutdown, and mid-loop/vessel flange operation. The staff also requested Westinghouse to discuss what instrumentation is operable in these modes and the availability of automatic injection. In response, Westinghouse provided Table 54-2 in the shutdown PRA that clearly delineates the systems availability and their associated actuation signals (manual and automatic) for all modes of operation. Section 54.2.5 of the shutdown PRA provides more detail on how these actuation signals were modeled in the shutdown PRA. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3-5 The staff requested Westinghouse to develop separate event trees for loss of normal RHR and LOOP during safe/cold shutdown and mid-loop/vessel flange operation. In response, Westinghouse developed and quantified these event trees and incorporated the results in the shutdown CDF estimate. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3-6 The staff requested Westinghouse to include maintenance unavailabilities in the shutdown PRA quantification and to document all maintenance assumptions in the shutdown PRA. In response, Westinghouse documented the maintenance unavailability assumptions by system in Table 54-8 of the PRA and in section 54A.1 of the PRA. Table 54-8 provides cross references to the AP600 TS and the Reliability Assurance Program where applicable. In addition, Westinghouse performed a separate sensitivity study (results discussed in 19.1.4.5) that evaluated the risk impact assuming a COL applicant only maintained systems available if they were required to be operable by TS. This sensitivity study provides an upper bound of the shutdown CDF assuming the COL applicant chooses to perform planned maintenance on a IRWST drain path, two 4th stage ADS valves, RNS valve V-23 during cold shutdown, and one out of two containment sump recirculation. The staff finds Westinghouse's response acceptable and, therefore, this open item is resolved.

Open Item 19.1.3.3-7 The staff requested Westinghouse to justify the mission time for hot/cold shutdown and mid-loop/vessel flange operation. In response, Westinghouse documented the mission times in Section 54.3.2 of the shutdown PRA. These mission times appear reasonable for a representative 35 day refueling outage for an operating PWR and are therefore acceptable. This open item is resolved.

Open Item 19.1.3.3-8 The staff requested Westinghouse to report the dominant shutdown sequences and cutsets, assuming no safety-related systems are available, including DAS and DIS. In response, Westinghouse provided the dominant shutdown sequences and cutsets, assuming no safety-related systems are available (including DAS and DIS) in Chapter 54 of the AP600 PRA, Attachment 54A, and Attachment Chapter 54B. The staff finds Westinghouse's response acceptable and , therefore, this open item is resolved.

## 19.2 Severe Accident Performance

### 19.2.1 Introduction

The purpose of Section 19.2 is to evaluate the approach proposed by Westinghouse for resolving severe accident issues for the AP600 design and determine whether the criteria in SECY-93-087, SECY-96-128, SECY-97-044 and the corresponding SRMs dated July 21, 1993, January 15, 1997, June 30, 1997, respectively, have been met.

To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and, if accidents should occur, to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, the NRC, State, and local governments mandate emergency response capabilities to provide additional defense-in-depth protection to the surrounding population.

The reactor and containment systems design are a vital link in the defense-in-depth philosophy. Current reactors and containments are designed to withstand a LOCA and to comply with the siting criteria of 10 CFR Part 100 and general design criteria of Appendix A to 10 CFR Part 50. The large-break LOCA and other accidents analyzed in accordance with the NRC's SRP are documented in Chapters 6 and 15 of the AP600 SSAR.

The high-level of confidence in the defense-in-depth approach results, in part, from stringent requirements for meeting the single failure criterion, redundancy, diversity, quality assurance, and utilization of conservative models. The staff concludes that existing requirements ensure a safe containment design.

The NRC also has requirements to address conditions beyond the traditional design-basis spectrum, such as anticipated transients without scram (10 CFR 50.62), station blackout (10 CFR 50.63), and combustible gas control (10 CFR 50.44); however, a definitive set of regulatory requirements for addressing specific severe accident phenomena does not exist. Existing regulations that require conservative analyses and inclusion of features for design-basis events provide margin for severe accident challenges. This design-basis margin coupled with regulatory guidance to address severe accidents in the form of policy positions ensures a robust design that satisfies the Commission's policy statement on severe accidents.

### 19.2.2 Deterministic Assessment of Severe Accident Prevention

#### 19.2.2.1 Severe Accident Preventive Features

The design of the AP600 copes with plant transients and LOCAs without any adverse impact on the environment. However, the potential does exist, albeit remote, for a LOCA or seemingly ordinary plant transient coupled with numerous plant failures to progress to a severe accident with the potential for substantial offsite releases.

Accident initiators separate into two general groups — transients and LOCAs. Transients include planned reactor shutdowns and transients that result in reactor scrams. Examples of transients are manual shutdown, steamline or feedline break, loss of offsite power, and loss of

feedwater. In addition to these transients, there is an entire spectrum of LOCAs that are accident initiators. LOCAs fall into three categories: small, medium, and large, dependent on the size of the line break.

Following the accident initiator, normal and emergency plant systems respond to control reactivity, reactor pressure, reactor water level, steam generator water level, and containment parameters within the design-bases spectrum. Of most importance is to ensure inventory control and sufficient heat removal from the core to prevent overheating and subsequent fuel damage. Failure to provide heat removal or inventory control results in core uncovery, fuel overheating, and the potential for oxidation and melting of the reactor core.

In response to accident initiators identified through operating reactor experience and performance of probabilistic risk assessments, the NRC developed criteria for advanced light water reactors (ALWRs) to prevent the occurrence of such initiators from leading to a severe accident. In SECY-93-087 the staff specifies these criteria and include design provisions for the following: anticipated transients without scram, mid-loop operation, station blackout, fires, and intersystem loss-of-coolant accidents.

19.2.2.1.1 Anticipated Transients Without Scram

An ATWS is an anticipated operational occurrence followed by the failure of the trip portion of the reactor protection system (RPS). Anticipated operational occurrences are those conditions of normal operation that are expected to occur one or more times during the life of the nuclear power plant and include, but are not limited to, loss of power to reactor coolant pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power. Depending on the transient and its severity, the plant may recover and continue normal operation, or the plant may require an automatic shutdown (scram) via the RPS. The RPS is designed to safely shut down the reactor to prevent core damage.

These transients, when coupled with a failure of the RPS, may lead to conditions beyond what some plants were originally designed to meet. In these cases, the reactor must be manually scrammed in order to avoid reactor fuel damage or coolant system damage. Subsequent failure of the manual scram system and inadequate core cooling would lead to core damage.

Transients with the greatest potential for significant damage to the reactor core and containment are those that lead to an increase in reactor pressure and temperature, a loss of feedwater, or a failure of the RPS to scram the reactor. During an ATWS event, reactor power, pressure, and temperature must be controlled or the potential exists for a severe accident.

In SECY-93-087, the staff indicated that it was evaluating the passive designs to ensure compliance with Commission regulations and guidance regarding ATWS. Regulations to address ATWS were promulgated in 10 CFR 50.62. The Commission issued further guidance in its SRM of June 26, 1990, which stated that diverse scram systems should be provided. However, the Commission also directed that the staff should accept an applicant's alternative to the diverse scram system, if the applicant can demonstrate that the consequences of an ATWS are acceptable.

As described in Section 7.7.1.11 of the SSAR, the AP600 has a diverse actuation system (DAS). The staff's evaluation of the DAS to meet the requirements of 10 CFR 50.62 is contained in Sections 7.7.2 and 15.2.7 of this report. On the basis of the staff's evaluation of the DAS to meet the requirements 10 CFR 50.62, the staff concludes that the AP600 design conforms to the ATWS criteria specified in SECY-93-087 and DSER Open Item 19.2.2.1-1 is resolved.

19.2.2.1.2 *Mid-Loop Operation*

During refueling or maintenance activities, the reactor coolant system is sometimes reduced to a "mid-loop" level. During this period, the potential exists for loss of decay heat removal capability as a result of air entrainment of the RHR pumps. In SECY-93-087, the staff indicates that all passive plants must have a reliable means of maintaining decay heat removal capability during all phases of shutdown activities, including refueling and maintenance. Westinghouse summarizes the specific AP600 design features that address mid-loop operations in Section 5.4.7.2.1 of the SSAR. Availability controls for the RNS during mid-loop operations have been provided in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the SSAR. On the basis of the staff's evaluation in Section 5.4.7.10, "Shutdown Operation Risk," and Section 5.4.7.11, "Regulatory Treatment of the RNS," of this report and the additional availability controls provided for the RNS during normal and reduced inventory in Table 16.3-2 of the SSAR, the staff concludes that the AP600 design conforms to the mid-loop operation criteria specified in SECY-93-087. This resolves DSER Open Item 19.2.2.1-2.

19.2.2.1.3 Station Blackout

An SBO involves the complete loss of alternating current (ac) electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., a LOOP concurrent with turbine trip and unavailability of the onsite emergency ac power system). An SBO does not include the loss of available ac power to buses fed by station batteries through inverters or by alternate ac sources, nor does it assume a concurrent single failure or DBA.

In accordance with SECY-90-016, the evolutionary designs provided a large-capacity, alternate ac power source with the capability to power one complete set of normal safe-shutdown loads. However, the AP600 does not rely on active systems for safe shutdown following an event. The AP600 design has redundant non-safety-related onsite ac power sources (diesel generators) to provide electrical power for the non-safety-related active systems that provide defense-in-depth. In SECY-93-087, which expanded on the guidance given in SECY-90-016, the staff indicated that it believed that the diesel generators might require some regulatory treatment.

The staff outlined the process for resolving the regulatory treatment of non-safety systems in Commission Policy paper SECY-94-084, dated March 28, 1994. This process includes a combination of probabilistic and deterministic criteria to identify risk-significant, non-safety-related systems. The staff evaluated non-safety-related ac power sources relative to these criteria in Section 8.6.2.4 of this report. Additional availability controls have been provided for the electrical power systems in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the SSAR. On the basis of the staff's evaluation in Section 8.6.2.1, "Station Blackout," of this report and the additional availability controls provided in Table 16.3-2 of the SSAR, the staff concludes that the AP600 design conforms to the station blackout criteria

specified in SECY-93-087, and is therefore, acceptable. This resolves DSER Open Item 19.2.2.1-3.

19.2.2.1.4 Fire Protection

The Commission concluded that fire protection issues that have been raised through operating experience and the External Events Program must be resolved for passive LWRs. In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed against the enhanced fire protection criteria specified for evolutionary designs in SECY-90-016. The Commission, in an SRM dated June 26, 1990, subsequently approved this position. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants and asked to be kept informed of the staff's resolution of the issue related to common-mode failures through common ventilation systems. A description of the AP600's fire protection system is in Section 9.5.1 of the SSAR and the fire protection analysis is contained in Appendix 9A of the SSAR. The staff's acceptance of the AP600 fire protection systems relative to the criteria in SECY-93-087 is discussed in Section 9.5.1 of this report. As discussed in that section, one issue remains as an open item concerning the location of the fire pumps. However, this issue is subsumed into FSER Open Item 9.5.1-1. This DSER Open Item 19.2.2.1-4 is closed.

19.2.2.1.5 Intersystem Loss-of-Coolant Accident

Intersystem LOCAs (ISLOCAs) are defined as a class of LOCAs in which a breach occurs in the interface of the RCS pressure boundary with a system of lower design pressure. The breach may occur in portions of piping located outside of the primary containment, causing a direct and potentially unisolable discharge from the RCS to the environment. An ISLOCA is of concern because of potential direct releases to the environment, loss of core cooling, and loss of core makeup. An ISLOCA occurs when high pressure is introduced to a low-pressure system as the result of valve(s) failure or an inadvertent valve actuation. In either case, the overpressurization can cause the low-pressure system or components to fail.

In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed for compliance with the ISLOCA criteria approved in the Commission's SRM of June 26, 1990, relating to SECY-90-016. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants.

In SECY-90-016, the staff recommended that designs reduce the possibility of a LOCA outside containment by designing (to the extent practicable) all systems and subsystems connected to the RCS to an ultimate rupture strength (URS) at least equal to the full RCS pressure. The "extent practicable" phrase is a realization that all systems must eventually interface with atmospheric pressure and that for certain large tanks and heat exchangers, it would be difficult or prohibitively expensive to design such systems to a URS equal to full RCS pressure. The staff further recommended that systems that have not been designed to withstand full RCS pressure should include the following attributes: (a) the capability for leak testing of the pressure isolation valves, (b) valve position indication that is available in the control room when isolation valve operators are de-energized, and (c) high-pressure alarms to warn control room

operators when rising reactor coolant pressure approaches the design pressure of attached low-pressure systems and both isolation valves are not closed.

The staff evaluated ISLOCA, relative to the criteria of SECY-93-087, as part of its resolution of Generic Safety Issue 105 in Section 20.3 of this report. On the basis of the staff's resolution of Generic Safety Issue 105, the staff concludes that the AP600 design conforms to the ISLOCA criteria specified in SECY-93-087, and is therefore, acceptable. On the basis of this evaluation DSER Open Item 19.2.2.1-5 is resolved.

19.2.3 Deterministic Assessment of Severe Accident Mitigation

19.2.3.1 Overview of the AP600 Containment Design

The AP600 primary containment design is a freestanding cylindrical steel vessel with ellipsoidal upper and lower heads. The steel vessel is 4 cm (1.625 in.) thick and has a design pressure of 310 kPa (45 psig). The vessel has an inner diameter of 40 m (130 ft) and net free volume of 48,100 $m^3$ (1,700,000 $ft^3$). The design basis leak rate is 0.10 weight percent per day of the containment air mass at the DBA peak pressure. A seismic Category 1 reinforced concrete shield building surrounds the containment.

The design provides passive containment cooling in case the normal containment fan coolers are not available or an accident has occurred that requires containment heat removal at elevated pressures and temperatures. The passive containment cooling system (PCCS) is a safety-related system that removes heat directly from the containment vessel and transmits it to the environment. The PCCS uses the steel containment vessel as a heat transfer surface. The surrounding concrete shield building is used, along with a baffle, to direct air from the top-located air inlets down to a lower elevation of the containment and back up along the containment vessel. A 1,510 $m^3$ (400,000 gallon) water storage tank is supported by the shield building to allow gravity drain of the water on the top of the steel containment vessel. Indications of inadequate containment cooling, such as high containment pressure or temperature, automatically initiate the PCCS water flow. These signals open valves to initiate the flow of water onto the top of the containment vessel. The air and the evaporated water exhaust through an opening in the roof of the shield building.

19.2.3.2 Severe Accident Progression

A description of the processes, both physical and chemical, that may occur during the progression of a severe accident, and how these phenomena affect containment performance, follows in this section. The intent of this description is to be generic in nature; however, many aspects of severe accident phenomena depend on the specific reactor type or on the containment design features. This information has been extracted from NUREG/CR-5132, NUREG/CR-5597, and NUREG/CR-5564.

Division of severe accident progression can be into two phases, an in-vessel stage and an ex-vessel stage. The in-vessel stage generally begins with insufficient decay heat removal and can lead to melt-through of the reactor vessel. The ex-vessel stage involves the release of the core debris from the reactor vessel into the containment, which results in phenomena such as core-concrete interaction, fuel-coolant interaction, and direct containment heating.

19.2.3.2.1 In-Vessel Melt Progression

In severe accidents that proceed to vessel failure and release of molten core material into the containment, the in-vessel melt progression establishes the initial conditions for assessing the thermal and mechanical loads that may ultimately threaten the integrity of the containment. In-vessel melt progression encompasses the phenomena and processes involved in a severe core- damage accident starting with core uncovery and initial heatup, and continuing until either of the following occurs: (a) stabilization and cooling of the degraded core within the reactor vessel, or (b) breach of the reactor vessel occurs and molten core material is released into the containment. The phenomena and processes in the AP600 that can occur during in-vessel melt progression include:

- core heatup resulting from loss of adequate cooling
- metal-water reaction and cladding oxidation
- eutectic interactions between core materials
- melting and relocating cladding, structural materials, and fuel
- formation of blockages near the bottom of the core as a result of the solidification of relocating molten materials (wet core scenario)
- drainage of molten materials to the vessel lower head region (dry core scenario)
- formation of melt pool, natural circulation heat transfer, crust formation, and crust failure (wet core scenario), and
- reactor vessel breach from a local failure or global creep-rupture.

Removal of decay heat produced by the core must take place in order to achieve adequate core cooling. In the event that all of the safety-related and non-safety-related systems fail to remove the decay heat, the core will heat up to the point at which damage to the fuel and fuel cladding may occur. Transfer of decay heat is through the radiative, conductive, and convective heat transfer to the steam, other core materials, and non-fuel materials within the reactor. The insufficient cooling supply results in coolant boiloff and a decreasing level within the reactor vessel as the decay heat generation exceeds the heat removal rate. The coolant level within the core further decreases so that the fuel rods above the coolant level cool only by rising steam. The fuel rods begin to overheat and cladding oxidation in the presence of steam begins at high temperatures. Generation of hydrogen and additional heat occurs as the cladding oxidizes in the presence of steam. A zirconium alloy called Zircaloy makes up the fuel cladding. The initial Zircaloy oxidation involves oxygen diffusion through a $ZrO_2$ surface layer. As the fuel rods continue to heat up from decay heat and the exothermic zirconium oxidation reaction occurs, the expectation is that materials within the reactor with low melting points will melt first and may form eutectics. Eutectics are mixtures of materials with a melting point lower than that of any other combination of the same components.

Zircaloy, with a melting point of 1,757 °C (3,194 °F), begins to melt, breaking down the protective $ZrO_2$ layer, which exposes unoxidized Zircaloy. Following this, local melting of the fuel rods may cause changes in the core geometry resulting in differing steam flow paths. This can lead, on the one hand, to an increase in the oxidation process as access to the unoxidized Zircaloy becomes available; on the other hand, the melt formation or changes in the steam flow path could reduce the Zircaloy surface available for oxidation and thereby decrease the overall reaction process. In some accident scenarios in which residual amounts of water remain in the bottom of the core and lower plenum, substantial steaming and oxidation can take place.

In addition to oxidation, the potential exists for the Zircaloy to interact with the $UO_2$ fuel, forming low-melting-point eutectics. Formation of eutectics may decrease the effective surface area for oxidation and the overall oxidation rate. The melting point of Zircaloy depends on its state and lattice structure. Zircaloy has three melting points: 1,877 °C (3,410 °F) (beta-Zr), 1,977 °C (3,590 °F) (alpha-Zr(O)), and 2,677 °C (4,850 °F) ($ZrO_2$). When partially oxidized Zircaloy is in contact with $UO_2$, an alpha-Zr(O)/$UO_2$-based eutectic will form with a liquefaction temperature of approximately 1,897 °C (3,446 °F). Therefore, in the presence of good fuel/cladding contact, fuel liquefaction and melt relocation will commence around this temperature. This has the potential to affect the oxidation behavior of Zircaloy-based melt.

Various severe fuel damage (SFD) test programs sponsored by the NRC indicate that the oxidation of the Zircaloy is largely controlled by the availability of a steam supply and that high rates of hydrogen generation can continue after melt formation and relocation. Some of these experiments indicate that the majority of the hydrogen generation occurred after onset of Zircaloy melting and fuel dissolution. In steam-rich experiments, oxidation took place over most of the fuel bundle length and most of the hydrogen generation occurred early. For steam-starved experiments, oxidation was limited to local regions of the fuel bundle, and the majority of the hydrogen generation occurs after the onset of Zr/$UO_2$ liquefaction and relocation.

Hydrogen production and accumulation may represent challenges to the containment in numerous ways, including deflagration, detonation, and pressurization, as hydrogen gas is non-condensible. The AP600 containment has 64 hydrogen igniters to consume hydrogen as it is produced during a severe accident.

The SFD tests indicated the potential for incoherent melt-relocation as a result of non-coherent temperatures within the test bundles. This is because of the different core materials present with a wide range of melting points and eutectic temperatures. Formation of eutectics would result in a nonuniform melting and relocation process. Further differences in the melt-relocation process can be attributed to asymmetric bundle heating that can increase upon Zircaloy oxidation. This process begins when one area of the fuel bundle is initially at a temperature higher than the other areas. The higher temperature Zircaloy will consume the available steam through oxidation at a quicker rate. The oxidation reaction increases the hotter areas to even higher temperatures, which further increases the oxidation rate and the local temperatures. This autocatalytic nature of Zircaloy oxidation appears to contribute to asymmetric bundle heatup and the potential for incoherent melt relocation behavior.

As the temperature of the core increases, vaporization and release of some fission products occur. Steam and/or hydrogen then carry these fission products throughout the primary system where they are subject to deposition on the surfaces of internal components. The deposition mechanisms include condensation, gravitational settling, and thermophoresis. The fission

products that are not deposited remain airborne and are released to the containment, where the dominant removal mechanisms are gravitational settling and diffusiophoresis.

The core melt progression, including relocation and fission product release, becomes increasingly difficult to predict as it continues to degrade. The core melt could relocate into the lower reactor vessel plenum. If water is present in the lower plenum, the potential exists for in-vessel steam explosions, where molten core rapidly fragments and transfers its energy, causing rapid steam generation and shock waves. Once in the lower plenum, the potential exists to halt the core melt progression through external vessel cooling. The AP600 is designed to flood up the reactor cavity with water from the IRWST, thereby providing cooling of the core debris through the reactor vessel.

The in-vessel core melt progression, including core degradation, relocation, and failure of the reactor vessel, contains considerable uncertainty. This uncertainty includes the following:

- the potential for in-vessel steam explosion (see Section 19.2.3.3.5.1 of this report)
- the interaction between core debris and internal vessel structures
- the potential for external vessel cooling of core debris (see Section 19.2.3.3.1 of this report)
- the time and mode of vessel failure
- the composition of the core debris released at vessel failure
- the amount of in-vessel hydrogen generation
- the in-vessel fission-product release and transport, and
- retention of fission products and other core materials in the RCS.

19.2.3.2.2 Ex-Vessel Melt Progression

The following conditions affect ex-vessel severe accident progression:

- the mode and timing of the reactor vessel failure
- the primary system pressure at reactor vessel failure
- the composition, amount, and character of the molten core debris expelled
- the type of concrete used in containment construction,
- the availability of water to the reactor cavity

The initial response of the containment from ex-vessel severe accident progression is largely a function of the pressure of the RCS at reactor vessel failure and the existence of water within the reactor cavity. If not prevented by design features, early containment failure mechanisms and bypass usually dominate risk consequences. Early containment failure mechanisms result from energetic severe accident phenomena, such as high pressure melt ejection with direct containment heating and ex-vessel steam explosions. The long-term containment pressure and

temperature response from ex-vessel severe accident progression is largely a function of CCI and the availability of mechanisms to remove heat from the containment.

At high RCS pressures, ejection of the molten core debris from the reactor vessel could occur in jet form, causing fragmentation into small particles. The potential exists for the core debris ejected from the vessel to be swept out of the reactor cavity and into the upper containment. Finely fragmented and dispersed core debris could heat the containment atmosphere and lead to large pressure spikes. In addition, chemical reactions of the core debris particulate with oxygen and steam could add to the pressurization loads. Hydrogen, pre-existing in the containment or produced during direct containment heating, could ignite adding to the loads on the containment. This phenomena is known as high pressure melt ejection with direct containment heating.

Reactor vessel failure at high or low pressure coincident with water present within the reactor cavity may lead to interactions between fuel and coolant with the potential for rapid steam generation or steam explosions. Rapid steam generation involves the pressurization of containment compartments from nonexplosive steam generation beyond the capability of the containment to relieve the pressure so that the containment fails because of local overpressurization. Steam explosions involve the rapid mixing of finely fragmented core debris with surrounding water resulting in rapid vaporization and acceleration of surrounding water creating substantial pressure and impact loads.

The eventual contact of molten core debris with concrete in the reactor cavity will lead to CCI. CCI involves the decomposition of concrete from core debris and can challenge the containment by various mechanisms, including the following: (a) pressurization as a result of the production of steam and noncondensible gases to the point of containment rupture, (b) the transport of high-temperature gases and aerosols into the containment leading to high-temperature failure of the containment seals and penetrations, (c) containment liner melt-through, (d) reactor support structures melt-through leading to the relocation of the reactor vessel and tearing of containment penetrations, and (e) the production of combustible gases such as hydrogen and carbon monoxide. CCI is affected by many factors, including the availability of water to the reactor cavity, the containment geometry, the composition and amount of core debris, the core debris superheat, and the type of concrete involved.

19.2.3.3 Severe Accident Mitigative Features

19.2.3.3.1 External Reactor Vessel Cooling

The AP600 design incorporates ERVC as a strategy for retaining molten core debris in-vessel in severe accidents. The objective of ERVC is to remove sufficient heat from the vessel exterior surface that the thermal and structural loads on the vessel (from the core debris which has relocated to the lower head) do not lead to failure of the vessel. By maintaining RPV integrity, the potential for large releases due to ex-vessel severe accident phenomena, i.e., ex-vessel FCIs and CCI, is eliminated. A residual threat from hydrogen combustion remains, but diminishes with successful ERVC since combustible gas production would be limited to in-vessel hydrogen generation. ERVC will remove some decay heat through the RPV in design basis LOCAs (which result in a flooded reactor cavity as a direct consequence of the sequence), but in the absence of loss of core cooling and core debris relocation, this heat removal is insignificant and is not credited in design-basis accidents.

The staff identified a number of technical issues associated with ERVC in the DSER and in SECY-95-172. The resolution of related issues was identified as DSER Open Item 19.2.3.3-1. This section provides the results of the staff's review of the ERVC strategy for the AP600 and resolution of the open item.

Background

The AP600 design includes several features that enhance ERVC relative to operating plants, specifically: (1) safety-grade systems to provide RCS depressurization and reactor cavity flooding, (2) a lower power density core relative to operating plants, (3) a "clean" lower head that is unobstructed by in-core instrument lines or other penetrations, and (4) a RPV thermal insulation system which limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents. The AP600 design further enhances the ability to flood the reactor cavity by a containment and reactor cavity arrangement which permits the RCS inventory (breakflow) to drain to the cavity, in addition to the manually-actuated cavity flooding system.

ERVC is credited with preventing RPV failure in the AP600 PRA on the basis of a DOE-sponsored analysis by the University of California, Santa Barbara (UCSB) using the Risk Oriented Accident Analysis Methodology (ROAAM). The UCSB analysis of ERVC, documented in DOE/ID-10460, "In-Vessel Coolability and Retention of a Core Melt", July 1995 (Peer Re-Review Version) and October 1996 (Final), concluded that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the RPV is submerged in water to a depth of at least the top of the debris pool. On this basis, sequences with successful RCS depressurization and reactor cavity flooding are assigned zero probability of vessel breach, and sequences with either inadequate RCS depressurization or reactor cavity flooding are assumed to fail the reactor vessel and containment in the AP600 PRA.

Staff review of ERVC centered on 3 major areas including: (1) the likelihood of achieving RCS depressurization and reactor cavity flooding in the AP600 design, both of which are required for successful ERVC, (2) the likelihood of maintaining RPV integrity given successful RCS depressurization and reactor cavity flooding, and (3) system-related considerations and design requirements for the cavity flooding system and the RPV thermal insulation system. The results of the review are provided below.

19.2.3.3.1.1 Likelihood of Achieving Requisite Conditions for ERVC in AP600

Both RCS depressurization and reactor cavity flooding are required for successful ERVC. Important considerations include the manner in which these conditions are defined in the PRA success criteria, the potential for the RCS to be depressurized automatically or by manual backup of ADS, and the potential for reactor cavity to be flooded passively by gravity draining or by manual actuation of the cavity flooding system.

The AP600 PRA defines the success criteria for ERVC as: (1) depressurization of the RCS to below 150 psi before RCS pressure boundary challenge, and (2) flooding of the reactor cavity to an elevation above the hemispherical lower head (83 ft elevation) before initial relocation of

core debris to the lower head, and above the maximum debris pool elevation (86 ft elevation) before slumping of the remainder of the core into the lower head. Each of these criterion is discussed below.

RCS Depressurization

RCS depressurization can occur as a result of the initiating event (e.g., a large LOCA), or operation of the safety-grade ADS. In the event that automatic actuation of the ADS does not occur, manual actuation is addressed in Emergency Response Guidelines and credited in the PRA. In the Level 1 PRA, the majority of Level 1 sequences (about 85 percent) involve events with at least partially successful RCS depressurization and relatively low RCS pressure (<150 psig) at the time of core uncovery. For high pressure core melt sequences, the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary is further evaluated in the Level 2 event trees. After credit for late depressurization, an even larger fraction of the core melt sequences (about 93 percent) are estimated to involve a depressurized RCS before the time of substantial core damage.

The RCS pressure associated with successful ERVC in the PRA (i.e., 150 psig or less) is greater than the RCS pressure assumed in the baseline analysis in the UCSB study (the UCSB study assumed a fully depressurized RCS). However, a supplemental structural analysis is provided in Appendix G of the UCSB report which illustrates that there is margin in the load carrying capacity of a thinned RPV (with 5 cm wall thickness) at an elevated pressure of 400 psig. The supplemental analysis considers the effect of vessel creep under high temperature and elevated pressure, and concludes that there is margin in the load carrying capacity of the vessel shell. Thus, the success criterion for RCS pressure is bounded by the UCSB analysis, and is therefore, acceptable.

Reactor Cavity Flooding

On the basis of an assessment of the timing of core debris relocation and associated uncertainties, Westinghouse estimated that initial debris relocation to the lower head would not occur until at least 45 minutes after initiation of rapid oxidation in the core, and full relocation would not occur until at least 75 minutes after initiation of rapid oxidation. Thus, the success criteria are as follows: (1) cavity water elevation greater than 83 ft within 45 minutes of rapid cladding oxidation, and (2) cavity water elevation greater than 86 ft within 75 minutes of rapid cladding oxidation. Successful IRWST injection is necessary to meet the latter criterion because CMT and accumulator water inventories alone are not adequate to achieve the necessary water level. Accordingly, the long-term reactor cavity water level corresponding to successful ERVC in the PRA is approximately 107 ft, which completely covers the RPV hot leg and cold legs. This final level is consistent with the containment water level simulated in tests performed by the University of California in the ULPU facility, which form the basis for the exterior heat transfer coefficients employed in the UCSB analysis.

An assessment of reactor cavity flooding rates presented in Chapter 39 of the PRA indicates that with one line open, the 83 ft elevation is reached within 20 minutes of opening the valves and the 86 ft elevation is reached within 40 minutes, assuming no credit for water accumulated in the reactor cavity before operator action. Thus, in the most limiting scenario the operator has about 25 minutes to open the cavity flood valves after rapid core oxidation signals the need for cavity flooding within emergency response guideline FR.C-1. In the quantification of human

error rates in the PRA, only 20 minutes are credited. The PRA assigns a probability of 0.003 to failure to recognize the need to flood the reactor cavity and open the recirculation valves in 1 of 2 lines to flood the cavity within this 20 minute window. The PRA assumes this will result in reactor vessel failure.

The effectiveness of reactor cavity flooding was confirmed by MAAP calculations for selected sequences for each accident class in the PRA. These calculations, documented in Chapter 34 of the PRA, indicate that the cavity would be passively flooded before or at the time of onset of oxidation in many sequences, and that a margin of about 40 minutes typically exists for manually flooding the cavity in those sequences where manual flooding is necessary.

The staff performed limited calculations using the SCDAP/RELAP5 and MELCOR codes at different stages of the AP600 design evolution to confirm the general nature of core melt progression in the AP600. Although these calculations revealed some significant differences in predicted behavior, such as the quantity of hydrogen generated, the code comparisons confirm the order and approximate timing of major events in the accident progression, and the overall thermal hydraulic behavior during the accidents analyzed. Of particular note is the SCDAP/RELAP5 calculation for the frequency-dominant sequence that would require manual actions to flood the reactor cavity (the 3BE sequence). The SCDAP/RELAP5 calculation (Enclosure 2 of a letter to Westinghouse dated May 22, 1996) provides the most detailed assessment of core melt progression, and indicates that there would be approximately 90 minutes between the onset of rapid core oxidation and the first relocation of core debris into the lower head, and approximately 120 minutes between the time of rapid oxidation and the final debris relocation. These results confirm that there is substantial margin implicit in the Westinghouse success criterion for cavity flooding. In view of this confirmation, the staff concludes that the Westinghouse characterization of melt progression and the time available for manual actions, which forms the basis for assessing the likelihood of successful operator action in the PRA, is reasonable and acceptable.

In the baseline PRA, adequate reactor cavity flooding is achieved in about 96 percent of the sequences. About half of the core damage events require operator actuation of the cavity flooding system to ensure successful cavity flooding, but the remaining half would adequately flood as a direct consequence of the accident progression, even without manual actions. The availability of the power sources, availability of the valves, ability of the operator to diagnose the situation, and success of the operator are all considered in the fault tree used to quantify the failure probability of cavity flooding. Since the system fault trees are linked to the CET, the availability of power sources is treated consistently for all sequences in the CET.

In summary, the staff concludes that the success criteria for RCS depressurization and reactor cavity flooding is appropriate, and that the safety-related systems for RPV depressurization and reactor cavity flooding provide high confidence that the requisite conditions for ERVC, i.e., a depressurized RCS and timely flooding of the reactor cavity, will be achieved in most core melt sequences. In those events where either condition is not met, the sequence is conservatively assumed to lead to containment failure in the AP600 PRA. The staff therefore considers the PRA models and assumptions for estimating the likelihood of achieving the requisite conditions for ERVC, and the consequences of not achieving these conditions, to be acceptable.

19.2.3.3.1.2 Likelihood of Successful ERVC

The UCSB study evaluated two debris configurations or debris/vessel contact modes that were considered to bound the thermal loads from all other debris configurations that can reasonably be expected to occur in the time period between the initial relocation event and the final steady state where essentially the entire core debris is contained in the lower head. One configuration was dominated by transient forced convection and jet impingement effects, and the other was dominated by natural convection in the final steady state. Analyses described in the UCSB report show that vessel failure would not occur as a result of jet impingement. This is consistent with the staff's independent assessment of this threat. Thus, thermal loads to the vessel for the final steady state configuration were considered bounding and were analyzed in detail. Key aspects of the steady state configuration, termed the "Final Bounding State" or FIBS in the UCSB report, are: (1) fully-developed natural circulation in the lower head with a molten pool comprised of oxidic constituents on the bottom of the vessel and an overlying molten pool comprised of unoxidized metallic constituents, (2) debris pool masses corresponding to relocation of essentially all of the core and most of the steel structures, (3) a depressurized RCS, and (4) heat transfer coefficients on the outside of the reactor vessel corresponding to a fully-flooded reactor cavity.

The technical treatment in the UCSB study includes the following: (1) new experimental data and correlations from tests conducted specifically to address ERVC for the AP600 design, including work carried out by UCSB to investigate boiling and critical heat flux in inverted, curved geometries (the ULPU experiments) and heat transfer from volumetrically heated pools and non-heated layers on top (the mini-ACOPO and MELAD experiments, respectively), (2) a detailed computer model to sample limited input parameters over specified uncertainty ranges, and to produce probability distributions of thermal loads and margins to departure from nucleate boiling at each angular position on the lower head, and (3) detailed structural evaluations that indicate that departure from nucleate boiling, i.e., heat flux in excess of critical heat flux (CHF); is a necessary and sufficient criterion for reactor vessel failure. The UCSB study concludes that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the vessel is submerged in water to a depth at least to the top of the debris pool. Additional conditions on the applicability of the UCSB conclusions are that the as-built reactor vessel thermal insulation system and RPV exterior coatings are in accordance with the system design and surface coatings evaluated in the prototypical testing carried out in the ULPU Configuration III tests and described in Appendices K and E.4 of the UCSB report, and that the insulation maintains its integrity under thermal-hydraulic loads associated with ERVC. RPV pressure loads associated with late reflood of the reactor vessel were not addressed as part of the UCSB analysis of ERVC.

The UCSB report was peer-reviewed by 17 internationally recognized experts in the fields of severe accidents, heat transfer, and structural mechanics. The peer review process occurred over a 2-year period and involved two iterations with the authors. Numerous technical issues related to ERVC were identified and addressed as part of the peer review. These included the issues raised by the staff in the AP600 DSER and in SECY-95-172, as well as many additional technical concerns, such as transient thermal loads on the RPV before achieving the steady state configuration modeled in the UCSB study, applicability of and uncertainties in correlations for heat transfer within the molten debris pool and from the RPV to the surrounding water, estimated heat fluxes from the vessel relative to critical heat flux, and reactor vessel material properties and strength at elevated temperatures. The impact of these issues on the study

conclusions was addressed as part of the peer review comment resolution process by performing sensitivity studies and additional evaluations to address the impact of these issues on the margins to failure. The results of the further assessments indicated that even when these issues are taken into consideration, the margins to failure are significant, and failure of the lower head is "physically unreasonable".

To assist in the NRC's evaluation of ERVC, parallel review efforts were undertaken by the NRC Office of Research (RES) and the Idaho National Engineering and Environmental Laboratory (INEEL). The Office of Research performed an internal review of the UCSB study, focussing on the major factors that impact lower head integrity, including: (1) transient thermal loads from jet impingement, (2) decay heat level and power density in the core debris pool, (3) heat transfer coefficients within the oxidic and metallic regions of the molten pool, (4) thermal load distribution on the inner surface of the lower head, (5) critical heat flux (CHF) and heat removal from the outer surface of the vessel from ex-vessel flooding, and (6) mechanical loads on the lower head. The review also included performing transient calculations of core melt progression and lower head cooling for AP600 using a modified version of the SCDAP/RELAP5 code, and additional calculations of fission product decay heat levels using the ORIGEN2 code together with the core temperature history from the SCDAP/RELAP5 analysis.

In support of the RES review, SCDAP/RELAP5 calculations were performed by INEEL using an AP600-specific model developed to allow simulation of unique plant design features and detailed representation of heat transfer within the lower head (Enclosure 2 of a letter to Westinghouse dated May 22, 1996). The lower head region and RPV wall were represented by a finite element mesh consisting of approximately 500 nodes and elements. The molten core relocations predicted by the SCDAP/RELAP5 models were used as transient boundary conditions or inputs to the lower head model. Natural convection heat transfer at interfaces between the molten pool and adjacent materials (in the upward direction and in the downward direction as a function of angular position) was based on steady-state heat transfer correlations from available literature. Heat transfer from the RPV exterior surface to the surrounding water was determined by the correlations developed from the Pennsylvania State University Subscale Boundary Layer Boiling (SBLB) CHF experiments. For the configuration modeled, the results of these calculations indicate that ERVC is adequate to prevent failure of the RPV under expected heat transfer conditions, and that uncertainties associated with external boiling heat transfer, the potential for lower core support plate relocation, and debris/vessel contact resistance do not adversely impact the effectiveness of ERVC. The SCDAP/RELAP5 calculations assume that the molten debris pool in the lower head remains homogenous (i.e., a stratified metallic layer does not form), since there are no experimental data proving that density differences would cause the melt to segregate and form the "final bounding state" assumed in the UCSB study. The calculations also assume that no debris quenching occurs in the lower head during slumping, however, sensitivity calculations investigating the "no quench" assumption found that this assumption did not impact conclusions regarding vessel failure.

The RES review, which was enclosed in a letter to Westinghouse dated April 24, 1998, concluded that the UCSB study provides a comprehensive treatment of the concept of retaining

the degraded core in-vessel through external cooling of the vessel wall, but identified the following as areas of concern:

- The potential to form a "stratified intermediate state" before final relocation of melt to the lower head. On the basis of the sequence of core debris relocations predicted in the SCDAP/RELAP5 calculations, a stratified intermediate state, if formed, would result in a thinner metallic layer on top of the oxidic melt pool than the "final bounding state" evaluated in the UCSB study, and proportionally higher heat fluxes to the vessel wall. A higher volumetric power density in the oxidic pool was also predicted on the basis of the ORIGEN2 calculations for AP600, and would further increase the heat loads to the vessel. Additional analyses of intermediate states, considering earlier times of melt relocation and higher power densities in the molten pool, were recommended.

- The potential for an inversion of the metallic and oxidic layers, is based on work by D. Powers ("Chemical Phenomena and Fission Product Behavior During Core Debris/Concrete Interactions," Proceeding of the Committee on the Safety of Nuclear Installations (CSNI) Specialists Meeting on Core Debris-Concrete Interactions, EPRI NP-5054-SR, February 1987). The presence of about 5 atom percent uranium in the metal phase is sufficient to make the metallic layer more dense than the oxidic layer. This could result in an inversion of the layers, i.e., the metallic layer settling below the oxidic layer. Such a configuration would result in a different partitioning of the heat fluxes, and increased thermal loads on the bottom part of the vessel where heat removal capability (CHF) is at a minimum. Recent post-test examination of two RASPLAV tests with corium composed of 81.5 percent $UO_2$, 5 percent $ZrO_2$, and 13.5 percent Zr revealed that the heavy phase of the melt (uranium rich oxides) occupied the lower part of the corium melt close to the bottom of the simulated vessel, with the light phase of the melt (zirconium rich metals) on the top (see report entitled "Intermediate Report of RASPLAV AW-20-2 Post-Test Analysis", RP-TR-32, October 1997). Based on these two tests, the potential for inversion of the metallic and oxidic layers appears unlikely. As part of RASPLAV Phase II, additional integral and separate effect experiments are planned in 1998 to further explore melt vessel interaction and melt stratification.

- The possibility of chemical interactions between the melt and the RPV wall. Such interactions could lead to thinning of the vessel wall and reduced margins to failure. A separate effects experimental study planned as a part of the RASPLAV project was identified as a means of confirming whether such interactions are likely to occur. It should be noted that in a preliminary separate effects test, immersion of a cooled tungsten specimen resulted in formation of a corium crust on the tungsten surface, possibly indicating that extensive thinning of the vessel wall as a result of melt-vessel interactions is not likely (see RASPLAV Test Report).

INEEL was separately tasked by NRR to conduct a more detailed assessment of the UCSB study, building upon the results and insights from the RES review. Specifically, INEEL was tasked to perform the following reviews and analyses: (1) an in-depth review of the UCSB study and the model used to assess ERVC effectiveness, (2) an in-depth review of the peer review comments and their resolution to identify areas where technical concerns were not addressed, and (3) independent analyses to investigate the impact of residual concerns and parameter uncertainties on the margins to failure and conclusions presented in the UCSB report. The latter activity included performing steady-state analyses of the thermal loads associated with

alternate debris bed configurations, including stratified intermediate states and inverted metallic and oxidic layers.

In INEEL's evaluation, which can be found in an enclosure to a letter to Westinghouse dated January 7, 1998, INEEL noted that peer review comments were typically addressed by performing sensitivity studies in which a particular parameter was varied individually or in conjunction with a limited number of other parameters, and that these sensitivity studies generally involved point estimates rather than a requantification of the uncertainty/probabilistic model. Although this treatment provides insights about the impact of a change in the varied parameter, the sensitivity calculations do not reveal integral effects of the changes suggested by peer reviewers. Because integral effects may significantly impact estimated vessel failure margins, INEEL developed a code equivalent to the uncertainty/probabilistic model used in the UCSB study, with capabilities to address peer reviewer comments and additional parameter uncertainties in an integral manner. This model was then used by INEEL to determine the impact of residual technical concerns on the margins to failure. Major differences in the input used in the INEEL analyses for the "final bounding state" include: replacing the UCSB Mini-ACOPO molten pool natural convection heat transfer correlations with correlations derived from the larger scale ACOPO facility, replacing the UCSB ULPU CHF correlation with the Pennsylvania State University Subscale Boundary Layer Boiling (SBLB) CHF correlations, assuming appropriate uncertainties in heat transfer correlations and decay power curves, assuming a metallic layer heat source corresponding to the fraction of fission products expected to reside in the metallic layer, basing melt relocation times on severe accident analyses code predictions rather than the qualitative analyses performed in the UCSB study, and basing material properties and uncertainties on a wider range of published experimental data.

Applying this model to the "final bounding state" configuration defined in the UCSB study, INEEL found that heat fluxes from the vessel remained below CHF even when peer reviewer concerns and additional parameter uncertainties were explicitly addressed in the integral solution. Reactor vessel integrity would therefore be expected to be maintained in the long term, provided the "final bounding state" can be achieved without prior vessel failure. However, the INEEL analyses found that margins to CHF are smaller at certain vessel locations, and could be eroded as demonstrated in several sensitivity analyses. These sensitivity analyses explored the impact on the probability of exceeding CHF in the "final bounding state" configuration as a result of increased upward heat transfer because of quasi-steady state vapor generation and transport, additional metallic layer heat sources, and various reductions in the mass of the metallic layer. The results indicate that a factor of four reduction in the mass of steel in the metallic layer (from approximately 70,000 kg to 20,000 kg) causes the probability of exceeding CHF to rise above 0.5 at certain locations. Although these calculations are scoping in nature, the reduced metallic layer masses evaluated are not inconsistent with the inventory of metals predicted to exist in the lower head just before the final core debris relocation event in the SCDAP/RELAP5 calculation for AP600 discussed in INEEL's report (enclosure 2 of a letter to Westinghouse dated May 22, 1996) and in the Office of Research's report (enclosure of a letter to Westinghouse dated April 24, 1998) and are therefore, judged credible. As stated in the UCSB report, heat flux in excess of CHF is a necessary and sufficient criterion for reactor vessel failure. Thus, reactor vessel failure cannot be completely ruled out given the large uncertainties in core melt progression, and debris bed/molten pool behavior in the lower head.

INEEL also found that the "final bounding state" defined in the UCSB report does not necessarily bound all possible heat loads to the vessel. Steady-state calculations performed for several postulated alternate debris bed configurations indicate that heat fluxes can be higher than for the final bounding state and greater than CHF. Three configurations were analyzed as follows: (1) a stratified intermediate state similar to the configuration analyzed in the UCSB study but with a thinner overlying metallic layer (corresponding to the cumulative masses predicted to be relocated in SCDAP/RELAP5 just before the final relocation, and an assumption that the unoxidized metallic components segregate in a top layer), (2) an intermediate state in which a limited amount of relocated metallic melt is trapped or sandwiched between two oxidic pools, and (3) a configuration in which a metallic/oxidic layer inversion occurs, resulting in a more dense heat generating metallic layer (consisting of uranium dissolved in zirconium) settling to the bottom of the vessel where CHF is at a minimum. Each of these postulated configurations were found to result in heat fluxes greater than CHF. However, these analyses and findings are only valid if the postulated configurations form and persist for a sufficient time to approach steady-state. This was not established as part of the INEEL study.

Uncertainties in the likelihood of forming such debris bed configurations are largely the result of the inherent limitations in the modeling of core melt progression/relocation and lower head debris bed behavior. Detailed, transient modeling of lower head debris bed and molten pool behavior would be needed to assess whether such configurations are viable. These calculations would need to be dependent on realistic, validated models for debris quenching, debris bed reheating and remelting, and mixing and stratification of the newly formed molten pool. Such calculations are considered to be beyond current severe accident analysis capabilities, and results of any such calculations would be highly speculative and be subject to considerable uncertainties.

The staff concludes that reactor vessel integrity is likely to be maintained if the requisite conditions for ERVC are met, but in view of the potential for certain hypothetical debris configurations to produce heat fluxes exceeding CHF, the staff believes that RPV failure cannot be ruled out for all possible core melt scenarios. In the longer term, insights into debris pool behavior may be obtained from separate effects experiments currently planned as a part of the OECD RASPLAV project. This would include insights into the likelihood of layer inversions and alternative debris configurations, and the possibility of chemical interactions between the melt and the RPV wall. However, significant uncertainties in debris bed formation are likely to remain.

For purposes of design certification, the staff has accepted the Westinghouse characterization of ERVC in the AP600 PRA on the basis of the significant margins to vessel failure for the more likely debris bed configurations, in conjunction with results of probabilistic and deterministic analyses of the impact of vessel failure on containment integrity. The deterministic analyses for core concrete interactions and ex-vessel FCI, described in Sections 19.2.3.3.3 and 19.2.3.3.5.2 of this report, indicate that RPV failure and subsequent melt relocation is not expected to result in early containment failure. The probabilistic assessment discussed in Section 19.1.3.2.3 of this report illustrates that if credit for successful ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption of no credit for ERVC, the containment failure frequency would approach the core melt frequency given the pessimistic characterization of containment response to an RPV breach in the PRA. Even then, however, the containment failure frequency would remain below the Commission's large

release frequency goal of 1E-06/y because of the low estimated core damage frequency. The staff therefore concludes that the design of the AP600 for ERVC, and the assumption in the PRA that the reactor vessel will remain intact are acceptable.

19.2.3.3.1.3 System Considerations

Reactor Cavity Flooding System

The reactor cavity flooding system is comprised of two 15.2-cm (6-in.) diameter lines drawing from the IRWST at the Elevation-96' and discharging into the recirculation sumps at the Elevation-83' of containment. The water flows out of the recirculation sumps and eventually fills the floodable region of containment to the Elevation-107'. One motor-operated valve and one explosive valve is installed in each line. All valves are Class 1E and are powered by Class 1E dc power. The line sizing for the system is based on the design function of the lines which is to provide suction for the RNS pumps in the recirculation mode.

The containment recirculation squib valves and isolation MOVs, and the containment recirculation screens are included as risk significant SSCs within D-RAP. In-service inspection and testing programs provide surveillance and maintenance requirements on the related piping and valves. The operator action to flood the cavity is specified in ERG FR.C-1, which instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission product releases as determined by a core damage assessment guideline. The core exit thermocouples are used to monitor the need for cavity flooding within the inadequate core cooling (ICC) portion of the EOPs, and are also Class 1E and powered by Class 1E dc power. The staff therefore concludes that treatment of the reactor cavity flooding system in the SSAR and ITAAC is acceptable.

Reactor Pressure Vessel Thermal Insulation System

In addition to RCS depressurization and reactor cavity flooding, several conditions were identified in DOE/ID-10460 and PRA Chapter 39 that must also be met in order to conclude that reactor vessel failure is "physically unreasonable", specifically: (1) the reactor vessel thermal insulation system is constructed in accordance with the design description in Appendix K of the UCSB report (which forms the basis for the ULPU test facility scaling and heat transfer correlations), (2) the reactor vessel insulation system maintains its integrity under the hydrodynamic loads associated with ERVC, and is not subject to clogging of the coolant flow path by debris, and (3) RPV exterior coatings do not preclude the wetting phenomena identified as the cooling mechanism in the ULPU testing. Each of these areas is discussed below.

The RPV thermal insulation system is designed to limit thermal losses during normal operations, but provide an engineered pathway for supplying water cooling to the vessel and venting steam during severe accidents. The insulation system is described in SSAR Section 5.3.5, and Chapter 39 of the PRA. Water enters the insulation system through water inlets located below the RPV lower head. From there, it flows upward and outward along the spherical lower head of the RPV where significant boiling and steam production occurs. The escaping liquid/steam mixture flows into the annular gap between the cylindrical portion of the RPV and the curved insulation panels until the elevation of the steam vent dampers. It then passes through the baffles in the RPV support blocks, through the annular openings between

the RPV nozzles and the biological shield wall, and into the steam generator compartment. The coolant returns to the RCDT room via a grated opening between the vertical access tunnel and the RCDT room (approximately 100 $ft^2$ area), and enters the reactor cavity compartment through a passively-actuated damper installed in the doorway between the reactor cavity compartment and the RCDT room.

Key attributes of the reactor vessel insulation system include the following:

- the water inlets at the bottom of the insulation and steam vents near the top of the lower insulation segment both of which change position during flood-up of the reactor cavity
- specific RPV/insulation clearances and water/steam flow areas on which experimental facility scaling was based
- insulation panel and support members designed to withstand the hydrostatic and hydrodynamic loads associated with ERVC

The water inlet at the bottom of the insulation is sized so that the pressure drop through the inlet is negligible during the circulation of water associated with the in-vessel retention phenomena. The steam vents at the top of the biological shield wall have a flow area greater than or equal to the minimum flow area in the structures forming the circulation loop. The minimum flow area is 0.7 $m^2$ (7.5 $ft^2$). On the basis of results from the ULPU Configuration II tests (without insulation), Westinghouse estimates that the upper limit flow rate past the RPV would be approximately 37.85 kL/min (10,000 gpm) (see summary of August 17, 1995 meeting between Westinghouse and NRC regarding External Reactor Vessel Cooling for the AP600 Design, dated August 30, 1995). The damper between the reactor cavity compartment and the RCDT room is normally closed to prevent air from flowing into the RCDT room during normal operation, but is designed to open passively during containment floodup to permit water to flow from the RCDT room into the reactor cavity compartment. The damper opening has a minimum flow area of 0.74 $m^2$ (8 $ft^2$), and is constructed of light-weight material to minimize the force necessary to open the door.

Hydrostatic pressure loads on the reactor vessel insulation during the reactor cavity flood-up phase, and the hydrodynamic loads resulting from vapor generation and steam bubble collapse within the region between the insulation and RPV surface represent a potential challenge to the structural integrity of the insulation panels and supports. Westinghouse's assessment of these loads is provided in Chapter 39 of the PRA. The loads on the horizontal, transitional, and vertical insulation panels were determined for both the cavity flood-up and longer-term phases of the accident. The loads are time-dependent and elevation-dependent and oscillatory in nature. The hydrodynamic component of the loads was founded on interpretation of pressure histories measured in the ULPU Configuration III experiments for heat fluxes ranging from 280 $kW/m^2$ to 550 $kW/m^2$. Westinghouse characterized the loads from these heat fluxes as bounding since the area-averaged heat flux for the "final bounding state" configuration is estimated to be about 250 $kW/m^2$. The analysis assumed that the insulation is rigid, but also considered the effect that flexing of the insulation panels would have on the pressure loads and the movement of the steam vent dampers.

Westinghouse specified the following functional requirements in Chapter 39 of the PRA on the basis of the ULPU experiments and the associated insulation loading analysis:

- maximum pressure loads on the insulation panels would be approximately 6.6 ft of water (2.7 psi) in a direction away from the RPV, and about 13 ft of water (5.4 psi) in an inward direction,

- pressurization should not cause the water inlets to restrict water flow into the region between the RPV and the insulation (the buoyancy of the balls and thus the flow could be affected by pressurization in the direction away from the vessel), and

- movement (flexing) of the insulation should be restricted to prevent partial closure of the steam vent dampers or egress of steam into the region between the insulation and reactor cavity walls (through the seams between the insulation panels). A maximum inward deflection of 10.2 cm (4 in.) under maximum inward load was specific as a target value, which would maintain a minimum 5.1-cm (2-in.) gap between the RPV and the insulation, and match the minimum flow area of 0.7 $m^2$ (7.5 $ft^2$) represented by the flow path through the reactor vessel supports. If insulation shifting is postulated, it is not expected to significantly affect the heat transfer. The lower head is spherical and the adjacent insulation panels are straight which results in single point contact with the vessel in the area of concern that would not seriously impair surface wetting.

Westinghouse indicated that a structural analysis was performed for the conceptual design of the RPV insulation system and that the results of the evaluation show that the design was able to meet each of the defined functional requirements. Thus, a design that meets the functional requirements is feasible.

The RCS blowdown during a LOCA may tend to carry debris created by the accident toward the reactor cavity. In response to a staff request, Westinghouse performed an evaluation of the potential for such debris to block the ERVC flow path. On the basis of the estimate of 10,000 gpm through the insulation, the maximum approach velocity toward the entranceway between the vertical access tunnel and the RCDT room is less than 1 ft/s. Such an approach velocity would prevent significant transport of large debris. The opening between the vertical access tunnel and the RCDT room is covered by a metal grating that will prevent any large pieces of debris from entering the RCDT room. In addition, the damper between the RCDT room and the reactor cavity compartment, as well as the entrance into the RPV insulation is elevated. Because the water level at the time of debris relocation is several meters above the bottom of the insulation, floating or submerged debris cannot be ingested into the insulation flowpath. Finally, a functional requirement is included in the RPV insulation design to assure that the minimum flow area through each water inlet, as well as around the recirculating flow loop is at least 45.2 $cm^2$ (7 $in.^2$). The staff considers the potential for debris blockage of the ERVC flow path to be adequately addressed by the functional requirements of the insulation design and the related system ITAAC, and therefore the resolution of debris blockage is acceptable.

The ULPU testing included tests using prototypical RPV steel with paint applied according to Westinghouse paint application specifications. This paint is intended to protect the vessel carbon steel surface during shipment and storage, and is not expected to be removed. In the

ULPU tests, the paint surface was judged to actually increase the wettability of the vessel external surface and increase the critical heat flux. Therefore it is important that Westinghouse paint application specifications for the RPV exterior be met.

The RPV insulation is purchased equipment. The COL applicant will verify that the insulation is consistent with the design bases established for in-vessel retention. This is COL Action Item 19.2.3-1. The RPV insulation system and the damper between the reactor cavity and the RCDT room are included as risk-significant SSCs in the reliability assurance program, and important criteria associated with the design are incorporated into the ITAAC. Therefore, this is acceptable and resolves DSER Open Item 19.2.3.3-1.

19.2.3.3.2 Hydrogen Generation and Control

In SECY-93-087, the staff recommended that the Commission approve the staff's position that passive plant designs must include the following provisions:

- accommodate hydrogen generation equivalent to a 100-percent metal-water reaction of the fuel cladding
- limit containment hydrogen concentration to no greater than 10 percent
- provide containment-wide hydrogen control (such as igniters or inerting) for severe accidents

These positions are codified in 10 CFR 50.34(f)(2)(ix). In its SRM, dated July 21, 1993, the Commission approved the staff's position. The staff's evaluation of the Hydrogen Igniter Subsystem to meet the requirements of 10 CFR 50.34(f)(2)(ix) and the criteria in SECY-93-087 is contained in Section 6.2.5 of this report. Open Item 19.2.3.3-2 was closed on the basis of the evaluation in Section 6.2.5 of this report.

19.2.3.3.3 Core Debris Coolability

Core concrete interactions (CCI) is a severe accident phenomenon that involves the melting and decomposition of concrete in contact with core debris. This phenomenon would occur following reactor vessel breach, if the molten core debris discharged from the RPV is not quenched and cooled. CCI can challenge the containment by various mechanisms including: (1) pressurization from non-condensible gas and steam production, (2) destruction of structural support members, and (3) melt-through of the containment liner and basemat.

Westinghouse has incorporated several features in the AP600 design to prevent and mitigate the effects of CCI. At the time of the DSER, the staff was still evaluating these design features to ensure compliance with the criteria of SECY-93-087. Accordingly, the resolution of issues related to core debris coolability and CCI was identified as DSER Open Item 19.2.3.3-3.

In SECY-93-087, the staff recommended that the Commission approve the position that both the evolutionary and passive LWR designs meet the following criteria:

- provide reactor cavity floor space to enhance debris spreading

- provide a means to flood the reactor cavity to assist in the cooling process
- protect the containment liner and other structural members with concrete, if necessary
- ensure that the best-estimate environmental conditions (pressure and temperature) resulting from CCI do not exceed ASME Code Service Level C limits for steel containments, or factored load category for concrete containments, for approximately 24 hours

In addition, the designs should ensure that the containment capability has margin to accommodate uncertainties in the environmental conditions from CCI. In its July 21, 1993, SRM, the Commission approved the staff's position.

The AP600 design relies primarily on safety grade RCS depressurization and reactor cavity flooding capabilities to prevent RPV breach and CCI, but also incorporates plant features consistent with the criteria in SECY-93-087 and the EPRI URD criterion regarding debris coolability. In the unlikely event of RPV failure, these features would reduce the potential for containment failure from CCI. The AP600 design features include the following items:

- a cavity floor area that provides for debris spreading
- a manually-actuated reactor cavity flood system for the purpose of covering the core debris with water and maintaining long-term debris coolability
- a minimum 0.85 m (2.78 ft) layer of concrete to protect the embedded containment shell, with an additional 1.8 m (6 ft) of concrete below the liner elevation

The cavity flooding system is discussed in Section 19.2.3.3.1 of this report. The reactor cavity floor area and response of the concrete basemat is discussed below.

The reactor cavity is comprised of two interconnected compartments – an octagonal shaped room below the RPV, and an adjacent room containing the normal containment sump and the RCDT. The total floor area is 48 $m^2$, divided approximately equally between the two compartments. A 5 foot wide tunnel, and a 3 foot wide ventilation duct connects the two volumes. The tunnel connecting the two regions of the cavity is protected by a door that serves as an HVAC barrier during normal operation. The door and ventilation ductwork are expected to be displaced by the pressurization associated with RPV breach before the arrival of core debris, thereby permitting core debris to spread within the two compartments.

The reactor cavity sump is located along the back side of the wall dividing the two compartments, and is surrounded by an 45.7-cm (18-in.) high, 30.5-cm (12-in.) thick concrete curb. The location of the sump (out of the line-of-sight of the RPV) and the concrete curb provide protection against entry of core debris into the sump, as discussed later. The sump is covered with a stainless steel plate that supports the reactor cavity drain pumps. A number of sleeved ½-inch drain holes pass through the curbing at floor level to permit water to drain into the sump, but these passages are sufficiently small that molten core material would be quenched in the passages before entering the sump.

The embedded steel containment liner beneath the reactor cavity region is ellipsoidal in shape. The minimum distance from the reactor cavity floor to the embedded steel liner (0.85 m (2.8 ft)) occurs at the end of the RCDT room furthest from the reactor vessel. The distance from the floor of the cavity sump to the steel liner is only slightly less (0.52 m (2.7 ft)) because of the ellipsoidal shape of the liner and the more central location of the sump. In the calculations discussed below, the thickness of concrete above the liner is taken to be the minimum distance of 0.85 m (2.8 ft).

The ratio of reactor cavity floor area to rated thermal power for the AP600 design is 0.025 $m^2/MW_{th}$. This ratio compares favorably with the EPRI URD design criterion of 0.02 $m^2/MW_{th}$ for debris coolability, which represents the EPRI estimate of what is required to adequately cool core debris. However, the EPRI criterion was established on the basis of core power densities typical of current operating plants, and corresponds to a debris depth of about 10-inches. The AP600 design has a lower core power density and a corresponding core debris depth considerably greater than 10-inches, calling into question the applicability of the EPRI criterion to AP600. The staff concludes that the floor area provided in the AP600 design, in conjunction with the reactor cavity flooding system, will promote the potential for debris coolability but will not necessarily ensure it. Accordingly, the staff has relied on deterministic calculations described below, rather than the EPRI criterion, in judging the adequacy of the reactor cavity design for CCI.

As described in Section 19.2.3.3.1 of this report, external reactor vessel cooling (ERVC) features reduce the frequency of RPV breach in the baseline PRA to less than 1E-08/y. The staff considers reliance on the ERVC strategy consistent with Commission guidance in the SRM pertaining to SECY-93-087. In particular, under the topic of core debris coolability, the Commission stated that the staff should not limit vendors to only one method for addressing containment responses to severe accident events, but permit other technically justified means for demonstrating adequate containment response. However, in view of the complexity of the technical issues impacting the reliability of the ERVC strategy, the staff, in SECY-96-128, recommended that the Commission approve the position that Westinghouse use a balanced approach, involving reliance on in-vessel retention of the core complemented with limited analytical evaluation of ex-vessel phenomena, to address the adequacy of the AP600 design for ex-vessel events. In its January 15, 1997, SRM, the Commission approved the staff's position. The deterministic calculations for CCI are of particular significance for AP600 since, compared to other ALWRs, the AP600 ex-vessel debris bed is deeper (because of the higher ratio of zircaloy to fuel in the AP600 core) and the concrete basemat is thinner. In addition, the AP600 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls.

Westinghouse performed deterministic calculations of CCI for a postulated vessel breach event. These calculations are documented in Appendix B to the PRA. Westinghouse assumed an initial in-vessel core debris pool configuration consistent with the "Final Bounding State" in the DOE assessment of external reactor vessel cooling (DOE/ID-10460), i.e., essentially the entire inventory of core materials and steel structures, with the metal layer overlying the oxide pool. Westinghouse assumed the release of the entire mass of core debris in a molten state. This represents a conservative upper limit in terms of the mass of debris that could participate in CCI.

The following two vessel failure scenarios were evaluated: (1) a "hinged failure" in which a localized opening occurs near the vessel beltline immediately followed by the vessel tearing around nearly all its circumference, and the lower head hinging/swinging downward and coming to rest on the cavity floor, and (2) a "localized failure" in which a localized opening occurs near the vessel beltline (releasing molten core debris above the breach), and over time, moves downward releasing additional debris. For the localized failure mode, which involves a slow release and greater water depth than the hinged failure mode, Westinghouse used the THIRMAL code to assess the break-up and freezing of the melt as it falls through the water pool; these metal-water interactions were not considered for the hinged failure mode.

The MELTSPREAD code was used to analyze the spreading of the core debris over the various regions of the cavity floor. This permitted the metallic and oxidic components of the in-vessel core debris to be tracked separately during the release, spreading, and CCI phases. For both RPV failure modes, the analyses show a non-uniform distribution of the melt constituents, with the debris consisting primarily of oxides (and most of the decay heat) in the region directly under the reactor, and primarily of metals at the opposite end of the reactor cavity. The equilibrium depth of the debris in the two regions of the cavity is approximately equal in the "hinged failure" case since the debris remains molten during the spreading. However, the equilibrium debris depth in the "localized failure" case is greater under the reactor than in the RCDT room because of an accumulation of solidified debris below the reactor in this scenario.

The results of the MELTSPREAD analyses were used as input to the MAAP4 code for analysis of CCI. Two separate MAAP analyses were performed for each RPV failure mode – the first analysis to treat the debris under the reactor vessel, and the second to treat the core debris at the opposite end of the cavity, where the sump and RCDT is located. The MELTSPREAD results were also used to assess the likelihood and impact of debris entering the reactor cavity sump in the two vessel failure scenarios considered.

Westinghouse evaluated the effects of CCI assuming two different reactor cavity/basemat concrete compositions, i.e., limestone/common sand and basaltic concrete. For a basemat composed of limestone concrete (which maximizes non-condensible gas generation and minimizes concrete ablation) containment pressure is predicted to reach Westinghouse's Service Level C estimate (90 psig) at about 11 days following the onset of core damage, with basemat penetration expected some time later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes non-condensible gas generation) the predicted time of basemat melt-through is reduced to about 3 days, with containment over-pressure failure expected some time later. For both RPV failure scenarios and both concrete types, the concrete basemat in the region under the reactor vessel is eroded more rapidly than the region of the RCDT, and is the limiting location for basemat failure.

Although basemat penetration is unlikely, the Westinghouse assessment indicates that the molten core debris will reach the embedded liner (i.e., ablate through 0.847 m (2.78 ft) of concrete) within 7 to 9 hours of RPV breach with basaltic concrete, and within 15 to 17 hours of RPV breach with limestone concrete. However, in all cases, the top of the molten core debris pool is well above the embedded liner when melt-through first occurs, thereby preventing an airborne release of fission products. The staff does not consider the interface between the concrete basemat and embedded containment liner to be a viable pathway for significant airborne release of fission products to the environment in AP600 in view of the minimal gaps, if

any, between the concrete and the liner, and the considerable distance that fission products would need to travel along this pathway to reach the environment (a distance approximately equal to the radius of the containment. Accordingly, the staff's focus in assessing the capability of the AP600 to cope with CCI is on the time of basemat penetration rather than the time of melt-through of the embedded liner.

The MELTSPREAD calculations for the "localized failure" case indicate a maximum core debris depth of 25.4 cm (10 in.) in the region of the sump at any time in the transient. Thus, the reactor curb will prevent the entry of core debris into the sump for this scenario. Calculations for the "hinged failure" mode predict that a wave of molten core debris would be reflected off the back wall of the RCDT room and achieve a height of about 55.9 cm (22 in.) in the vicinity of the sump curb following the passage of the wave. The continued presence of core debris on the sump cover is expected to result in failure of the cover and debris entry into the sump in this scenario. Westinghouse does not consider this situation to pose a threat to containment because the core debris entering the sump would consist primarily of the metallic component of the melt, similar to the rest of the RCDT compartment. MAAP calculations show that the concrete penetration on the RCDT side of the cavity (by debris composed primarily of metals) is minimal compared to the penetration on the reactor side of the cavity (by debris composed primarily of oxides). Since the distance to the liner in the sump (0.82 m (2.7 ft)) is not significantly different than the distance assumed in the CCI calculations (0.85 m 2.8 ft)), the concrete penetration on the reactor side of the cavity is still expected to be limiting.

The staff considers Westinghouse's rationale regarding the significance of CCI in the cavity sump to be consistent with our expectations for the postulated failure scenarios, and reasonable. In judging the adequacy of the sump protection, the staff has also considered the following:

- the low probability of reactor vessel breach in the AP600 design, given that the requisite conditions for in-vessel retention (RCS depressurization and reactor cavity flooding) would be achieved in over 90 percent of core damage events, and the high confidence that vessel integrity would be maintained when these conditions are achieved

- the likelihood that considerably less core debris would be released than assumed by Westinghouse, particularly in events with earlier times to reactor vessel breach, such as the alternate debris bed configurations postulated in Section 19.2.3.3.1 of this report

- the AP600 will have no piping embedded in the concrete floor that could represent a potential path out of containment

On these bases, the staff considers the sump protection in the AP600 design to be acceptable.

The staff performed calculations using the MELCOR code to confirm the degree of basemat ablation for AP600 (ITS/SNL-95-006). The calculations indicate a maximum ablation depth of 0.52 m (1.7 ft) and 0.21 m (0.7 ft) for basaltic and limestone concrete 9 hours after vessel failure, assuming the debris is spread uniformly throughout the reactor cavity. (The calculations were terminated at this time.) If the debris does not spread outside the area below the reactor vessel, the maximum ablation depth predicted by MELCOR increases to 0.34 m (1.1 ft) at 9

hours for limestone concrete. The ablation rates predicted by MELCOR are considerably lower than estimated by Westinghouse, partially as a result of the following:

- the assumption of a homogeneous debris bed composition in MELCOR, in contrast to a segregated melt configuration modeled in the MELTSPREAD code (which results in a higher debris bed power density below the reactor vessel)

- a later time of RPV failure in the MELCOR calculation (15 hours in MELCOR versus 3 hours in MELTSPREAD).

While not directly comparable to the MAAP calculations, the MELCOR calculations support the Westinghouse finding that basemat penetration would not occur for several days.

The staff concludes that in the event that core debris is not retained in vessel, the AP600 design provides adequate protection against early containment failure and large releases resulting from CCI. Specifically, the AP600 incorporates features that adequately address all criteria called out in SECY-93-087 related to core debris coolability. Although several factors in the AP600 design mentioned earlier could tend to increase the severity of basemat melt-through, best-estimate calculations performed by Westinghouse and confirmed by NRC-sponsored calculations indicate that in the event of unabated CCI, containment basemat penetration or containment pressurization above ASME Code Service Level C limits will not occur until well after 24 hours, regardless of concrete composition. On this basis, the staff finds the AP600 design acceptable in terms of its protection against CCI. Therefore, DSER Open Item 19.2.3.3-3 is resolved.

19.2.3.3.4 High-Pressure Core Melt Ejection

High pressure core melt ejection (HPME) and subsequent direct containment heating (DCH) is a severe accident phenomenon that could lead to early containment failure with large radioactive releases to the environment. HPME is the ejection of core debris from the reactor vessel at a high pressure. DCH is the sudden heatup and pressurization of the containment resulting from the fragmentation and dispersal of core debris within the containment atmosphere. In addition, DCH can also lead to direct attack on the containment shell.

Westinghouse has incorporated several features in the AP600 design to prevent and mitigate the effects of DCH, specifically, the automatic depressurization system and reactor cavity design features. At the time of the DSER, the staff was still evaluating these features against the criteria of SECY-93-087. Accordingly, the resolution of issues related to high pressure core melt ejection and direct containment heating was identified as DSER Open Item 19.2.3.3-4.

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the evolutionary and passive LWR designs provide a reliable depressurization system and cavity design features to decrease the amount of ejected core debris that reaches the upper containment. Examples of cavity design features that will decrease the amount of ejected core debris reaching the upper containment include ledges or walls that would deflect core debris and an indirect path from the reactor cavity to the upper containment. In its July 21, 1993, SRM, the Commission approved the staff's position.

One of the major features of the AP600 design is the automatic depressurization system (ADS). The ADS is an automatically-actuated, safety-grade system consisting of 4 different valve stages that open sequentially to reduce RCS pressure sufficiently so that long-term cooling can be provided from the passive core cooling system. In the event that automatic actuation fails, the ADS is initiated by operator action from the main control room using the diverse actuation system. The ADS valves are designed to remain open for the duration of any ADS event, thereby preventing repressurization of the RCS. The performance of the ADS for design-basis accident is discussed in SSAR Section 6.3 and Sections 5.1.3.7 and 6.3 of this report. The modeling of ADS in the PRA is described in Chapters 11 and 36 of the PRA.

The Level 1 PRA includes consideration of RCS depressurization (by automatic and manual actuation of ADS) early in an event to prevent core damage. For those sequences that proceed to core uncovery at high RCS pressure, the potential to manually depressurize the RCS before the occurrence of thermally-induced SGTR or HPME is further evaluated in the Level 2 PRA. The survivability of the ADS valves and related instrumentation within the early phase of a severe accident during which late depressurization is viable is addressed in Appendix D of the PRA and Section 19.2.3.3.7 of this report. This assessment indicates that the design basis temperature will only be exceeded for a short time preceding late actuation of the valves. Because the ADS valves will be actuated before the time of rapid cladding oxidation and high RCS blowdown temperatures and because of the high likelihood that the valves will be available well into a severe accident, the staff concludes that the ADS valves will be available to depressurize the RCS during a severe accident.

As discussed in Section 19.1.3.2.1 of this report, the majority of Level 1 sequences in the baseline PRA (about 85 percent) involve events with at least partially successful RCS depressurization, and relatively low RCS pressure (<150 psig) at the time of core uncovery. With credit for late RCS depressurization, an even larger fraction of the core melt sequences (about 90 percent) are estimated to involve a depressurized RCS at the time of RCS pressure boundary challenge. Thus, only about 10 percent of the core damage events would potentially result in DCH. In the PRA, high pressure core melt sequences (with unsuccessful late depressurization) are assumed to result in failure of the SG tubes before reactor vessel failure. This obviates the need for additional thermal-hydraulic and probabilistic analyses of the following:

- the likelihood of RCS piping versus steam generator tube over-pressure failures in ATWS events
- the likelihood of containment failure from DCH pressure loads in high pressure core melt accidents
- the relative threat and timing of creep-rupture failures in RCS piping, hot legs, and steam generator tubes in high pressure core melt accidents

However, if such a failure does not occur and all high pressure core melt accidents result in RPV failure, the resulting frequency of HPME events would remain very small (about 2E-08/y).

The design of the reactor cavity is expected to decrease the amount of ejected core debris that reaches the upper containment. The pathways for debris transport from the AP600 reactor cavity include the following:

- the annular openings between the coolant loops and the biological shield wall, that lead to the steam generator compartments
- the area around the reactor vessel flange that leads directly to the upper compartment (blocked by a permanent refueling cavity seal ring)
- a ventilation shaft from the roof of the RCDT room, that leads to the steam generator compartments

Debris particles traveling along the first two paths would pass between the RPV and the cavity walls, around the boro-silicone neutron shield blocks, through the HVAC air flow slots in the RPV vessel supports, and into the nozzle gallery surrounding the upper portion of the vessel, before passing through either the annular openings between the coolant loops and the biological shield or the gap around the permanent cavity seal ring. Particles traveling along the third path would pass into the RCDT side of the reactor cavity, up into a ventilation shaft in the ceiling of the RCDT room, into a common tunnel between the two steam generator compartments, and into the steam generator compartments. In all cases, the particles would change direction and encounter obstacles before reaching the upper containment.

Westinghouse evaluated the containment pressure loads for a postulated RPV breach event in the AP600 design using the Pilch 2-cell model developed under NRC-sponsorship for resolution of the DCH issue. This calculation is documented in Appendix B to the PRA. In the calculation, the steam generator compartments were modeled as one cell and the volume above the operating deck was modeled as the second cell. Because the flow configuration from the reactor cavity during DCH can not be easily determined because of the impact of dislodging or damaging the reactor vessel insulation and ventilation-related structures adjacent to the RPV, a bounding calculation was performed that assumed the permanent refueling cavity seal ring is completely dislodged at the beginning of the melt ejection, and the reactor vessel insulation and ventilation-related structures completely block the flowpaths through the biological shield wall.

The RPV was assumed to fail at the bottom of the hemispherical head and result in forcible ejection of 50 percent of the total UO2 and zirconium in the core. In addition, it was assumed that 90 percent of the zirconium was unoxidized, further increasing the pressurization. The peak containment pressure for a postulated DCH event was estimated to be about 81 psig. This value is below Westinghouse's estimated value for Service Level C and is sufficiently small that the corresponding probability of containment failure is negligible (less than 0.1 percent).

The staff concludes that the AP600 design provides adequate protection against early containment failure and large releases due to DCH. Specifically, the AP600 incorporates a safety-grade depressurization system, and reactor cavity design features that are expected to decrease the amount of ejected core debris that leaves the reactor cavity in the event of a high pressure melt ejection event. These features adequately address all criteria called out in SECY-97-187 related to high pressure melt ejection. In the event of an RPV breach at high pressure, calculations performed by Westinghouse using the NRC-developed model for DCH

issue resolution indicate that the peak containment pressure will remain sufficiently small, and that the corresponding probability of containment failure is negligible. On these bases, the staff finds the AP600 design acceptable in terms of its protection against DCH. Therefore, DSER Open Item 19.2.3.3-4 is resolved.

19.2.3.3.5 Fuel-Coolant Interactions

The containment function can be challenged by energetic fuel-coolant interactions (FCI) that result in a steam explosion. The term steam explosion refers to a phenomenon in which molten fuel rapidly fragments and transfers its energy to the coolant, resulting in rapid steam generation, and shock waves. Section J, "Containment Performance," of SECY-93-087 indicates that the staff will evaluate the impact of FCI on containment integrity by using the containment performance goal. The purpose of this section is to perform such an evaluation for steam explosions that may occur either inside (in-vessel) or outside (ex-vessel) the AP600 reactor vessel.

19.2.3.3.5.1 In-Vessel Steam Explosions

In-vessel steam explosions were not modeled in the AP600 PRA on the basis of the assumption that the phenomenon is "physically unreasonable." The basis for this assumption was the report, "Lower Head Integrity Under In-Vessel Steam Explosion Loads," DOE/ID-10541, henceforth denoted as the IVSE report. The IVSE report along with its companion reports, "Propagation of Steam Explosions: ESPROSE.m Verification Studies," DOE/ID-10503, "Pre-mixing of Steam Explosions: PM-ALPHA Verification Studies," DOE/ID-10504, and, "In-vessel Coolability and Retention of a Core Melt," DOE/ID-10460 are referenced in Chapter 39 of the AP600 PRA. DOE/ID-10460 will be referred to as the IVR report in this section.

The overall approach taken in the IVSE report generally follows the framework of Risk Oriented Accident Analysis Methodology (ROAAM). Briefly, the approach involves decomposing the in-vessel steam explosion issue into a set of contributing physical processes, quantifying these processes through a combination of "causal relations" representing best estimate physics and probability distributions representing "intangible parameters" and finally, combining the quantification of individual processes into an integral assessment of the overall issue. The physical processes are as follows:

- melt relocation into the lower plenum
- initial melt-water interactions leading to coarse breakup of melt and forming a premixture
- triggering of premixture and further melt-water interactions of the energetic type leading to steam explosions
- consequent loading of the lower head and its response

The causal relations describing these physical processes, in their respective order, are:

- melt progression (analytical treatment founded on physics)
- premixing (PM-ALPHA code and associated models)

- explosion propagation (ESPROSE.m code and associated models)
- structural loads and response (ABAQUS code)

The intangible parameters, identified in the IVSE report, are as follows:

- the location and size of the failure
- melt characteristic length scale (initial size of melt particles)
- evolution of melt length scale (breakup rate)
- trigger strength and timing

Of these intangible parameters, some were treated in a deterministic manner (e.g., failure location, trigger strength), whereas probability measures or range of values were assigned to others (e.g., failure size, initial melt particle size, melt breakup rate, and trigger timing).

The problem of in-vessel steam explosions in AP600 is formulated within the structure of ROAAM. However, the usual ROAAM approach, i.e., consideration of splinter scenarios, assignment of probability distributions to intangibles, and convolution of causal relations with the probability distribution (illustrated in Figure 2.3 of the IVSE report) was not rigorously followed in this case. Three reasons were cited: (1) a unique melt relocation scenario, (2) bounding approach taken with regard to premixing and explosion calculations, and (3) non-intersecting load and fragility curves. Moreover, the IVSE report argued that the bounding approach obviated any parametric and sensitivity calculations. Table 19.2-1 summarizes the treatment of intangible parameters identified in the report.

19.2.3.3.5.1.1 Quantification of Melt Relocation Characteristics

The objective of the IVSE report was to take a "bounding" approach with regard to the location and size of melt release. Specifically, the IVSE report concluded that in an AP600 geometry, the melt release would occur following a sideways growth of the crust surrounding the melt pool, breach of the reflector and the core barrel, and melt flow out of the pool into the lower plenum water. The location was predicated upon a melt relocation scenario that would lead to a stable blockage (crust) formation at the lowest region of the active fuel (i.e., on top of the lower core support plate) thus making the downward relocation path unavailable. Calculations were provided for the timing of core barrel and reflector meltthrough as well as the timing of core plate dryout, and it was shown that the sideways failure would occur before the core plate dryout. Note that these calculations are dependent on the physical properties of crust (e.g., thermal conductivity, porosity), its growth rate, and heat flux distribution in the melt pool (i.e., up, down, and side).

The AP600 design has a relatively flat radial power profile and a high aspect ratio. Also, the core plate is much thicker in the AP600 design (about twice that of operating reactors) so that it acts as a substantial heat sink. These design features make the sideways meltthrough more likely to precede the core plate meltthrough. However, given the uncertainties in the current understanding of late phase melt progression, it is difficult to completely rule out, as the IVSE report did, the downward relocation of melt. The staff has commented on the uncertainties in crust properties, heat flux distribution, etc., with regard to their implication on the likelihood of downward relocation, and recommended that sensitivity studies involving these parameters be performed. The staff has also commented on the possibility of bottom crust failure from a

primary explosion which could create a path for downward relocation, possibly leading to secondary explosions strong enough to challenge the lower head integrity. The DOE peer review raised this latter issue as well.

In response to these comments, Westinghouse performed additional sensitivity studies involving crust porosity and thermal conductivity, and submitted the results in the "Addendum to Chapter 4" of the DOE report. The results showed that the bottom crust was indeed stable in all cases and that the downward heat flux (relevant to core plate meltthrough timing) was still within the range estimated previously. The partitioning of the upward, sideward, and downward heat fluxes at the boundaries of the oxide pool is presented as a function of time in Figure 4.13(b) of the IVSE report. The heat flux partitioning was determined by correlations that were derived from the mini-ACOPO data as documented in the IVR report or correlations available in the literature on the basis of other similar experiments. It is recognized that there are some uncertainties in the various correlations used. However, the downward heat flux (relevant to downward relocation) calculated by Westinghouse is an order of magnitude smaller than the upward and sideward heat fluxes so that even relatively large uncertainties in heat flux calculations are not likely to alter the original partitioning in any significant manner. On this basis, Westinghouse concluded that the possibility of a downward relocation need not be considered further.

The IVSE report initially dismissed the possibility of bottom crust failure from a primary explosion that could result in a downward relocation and subsequent secondary explosions from a much higher secondary release rate. Later, Westinghouse agreed to deterministically evaluate the NRC's postulated scenarios. However, only qualitative arguments were offered that any secondary explosion would involve a complex relocation process, and would not be conducive to producing an explosion load to threaten the containment. To strengthen these qualitative arguments, the staff requested that Westinghouse quantify the scenario. Westinghouse declined to provide additional quantification because they believed that such analyses would be of limited value due to the uncertainties associated with crust failure. The staff acknowledges that this scenario is less likely because the initial FCI will cause significant voiding and limit the amount of water in the lower head available for a subsequent FCI. Nevertheless, because of the uncertainty associated with crust failure and the limited qualitative arguments provided by Westinghouse, the staff is unable to eliminate this scenario from further consideration.

For the sideways meltthrough, melt release rates considered (100, 200, and 400 kg/s) are comparable to the TMI-2 scenario. These rates were calculated on the basis of an exit velocity of 1 m/s under gravity draining and exit hole sizes of 10 cm x 10 cm, 10 cm x 20 cm, and 10 cm x 40 cm, respectively. Westinghouse claimed these numbers formed a reasonable range to bound the release rates, but the staff noted that the hole size in TMI-2 was much larger (60 cm x 150 cm) and asked why the hole size seen at TMI-2 should not be considered for the AP600 analysis. In response, Westinghouse furnished additional information on the TMI-2 release scenario including quantifications of the release rate and the hole size, which provided further confirmation of the acceptability of release rates considered for AP600. Specifically, Westinghouse stated that in the TMI-2 scenario, the side-pour of about 30 tons of melt (comprising of approximately 20 tons of melt which relocated into the lower plenum and 10 tons that froze in the core barrel assembly and core support assembly regions) occurred over a time period (quoted as 60 seconds, but widely reported in the literature between 60 and 120 seconds). This makes the release rates to range between 250 kg/s and 500 kg/s.

However, it is generally accepted, on the basis of neutron flux and other signatures, that the duration of TMI-2 relocation was between 90 and 120 seconds, making the release rates to range between 250 kg/s and 330 kg/s. Predicated on this, the staff finds the AP600 release rates to be comparable to that of the TMI-2. Also, the melt was released in the TMI-2 scenario with an initial jet diameter of 10 cm (as deduced from the post-accident examinations), but gradually burned a hole in the baffle plate having the approximate dimensions of 60 cm x 150 cm. Therefore, the staff finds the exit hole sizes assumed in the AP600 analysis to be comparable to that of TMI-2, and acceptable.

19.2.3.3.5.1.2 Quantification of Premixtures

The approach to quantification of premixtures, taken by Westinghouse in the IVSE report, involved specifications of a range of values (20 mm to 80 mm) of the initial melt length scale, a range of values (from 10 to very large or no breakup, denoted as nb) of the breakup parameter (beta), and formulation of a causal relation (founded on the PM-ALPHA code calculations) for the quantity of fuel mass in a premixture. Originally, a single value (20 mm) of the melt length scale was chosen, but the basis for the choice was not stated. The staff recommended additional PM-ALPHA calculations with higher values of the initial melt length scale to determine if larger length scales would affect the mixing and, subsequently, the explosion calculations on the side of producing larger explosion loads.

In response to the staff recommendations, Westinghouse performed a parametric study of the effect of melt length scale by considering two additional scales (40 mm and 80 mm). First, the premixing calculations were done for both scales without any breakup to examine the premixture configurations in an extreme case (i.e., no breakup). Next, premixing calculations were performed with a breakup parameter (beta) of 20 and 30. These values of beta were chosen because they produced the highest impulse loads in Tables 6.1 and 6.a1 of the IVSE report. The results of the premixing calculations with beta equal to 20 were used as input into the explosion calculations using ESPROSE.m. As a result of lower surface area for the large melt length scale and excessive voiding of the premixture zone, no explosions developed. Thus, it was demonstrated that larger melt length scales would actually produce mixtures that were much more difficult to explode. On the basis of this, Westinghouse concluded that the original choice of length scale was conservative. The staff agrees with the conclusion noting that the breakup or coarse fragmentation is modeled parametrically in PM-ALPHA. The IVSE report fully recognized this but emphasized that other important aspects of premixing physics were mechanistically treated in the code. Moreover, the report pointed out that through the choice of multiple breakup parameters, a bounding treatment of fragmentation during premixing was provided.

In response to comments from the DOE peer reviewers on the applicability of PM-ALPHA and its predictive capability over a wide range of mixing conditions, Westinghouse provided the following additional information in an addendum to Chapter 5 of DOE/ID-10541:

- Premixing calculations to longer mixing times
- Premixing calculations at higher (3 bars) system pressure
- Premixing calculations with subcooled (10 °C) water
- Premixing calculations with finer grid (mesh) size

It was concluded from the results of the sensitivity studies that the "sensitive" premixtures in all cases considered are small in size and of a short time duration. Westinghouse also furnished a report (DOE/ID-10504) on the PM-ALPHA verification studies. This report is an account of code assessment against separate effects experiments, integral experiments, and code-to-code comparison. Finally, additional perspectives on the regimes of premixing was provided in Appendix B to DOE/ID-10541, in which data from the MAGICO-2000 (high temperature) experiments were produced. On the basis of the additional information, Westinghouse claimed that PM-ALPHA adequately demonstrated the "fitness-for-purpose" and performed in a satisfactory to excellent manner when assessed against a large body of experimental data.

The staff has not conducted an independent verification of the PM-ALPHA code. However, on the basis of its review of the information submitted by Westinghouse, the staff notes that a reasonably large assessment data base supports Westinghouse's use of the PM-ALPHA code for this assessment. The staff finds the use of the code to quantify pre-mixtures as applied to the AP600 acceptable.

19.2.3.3.5.1.3 Quantification of Explosion Loads

Westinghouse's approach to the quantification of explosion loads, was founded on the assumption that a given premixture was always triggerable (i.e., the probability of triggering is unity) and, as such, involved specification of a trigger of sufficient strength (~ 100 bar) to initiate explosions. Further, the approach involved consideration of a range of values of trigger timing (0.05 s to 1.0 s) and formulation of a causal relation (determined by the ESPROSE.m code) for the impulse loading from steam explosions. A total of 24 loading calculations were performed initially. Of these, 7 cases produced a peak pressure in the range between 200 MPa and 1000 MPa (an indication of the degree of severity). However, the calculated impulse loads in these seven cases were between 90 kPa-s and 190 kPa-s, i.e., below the fragility limit of the lower head material.

The staff questioned the conclusion that "peak impulses do not depend strongly on the size of the mixing zone," and expressed concern that in one calculation (release rate of 400 kg/s, $\beta = 20$, trigger timing of 0.12 s), the peak pressure was very high (about 1000 MPa). Westinghouse acknowledged this concern and in the addendum to Chapter 6 of DOE/ID-10541, furnished results of a revised and expanded assessment (Table 6.a1) using a later version of PM-ALPHA and ESPROSE.m which had received additional verification and validation against experimental data. A total of 24 additional calculations were presented in the addendum for trigger times well above those in the original 24 calculations (i.e., for trigger times between 0.23 s and 1.45 s). The new calculations were done to also respond to a DOE peer review comment on the impact of trigger timing and location on explosion loads. The additional calculations spanned, in some cases, longer propagation times and finer grid sizes.

The trends of the new calculations were similar to those presented in Table 6.1 of the IVSE report. In all the latter 24 cases, the impulse loads were found to be below the fragility limit (loads ranging from 11 kPa-s to 140 kPa-s). There was no discernible pattern of the magnitude of impulse and its dependence on trigger timing.

With regard to trigger location, the IVSE report stated that "we did not do extensive variations on location of trigger, but what we have seen agrees with what we expect; it is the premixture composition rather than the location or magnitude of trigger that controls the energetics." The

staff believes that the Westinghouse approach to triggering, i.e., that a premixture will always trigger, is conservative. Moreover, the influence of trigger location to energetics, if discernible, is likely to be bounded by sensitivity analysis involving trigger timing. Therefore, the staff considers this to be acceptable and the issue is resolved.

As in the case of premixing, the DOE peer reviewers questioned the maturity (i.e., the state of development and assessment) of the ESPROSE.m code as well as various models (e.g., fragmentation, "microinteractions", and wave propagation). Westinghouse furnished report DOE/ID-10503 on the ESPROSE.m verification studies. However, the assessment is not nearly as extensive as that of PM-ALPHA. For example, besides the single-drop SIGMA (separate effects) experiments, the code was assessed against only one integral experiment (KROTOS-38). A relatively large number of assessments against analytical tests was carried out. One major shortcoming of the code is that the microinteraction concept is yet to be verified experimentally with the real reactor material, and the verification study clearly acknowledged this. Another issue, much like the PM-ALPHA code, is the parametric nature of the fragmentation modeling. Specifically, the fragmentation model in ESPROSE.m is built upon three parameters: (1) a correlation constant in the hydrodynamic fragmentation model, (2) a second correlation constant to simulate the thermal effect, and (3) a fuel entrainment factor. These parameters were determined empirically from a relatively small number of experiments at low to moderate temperatures. As such, the domain of applicability of the model is somewhat limited. Again, the study recognized this limitation and suggested additional experiments to gain further insights.

The staff believes that, despite some limitations, the ESPROSE.m assessment, as documented in the DOE/ID-10503 report, demonstrated the reasonableness of the code as intended. On the basis of the review of the information submitted by Westinghouse, the staff finds the use of the code as applied to the AP600 acceptable.

19.2.3.3.5.1.1.4 Structural Failure Criteria

The IVSE report used the ABAQUS structural code to determine the response of the lower head for a given impulse load (equivalently, a pressure peak with a corresponding pulse width). The calculated values were then compared to some failure criteria (e.g., percentage of cross section exceeding certain strain values) to determine if the lower head is going to survive (expressed in the report in terms of the failure probability). For the calculated impulse loads (190 kPa-s maximum, from the quantification of explosion loads in the initial set of calculations), the equivalent plastic strain was calculated to be less than 11 percent (Figures 3.4 and 3.8 of DOE/ID-10541).

As shown on Table 3.3 and Figure 3.10 of the IVSE report, failure probabilities were then assigned to percentages of the lower head cross section exceeding 11 percent strain for given impulse loads and for different loading patterns. This form of probabilistic quantification is reasonable, in particular, if uncertainties or sensitivities (e.g., material properties) are to be accounted for. It is noted from the fragility plots (Figure 3.11 of DOE/ID-10541) that the failure probability is $10^{-3}$ or less for impulse loads below 200 kPa-s. For impulse loads in excess of 300 kPa-s, the failure probability is close to one. Since the maximum impulse load calculated is 140 kPa-s, it means there is a margin of over 150 kPa-s in Westinghouse's estimate (difference between 300 kPa-s load that will fail the vessel and the actual 140 kPa-s).

With the exception of downward relocation resulting from crust failure which the staff considers less likely, the staff concludes that the main report, "Lower Head Integrity Under In-Vessel Steam Explosion Loads (IVSE report)," along with it's companion reports, DOE/ID-10541, "Premixing of Steam Explosions: PM-ALPHA Verification Studies," DOE/ID-10504, and "Propagation of Steam Explosions: ESPROSE.m Verification Studies," DOE/ID-10503, are acceptable in addressing the topic of in-vessel steam explosions in AP600. The main report, along with the companion reports listed above are acceptable for determining the magnitude of in-vessel steam explosions for the sideways melt release scenario for the AP600. Although the staff did not review and approve Westinghouse's structural analyses, there appears to be adequate margin, as discussed above, to support the conclusion that in-vessel steam explosions (for the sideways melt release scenario) of sufficient magnitude to challenge the structural integrity, as calculated by Westinghouse, of the AP600 lower head are of sufficiently low probability to be discounted from further consideration. This evaluation closes DSER Open Item 19.2.3.3-5.

19.2.3.3.5.2 Ex-Vessel Steam Explosion

Section J, "Containment Performance," of SECY-93-087 indicates that the staff will evaluate the impact of interaction between molten fuel and coolant, on the integrity of the containment, consistent with the containment performance goal. Westinghouse states, in Chapter 34.2.2, "Fuel-Coolant Interaction (Steam Explosions)," of the PRA, that ex-vessel steam explosion is mitigated by the in-vessel retention of the core debris. In the event that the reactor cavity is not flooded and the vessel fails, the PRA does not credit containment integrity. The staff finds this treatment of ex-vessel steam explosions in the PRA to be conservative, with respect to the containment performance goal. Nevertheless, the staff also stated in SECY 93-087 that it would evaluate the dynamic forces attributable to ex-vessel fuel-coolant interactions outside the reactor vessel.

Westinghouse's assessment of ex-vessel steam explosion loadings on the reactor cavity, reactor pressure vessel, and the containment liner is contained in Appendix B.3 to the AP600 PRA. Two reactor vessel failure modes were considered in the assessment: (1) localized creep rupture of the vessel at the locations of highest heat flux leading to a small localized opening, and (2) global creep rupture leading to "unzipping" of the lower head (denoted as the "hinged" failure mode) at or near the transition between the hemispherical lower head and cylindrical vessel structure. The first of these modes produces a small (~3.8 kg/s), localized flow of melt out of the vessel sidewall into the cavity water pool through an equivalent 6.0 cm diameter opening, while the second produces a massive flow (15,100 kg/s) through a much larger opening (~100 cm diameter) caused by global creep rupture failure at the belt line (transition between the hemispherical and the cylindrical parts). The details of each of the assumed reactor vessel failure modes are provided in Reference B-6, DOE/ID-10523, "Analysis of Melt Spreading in an AP600-Like Cavity," of Appendix B to the AP600 PRA. Both failures are considered at a fully depressurized RPV condition and, as such, the conclusions are valid only for that condition.

Westinghouse used the NRC sponsored TEXAS code to run two baseline calculations – one each for the localized and hinged failure modes – and four sensitivity calculations for the localized failure mode only. The input parameters for TEXAS calculations are shown in Table 19.2-2 of this report and the results (peak pressure and impulse load) are summarized in Table 19.2-3 of this report. From the results of TEXAS calculations, it was concluded that in all

but the case of hinged failure, the impulse loads were very small so as not to cause any concern about the integrity of the cavity concrete structure. In the case of hinged failure, the conclusion was that the structural integrity of the concrete cavity floor and wall would not be retained, but that the structural integrity of the steel containment vessel would be maintained. Westinghouse also assessed the vertical uplift of the reactor pressure vessel resulting from the impulse loads calculated for the hinged failure mode, and determined that the energy release was insufficient to propel the reactor vessel far enough to impact the containment vessel.

The staff questioned the basis of the hole sizes chosen for both the localized failure and the hinged failure cases. In response, Westinghouse stated that the hole size of 0.06 m for the localized failure case was chosen arbitrarily and offered the engineering judgement that such a small hole would be consistent with draining the metallic upper layer of the in-vessel molten core debris pool before the oxidic layer. While the staff is not convinced of the explanation, it is noted that even with a reasonable variation in hole sizes for the localized failure case, the overall conclusion that the containment integrity would not be challenged is not expected to change. The hinged failure case was modeled as 236 coherent jets with a diameter of .068 m, and the model was chosen to represent the upper metallic layer spilling from the "unzipped" lower crucible. The diameter and number of coherent jets were calculated assuming a melt mass flow rate of 15,100 kg/s from the cylindrical part of the RPV. The staff finds this modeling of the hinged failure case to be acceptable.

The staff also questioned the choice of melt temperature and superheat for the hinged failure case, noting the values used for these parameters in the TEXAS calculations were those of steel, i.e., a metallic melt. Westinghouse assumed that the initial fuel-coolant interactions would involve molten steel and water in the hinged failure configuration, as shown in Figure B-1 of the PRA. It is not evident that would be the case if the melt pool is well mixed. Even in a stratified situation, there are two possible scenarios in which the oxidic melt may be released before the metallic melt in the event of a vessel breach. The first possibility arises from a breach at a location slightly below the metallic upper layer of the melt pool. The second possibility arises from a layer inversion process in the melt pool as considered in the IVR report. In Section 19.2.3.3.1 of this report, the staff concluded that layer inversion, if it occurs, could result in heat fluxes that exceed the critical heat flux which, according to the ROAAM study, is necessary and sufficient for the RPV failure.

In response, Westinghouse stated that a fully mixed pool is not consistent with the AP600 relocation scenario considered in the IVR study. Likewise, Westinghouse considered a layer inversion as speculated within the context of the IVR study. Westinghouse further confirmed that the top metal layer will essentially contain reflector steel relocated late in the melt progression sequence and, as such, the issue of zirconium oxidation did not arise. The latter issue was raised by the staff, particularly for the case of a well mixed pool containing some unoxidized zirconium that would then provide a source for additional chemical energy release. Finally, Westinghouse concluded in the IVR report that the conditions that would produce peak heat flux at the top of the oxide layer (below the metal layer) would also produce significant margin to vessel failure. Therefore, the IVR report did not support the vessel failing below the metal layer. The staff evaluated the IVR report in Section 19.2.3.3.1 of this report. As part of this evaluation the staff's contractor performed calculations, such as Figure 3.3, of the report titled, "Potential For AP600 In-Vessel Retention Through Ex-Vessel Flooding," INEEL/EXT-97-00779, December 1997. Figure 3.3. shows that the minimum margins to failure

were at or above the oxide-metallic layer. Therefore, the staff accepts Westinghouse's explanation that the melt composition participating in FCI in the hinged failure case would be metallic comprised essentially of steel.

Westinghouse provided an assessment of ex-vessel steam explosion loadings on the structural integrity of the containment in Appendix B.3.2 to the AP600 PRA. In the assessment, Westinghouse used the loading associated with the hinged reactor vessel failure mode described above. Westinghouse determined that the reactor cavity floor cracked and the wall structures failed from this loading. Westinghouse than assessed what impact this loading would have on the structural integrity of the containment vessel. Using a triangular impulse load with a peak pressure of 175 MPa and a duration of 0.006 seconds, Westinghouse calculated that the containment vessel will be less than 20 percent of its ultimate strain capacity, and therefore, can withstand the peak postulated loading from a hinged reactor vessel failure. The staff performed an independent evaluation and found that the tensile elongation of the embedded steel plate was less than the ultimate tensile elongation of SA517, Class 2 at the lowest stiffness soil case of 520 kips/ft$^3$ even considering the strain rate effect of the loading. The staff finds the structural analysis described above to be acceptable for addressing DSER Open Item 19.2.3.3-7. Therefore, DSER Open Item 19.2.3.3-7 is closed.

For the RPV uplift evaluation, Westinghouse used an one-degree-of-freedom model consisting of the RPV without its internals which would be lost in the explosion. A triangular impulse load with 175 MPa peak pressure and a duration of 0.004 seconds was used. The RPV supports are assumed to be unavailable and the stiffness of the model is associated with the RPV piping. The piping stiffness is varied since it is not known what stiffness the piping will have due to inelastic behavior. A wide range of stiffness (corresponding frequency range is 0.001 to 300 Hz) was used. The staff performed an evaluation and found that Westinghouse's conclusion founded on these calculations is reasonable. The staff's 175 MPa case produced 22' of uplift. This assumes the hot and cold legs shear due to the explosion loadings and the RPV becomes a projectile. This evaluation did not consider splinter scenarios such as the following:

- large concrete projectiles created by the explosion piercing the containment vessel
- the RPV piping does not shear and their collapse causes the failure of their penetrations

The refueling canal is 28'1" high, therefore, the RPV remains in the refueling canal area on the basis of the assumed scenario.

The staff, through its contractor Energy Research, Incorporated (ERI), sponsored a study to assess ex-vessel steam explosions in the AP600 reactor cavity. The assessment was performed using the PM-ALPHA/ESPROSE.m (older version than that used by Westinghouse for the in-vessel steam explosion calculations) and the one dimensional TEXAS computer codes. The results of the assessment are documented in a report titled, "An Assessment of Ex-Vessel Steam Explosions in The AP600 Advanced Pressurized Water Reactor," Report Number ERI/NRC 95-211, dated September 1996. The study consisted of a base case and a number of parametric calculations each for a fully submerged RPV, a partially submerged RPV, and an unsubmerged RPV. The study did not consider chemical augmentation of the steam explosion energetics, nor did it consider initial conditions representative of a slightly elevated RPV pressure scenario.

The mass, composition, and temperature of the core debris were determined by SCDAP/RELAP5 and MELCOR analyses of low pressure accident scenarios. The initial pressure of the reactor cavity was assumed to be 0.164 MPa. For the baseline scenarios, the study assumed 109,900 kgs of core debris in the lower plenum at a temperature of 3100°K with a melt superheat of 300 °K. The core debris was composed of $UO_2$, $ZrO_2$, Zr, Ag, and steel. The water pool in the cavity was assumed at a temperature of 387 °K.

Thermal load calculations in combination with structural calculations were performed in order to predict the location of the lower RPV head failure. These analyses are documented in Appendices A and B to the ERI report. The results of the thermal response analyses indicate that the high heat transfer rate from the molten pool causes local melting of the inner vessel wall at the side-wall location, for both unsubmerged and submerged conditions. The structural calculations founded on the thermal response of the lower head indicate that the most likely failure is a 0.4 m diameter hole at the side-wall. This resulted in a melt discharge velocity of 2.9 m/s into a flooded reactor cavity.

Mechanistic prediction of hole size at the failure location was judged not to be possible, given the uncertainties associated with the RPV failure. Therefore, the failure size was treated parametrically. For the base case calculations the size of the lower head failure was taken to be 0.4 m, and as a sensitivity, it was decreased and increased by a factor of two to span a range of variations, i.e., between 0.2 m and 0.8 m. Note, in comparison, the equivalent hole size considered by Westinghouse for the massive flow case is 1.0 m in diameter.

Other parametric sensitivity calculations addressed the sensitivity of code calculated loads to subcooled water in the cavity, temperature of the melt pour, and composition of the melt pour (metallic versus ceramic). In addition, the sensitivities of the calculated loads to the variations in the uncertain model parameters (i.e., the particle diameter, the maximum rate of fragmentation per particle in ESPROSE.m, and the fragmentation rate constant in TEXAS) were also studied. The results of the study are summarized in Table 19.2-4 of this report.

Because some of the loadings calculated by the sensitivity studies exceeded the loading used by Westinghouse to assess the structural integrity of the containment liner, the impact of a 644 kPa-s impulsive loading on the cavity floor and a 670 kPa-s impulsive loading on the lower head of the RPV was evaluated. The staff estimated that a loading of 644 kPa-s would produce less than 5 percent elongation on the steel containment vessel. Therefore, the staff concludes that the embedded steel plate of the containment vessel would remain intact for the sensitivity cases which bound the base case scenarios. Assuming the RPV supports are unavailable an impulsive load of 670 kPa-s would raise the vessel 55.4 ft. Although this impulsive load would raise the RPV above the refueling pool, it would not hit the top of containment and would most likely be stopped by the missile shield above the refueling pool. Therefore, the staff concludes that the RPV exposed to such impulse loadings would not impact the containment vessel.

Based on the above discussion, the staff concludes that the structural integrity of the concrete cavity floor and wall would not be retained, but that the structural integrity of the steel containment vessel would be maintained given the staff's best estimate ex-vessel steam explosion. Because the embedded steel plate of the containment vessel remains intact for the best estimate ex-vessel steam explosion loading and various sensitivity cases, the staff finds the ability of the AP600 design to accommodate an ex-vessel steam explosion acceptable,

relative to the containment performance goal. Therefore, the guidance, provided in SECY-93-087, pertaining to the interaction between molten fuel and coolant has been satisfied and DSER Open Item 19.2.3.3-6 is closed.

19.2.3.3.6 Containment Bypass

Severe accident containment bypass for the AP600 includes three issues: (1) interfacing system LOCAs (ISLOCA) outside containment, (2) steam generator tube rupture (SGTR) events leading to offsite releases through the steam generator relief valves, and (3) containment integrity failure during a severe accident scenario. In the DSER, the staff indicated that Westinghouse should address the issue of containment bypass resulting from SGTR events in accordance with the guidance in SECY-93-087, and address the maintenance of containment integrity during severe accident scenarios. This was identified as DSER Open Item 19.2.3.3-8. The evaluation of design options to minimize containment bypass from SGTR events is addressed below. Containment bypass from SGTR events is discussed in Section 5.4.2.2 of this report. ISLOCA is addressed in Section 19.2.2.1.5 of this report, and maintenance of containment integrity during severe accidents is addressed in Sections 19.2.3.3.7 and 19.2.6 of this report.

In SECY-93-087, the staff recommended that the Commission approve the position to require that the advanced plant designer consider design features to reduce or eliminate containment bypass leakage that could result from SG tube ruptures. The following design features were identified as able to mitigate the releases associated with a tube rupture:

- a highly reliable (closed loop) SG shell-side heat removal system that relies on natural circulation and stored water sources
- a system that returns some of the discharge from the SG relief valve back to the primary containment, and
- increased pressure capacity on the SG shell side with a corresponding increase in the safety valve setpoints

In its July 21, 1993, SRM, the Commission approved the staff's position.

In response, Westinghouse evaluated the following design options as part of their assessment of Severe Accident Mitigation Design Alternatives (SAMDAs) for AP600, and provided the results of their evaluation in Section 1B.7 of the SSAR:

- a passive safety-related heat removal system to the secondary side of the steam generators. The system would provide closed loop cooling of the secondary side using natural circulation and stored water cooling, thus preventing a loss of primary heat sink in the event of a loss of startup feedwater and passive RHR heat exchanger. The system was estimated to reduce risk (for internal events at power) by about 7 percent and cost $1.3 million.
- redirecting the flow from all steam generator safety and relief valves to the IRWST (as well as a lower cost option of this design improvement, consisting of redirecting only the discharge from the first stage safety valve to the IRWST). The system would prevent or

reduce fission product release from bypassing the containment in the event of a SGTR event. The system was estimated to reduce risk by about 6 percent and cost $0.6 million.

- increasing the design pressure of the steam generator secondary side and safety valve setpoint to the degree that a SGTR will not cause the secondary system safety valve to open. This design change would also prevent the release of fission products that bypass the containment via the SGTR. The system was estimated to reduce risk by about 6 percent and cost $8.2 million.

In Section 19.4 of this report, the staff indicates that on the basis of the estimated CDF and risk from internal events in the AP600 design, any potential design modifications for accident mitigation that cost more than about $500 would not be cost effective, even if the modifications were to totally eliminate all offsite consequences. If the baseline core damage frequency is increased by a factor of 100 to account for external events and other accident sequences not included in the analysis, and the design modifications completely eliminate all offsite consequences, this value rises to about $50,000. The above design changes involve a major redesign effort, pose serious design drawbacks and are prohibitively expensive. In view of the low residual risk for AP600 and the significant costs associated with the aforementioned design changes, the staff concludes that the risk reduction offered by the design changes is not significant, and that the design changes are impractical and would excessively impact on the plant.

In Section 19.1.3.1.2 of this report, the staff concludes that preventive and mitigative features in the AP600 design result in a reduction in the estimated CDF for SGTR sequences to about 6E-09/y. In Section 15.6.3 of this report the staff concludes that there is reasonable assurance that SGTR events pose no undue threat to the public health and safety. The staff further concludes that the three design alternatives identified in SECY-93-087 have been adequately assessed and that the criteria of SECY-93-087 have been met. This resolves DSER Open Item 19.2.3.3-8.

19.2.3.3.7 Equipment Survivability

The purpose of this section is to discuss the survivability of equipment, both electrical and mechanical, that is needed to prevent and mitigate the consequences of severe accidents. Westinghouse addressed equipment survivability in Appendix D to the PRA.

Safety-related equipment, both electrical and mechanical, must perform its safety function during design bases events. Section 3.11 of the AP600 SSAR defines the environmental conditions with respect to limiting design conditions for all safety-related mechanical and electrical equipment. The common terminology used for the level of assurance provided for equipment necessary for design bases events is "environmental qualification" or "equipment qualification."

Beyond design-basis events can generally be categorized into in-vessel and ex-vessel severe accidents. The environmental conditions resulting from these events are generally more limiting than those from design bases events. The NRC established a criterion to provide a reasonable level of confidence that the necessary equipment will function in the severe accident

environment for the time span for which it is needed. This criterion is commonly referred to as "equipment survivability" and is fundamentally different from equipment qualification.

SECY-93-087 indicated that the staff would evaluate the ALWR vendor's identification of equipment needed to perform mitigative functions and the conditions under which the mitigative systems must operate. In SECY-93-087, the staff recommended that the Commission approve the staff's position that passive plant design features provided only for severe accident mitigation need not be subject to the 10 CFR 50.49 environmental qualification requirements; 10 CFR Part 50, Appendix B quality assurance requirements; and 10 CFR Part 50, Appendix A redundancy/diversity requirements. The staff concluded that guidance such as that found in Appendices A and B of RG 1.155, "Station Blackout," is appropriate for equipment used to mitigate the consequences of severe accidents. In the SRM dated July 21, 1993, the Commission approved the staff's position.

The applicable criterion for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents is provided in 10 CFR 50.34(f).

- In Part 50.34(f)(2)(ix)(C), the NRC states that equipment necessary for achieving and maintaining safe shutdown of the plant and maintaining containment integrity will perform its safety function during and after being exposed to the environmental conditions attendant with the release of hydrogen generated by the equivalent of a 100 percent fuel-clad metal-water reaction including the environmental conditions created by activation of the hydrogen control system.

- In Part 50.34(f)(3)(v), the NRC states that systems necessary to ensure containment integrity shall be demonstrated to perform their function under conditions associated with an accident that releases hydrogen generated from 100 percent fuel-clad metal-water reaction.

- In Part 50.34(f)(2)(xvii), the NRC requires instrumentation to measure containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity, and noble gas effluents at all potential accident release points.

- In Part 50.34(f)(2)(xix), the NRC requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

These regulations collectively indicate the need to perform a systematic evaluation of all equipment, both electrical and mechanical, and instrumentation to ensure its survivability for intervention into an in-vessel severe accident. At the time of the DSER Westinghouse had not provided this information. This was identified as DSER Open Item 19.2.3.3-9.

The staff requested that Westinghouse provide the results of an evaluation using best-estimate means of a degraded in-vessel core damage accident that results in a 100 percent metal-water reaction. The foundation for the evaluation was to be included. The evaluation was to identify the most likely sequences resulting in substantial oxidation of the fuel cladding as a result of the probabilistic safety assessment. An example of an acceptable sequence would involve accident conditions in which emergency core cooling system performance is degraded for a sufficient time to cause cladding oxidation but is later recovered to ensure a safe shutdown. If the analysis assumes an intact primary loop, the basis for this was to be supported by the

results of the probabilistic safety assessment (i.e., LOCA does not contribute significantly to core melt). The impact on the reactor system and containment system from the pressure, temperature, and radiation released was to be evaluated. Plots showing pressure and temperature as a function of time were requested.

If the in-vessel severe accident environment has no effect on the equipment performance, this was to be clearly indicated along with the supporting rationale. Examples of such instances include cases in which the equipment has already performed its function before the onset of the accident conditions or the equipment is located in an area not exposed to the environmental conditions, such as being located outside the primary containment. For equipment in which environmental conditions as a result of the in-vessel severe accident are in excess of the equipment qualification range, an engineering rationale was to be developed as to why the equipment would survive the environment for the needed time span. This rationale could include such factors as limited time period in the environment; the use of similar equipment in commercial industry exposed to the same environment; the use of analytical extrapolations; or the results of tests performed in the nuclear industry or at national laboratories.

With respect to instrumentation requirements, sufficient instrumentation should exist to inform operators of the status of the reactor and the containment at all times as the in-vessel severe accident is intended to be recoverable from and lead to safe shutdown with containment integrity maintained. The emergency response guidelines (ERGs) direct specific manual operator actions determined by instrumentation readings and as such all instrumentation should exist where manual operator actions are specified within the ERGs.

Some or all of the instrumentation may be designed to survive the environment specified in RG 1.97. However, RG 1.97 only ensures that the instrumentation will survive in the worst environment resulting from a design bases event and not a severe accident. Therefore, an engineering rationale was requested to justify why the instrumentation would survive the environment. This rationale could include such factors as limited time period in the environment; the use of similar equipment in commercial industry exposed to the same environment; the use of analytical extrapolations; or the results of tests performed in the nuclear industry or at national laboratories.

The applicable criteria for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents is discussed in the "Equipment Survivability" section of SECY-93-087. Mitigative features should be designed to provide reasonable assurance that they will operate in the severe-accident environment for which they are intended and over the time span for which they are needed. In cases where safety-related equipment (equipment provided for DBAs) is relied upon to cope with severe accident situations, there should be reasonable assurance that this equipment will survive accident conditions for the period that is needed to perform its intended function.

According to SECY-93-087, Westinghouse was to review the various severe accident scenarios analyzed and identify the equipment needed to perform various functions during a severe accident and the environmental conditions under which the equipment must function. Equipment survivability expectations under severe accident conditions should include consideration of the circumstances of applicable initiating events (e.g., SBO and earthquakes)

and the environment (e.g., pressure, temperature and radiation) in which the equipment is relied upon to function.

The staff requested that Westinghouse provide an evaluation of the dominant accident sequences. For each accident sequence, Westinghouse was to identify the mitigative features. In addition, the specific environment profile (pressure, temperature, radiation fields) was to be specified. This was to include the environment associated with a hydrogen burn. For each mitigative feature, an assessment of survivability was to be done using ground rules similar to those specified for in-vessel accidents.

With respect to instrumentation requirements, sufficient instrumentation was to be identified to inform operators of the status of the containment at all times. This instrumentation was to provide the status of the reactor during the early stages of the accident to verify reactor failure at low pressure.

Some or all of the identified instrumentation may be designed to survive the environment specified in RG 1.97. However, RG 1.97 only ensures that the instrumentation will survive in the worst environment resulting from a design bases event and not from a severe accident. Therefore, Westinghouse was to provide an engineering rationale to justify why the identified instrumentation would survive the more severe environment. This rationale could include such factors as limited time period in the environment; the use of similar equipment in commercial industry exposed to the same environment; the use of analytical extrapolations; or the results of tests performed in the nuclear industry or at national laboratories.

19.2.3.3.7.1 Equipment and Instrumentation Necessary to Survive

Westinghouse reviewed the actions defined by the AP600 Emergency Response Guidelines, Revision 3, May 1997, and WCAP-13914, "Framework for AP600 Severe Accident Management Guidance (SAMG)," Revision 1, November 1996 to determine the equipment and instrumentation needed for achieving a controlled, stable state. In WCAP-13914, Westinghouse defines a controlled, stable core state and a controlled, stable containment state. The core state can be summarized as having a process for transferring the energy being generated in the core to a long-term heat sink such as a flooded reactor cavity. The conditions associated with this state are considered indicative of a degraded in-vessel core damage accident. The containment state can be summarized as having a process for transferring the energy that is released to an intact containment to a long-term heat sink such as the PCCS. The conditions associated with this state are considered indicative of an ex-vessel severe accident.

As a result of this review, Westinghouse determined that the necessary equipment and instrumentation along with the environmental conditions varied over the course of a severe accident. Therefore, Westinghouse identified four equipment survivability time frames. Time Frame 0 is defined as the period of time in the accident sequence after accident initiation and before core uncovery. Time Frame 1 is defined as the period of time after core uncovery and before the onset of significant core damage as evidenced by the rapid oxidation of the core. Time Frame 2 is the period of time in the severe accident after the accident progresses beyond the design basis of the plant and before the establishment of a controlled, stable core state or before reactor vessel failure. Time Frame 3 is defined as the period of time after the reactor vessel fails until the establishment of a controlled, stable containment state or the end of the

sequence. The equipment and instrumentation needed for each time frame are summarized in Tables D.6-2 through D.6-4 of the AP600 PRA . The staff also performed a review of the AP600 Emergency Response Guidelines and the AP600 SAMG to confirm the equipment and instrumentation identified in Tables D.6-2 through D.6-4 of the AP600 PRA.

The equipment listed provides the operator with the ability to (1) inject into the RCS, steam generators and containment, (2) depressurize the RCS, steam generators and containment, (3) control hydrogen, (4) isolate containment, and (5) remove heat and fission products from the containment atmosphere. The list of equipment also includes the cavity flooding system and the containment penetrations. The instrumentation was chosen so that the operator could confirm and trend the results of actions taken and that adequate information would be available for those responsible for making accident management decisions.

The staff performed an independent assessment of the list of equipment and instrumentation provided in Tables D.6-2 through D.6-4 and compared them to the more extensive lists required by RG 1.97 and 10 CFR 50.34(f) to ensure that the equipment and instrumentation provided is sufficient. The staff concludes that the equipment and instrumentation needed to perform and monitor the mitigative functions necessary during a severe accident are adequate.

19.2.3.3.7.2 Severe Accident Environmental Conditions

Westinghouse used the MAAP4 computer code (version 4.0.2) to support the quantification of the four equipment survivability time frames and the severe accident environment within each time frame. Two basic sequences and four sensitivity cases for each base sequence were quantified to establish the environments including hydrogen combustion in the containment. Each sequence's input data was adjusted to assure that a 100 percent fuel-clad metal-water reaction occurred so that the required bounding hydrogen source was considered.

The two base sequences were a large 0.2 $m^2$ (2.2 $ft^2$) hot-leg break into a steam generator compartment and a 10.2-cm (4-in.) DVI line break in a valve vault room. For each of these LOCA sequences, four sensitivity cases were run to determine the effects of cavity flooding, core-concrete interaction, igniters (local burn versus global burn) and jet burning of the heated hydrogen-rich RCS gas discharge.

The key event timing for each of the sequences is summarized in Table D.7-2 of the SSAR. These key events in the severe accident progression directly relate to the equipment survivability time frames. Time Frame 0 is defined as the period of time in the accident sequence after accident initiation and before core uncovery. Time Frame 1 is defined as the period of time after core uncovery and a core exit gas temperature exceeding 1367 K (2000°F) which is indicative of rapid oxidation of the core. Time Frame 2 is the interval between the core exit gas temperature exceeding 1367 K (2000 °F) and either the end of core material relocation into the lower head or vessel failure. Time Frame 3 is the interval between vessel failure and the end of the sequence.

The MAAP4 results provide the containment environment associated with the combustion of hydrogen resulting from the equivalent of 100 percent oxidation of the active fuel cladding where (1) igniters are functioning (local burning scenario), (2) igniters were artificially defeated (global burning scenario), and (3) jet burning and igniters were defeated (global burning

scenario). To calculate more severe bounding containment environments, cavity flooding was defeated in some sequences resulting in ex-vessel hydrogen generation as a result of core-concrete interaction. However, Westinghouse failed to identify the regions of active burning caused by diffusion flames or igniters in the global and local burning scenarios. Equipment or instrumentation located within these regions could be exposed to thermal environments more severe than the three discussed above. Table D.8-1 of the SSAR assessed the impact of sustained burning on the equipment and instrumentation to be used in Time Frames 2 and 3. One area found to be impacted by diffusion flames was the containment shell near the IRWST. The staff finds the design of the containment shell near the IRWST vents acceptable because igniters have been provided inside the IRWST, a PAR is to be installed in an IRWST vent, actuation of the fourth stage of the ADS reduces the build up of hydrogen inside the IRWST, and radiative shielding would diminish heat transfer across the containment shell, thereby, impacting PCCS performance.

The results of the DVI line break sequences are very similar to the hot-leg large LOCA results because the ADS fourth stage valves are opened in both sequences. The peak temperature calculated in the upper plenum gas was about 1800 K (2780°F). Since these sequences are low pressure sequences with the ADS fourth stage valves open, the gas temperature in the pressurizer stayed below the nominal temperature 625 K (665 °F) for most of the transient in all of the analyzed sequences. The gas temperatures in both steam generators stayed below 570 K (566 °F) for all of the analyzed sequences because water was present in the secondary side of both steam generators. Figures D.7.1-1 through D.7.1-6 of the PRA show gas temperatures in the containment compartments, the containment pressure and the RPV pressure.

The staff, through its contractor at SNL, analyzed with its computer model, MELCOR, the 3BE-FRF1 sequence to confirm the results of the Westinghouse computer model, MAAP 4, to predict the environmental conditions attendant with a severe accident. On the basis of this confirmation, the staff concludes that the thermal hydraulic profiles predicted above by MAAP are acceptable approximations of the environmental conditions for which mitigative features and instrumentation, identified in this section, must survive.

The radiation exposure inside the containment for a severe accident is estimated by considering the dose in the middle of the AP600 containment with no credit for the shielding provided by internal structures. The instantaneous gamma and beta dose rates are provided in SSAR Figures D.7.0-1 and D.7.0-2. The source term is based on the emergency safeguards system core thermal power rating of 1,972 MWt.

The radionuclide groups and elemental release fractions are consistent with the accident source term presented in NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," February 1995. The timing of the release is founded on NUREG-1465 assumptions. Westinghouse assumes an initial release of activity from the gaps of a number of failed fuel rods at 10 minutes into the accident. The instantaneous release of 3 percent of the core inventory of the noble gases, iodine and cesium. Over the next 30 minutes following the instantaneous gap activity release from 10 to 40 minutes into the accident, an additional 2 percent of the core inventory is added. At this point, 5 percent of the total core inventory of volatile species has been assumed to be released. During the early in-vessel release phase, the fuel as well as other structural materials in the core reach sufficiently high temperatures that the reactor core geometry is no longer maintained and fuel and other materials melt and

relocate to the bottom of the reactor vessel. The in-vessel phase is estimated to last 1.3 hours. The ex-vessel release phase begins when molten core debris exits the reactor pressure vessel and ends when the debris has cooled sufficiently that significant quantities of fission products are no longer being released. The ex-vessel phase is expected to last 2 hours. The staff finds the timing and duration for the early in-vessel, late in-vessel, and ex-vessel release phases acceptable because they are consistent with NUREG-1465.

19.2.3.3.7.3 Basis for Acceptability

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the staff evaluate the ALWR vendor's review of the various severe accident scenarios analyzed and identify the equipment needed to perform its function during a severe accident and the environmental conditions under which the equipment must function. In its July 21, 1993 SRM, the Commission approved the staff's position.

The staff has performed this evaluation and concludes that the equipment and instrumentation identified by Westinghouse in Tables D.6-2, D.6-3, and D.6-4 of the PRA and the applicable environments described in Section 19.2.3.3.7.2 of this report meets the above guidance of SECY-93-087 and 10 CFR 50.34(f) as delineated in Section 19.2.3.3.7 of this report. Reasonable assurance that the equipment and instrumentation identified in this section will operate in the severe accident environment for which they are intended and over the time span for which they are needed is provided by the environmental qualification ITAAC and because of a COL Action Item. Specifically, the COL applicant referencing the AP600 certified design will perform a thermal lag assessment of the as-built equipment used to mitigate severe accidents to provide additional assurance that this equipment can perform its severe accident functions during environmental conditions resulting from hydrogen burns. This assessment is COL Action Item 19.2.3.3.7-1. This resolves DSER Open Item 19.2.3.3.3-9.

19.2.3.3.8 Containment Vent Penetration

Use of a containment vent to prevent containment over-pressure failure is a means of mitigating the consequences of a severe accident. The staff was still evaluating the need for a containment vent for the AP600 design at the time of the DSER. Accordingly, this was identified as DSER Open Item 19.2.3.3-10.

In SECY-93-087, the staff indicated that the need for a containment vent for the passive plant designs would be evaluated on a design-specific basis, and that if acceptable analyses indicate that a vent would not be needed to meet the severe accident criteria, such as the Commission's containment performance goal discussed in Section 19.2.4 of this report, the staff would not propose to implement a vent requirement.

The staff relied on the evaluation of the containment performance goal in Section 19.2.4 of this report for determining the need for inclusion of a containment vent. As discussed therein, for the most likely severe accident challenges, containment pressure would remain below Service Level C as a result of successful retention of core debris in-vessel, and operation of PCS. Accordingly, containment venting will not be required for the more likely severe accident sequences since they do not result in over-pressure failure.

The staff identified two situations in which venting would eventually be required, specifically, events involving either RPV failure followed by unmitigated CCI, or failure of PCS as a result of blockage of the annulus drain valves. However, these events are much less likely, and do not contribute appreciably to containment failure frequency, as discussed below.

In the event of PCS drain valve blockage, containment pressure would reach Service Level C in about 30 hours, necessitating containment venting (see Section 19.1.3.2.2). In the baseline PRA, the probability of PCS drain valve blockage is estimated to be 1E-04, and the corresponding containment failure frequency is estimated to be 1.5E-11/y. In the event of RPV failure followed by unmitigated CCI, containment pressure would reach Service Level C in about 3 to 11 days depending on the type of concrete used in the basemat (see Section 19.2.3.3.3). The frequency of core damage with RPV failure and relocation of core debris to the reactor cavity is 7E-09/y in the baseline PRA, on the basis of an assumption that RCS depressurization and reactor cavity flooding always result in successful retention of molten core debris in-vessel. As discussed in Section 19.2.3.3.1, the staff's review of ERVC supports this assumption for the core debris configuration considered in the related ROAAM analysis, but identified several alternative debris bed configurations that, if achieved for a sufficient period of time, would lead to thermal loads that could fail the RPV. Uncertainties in the likelihood of forming such debris bed configurations are large because of the inherent limitations in the modeling of core melt progression/relocation and lower head debris bed behavior. Under the most limiting assumption of no credit for ERVC, the frequency of events that result involving reactor vessel failure would approach the core melt frequency. However, the frequency of events that require containment venting would be somewhat less than this since the reactor cavity would be flooded in these sequences, potentially resulting in quenching of the core debris and termination of CCI.

The frequency of events that would necessitate containment venting is on the order of 1E-08/y founded on the PRA for internal events. This frequency could increase substantially if ERVC is not effective in preventing RPV failure. However, even with no credit for ERVC, the frequency of events requiring venting would be on the order of 1E-07/y and well below the Commission's 1E-06/y large release frequency goal. The staff concludes that the containment performance goals regarding large release frequency and CCFP are met without a containment vent, and therefore, a containment vent is not required for the AP600 design. This resolves DSER Open Item 19.2.3.3-10.

Although containment venting capability is not required to meet the containment performance goals it may be beneficial to depressurize the containment in a controlled manner under certain conditions during a severe accident. In this regard, the AP600 designers have identified a containment vent path that can be used to control containment pressure in the unlikely event of long-term over-pressurization of containment. Specifically, with the RCS depressurized and open to the containment atmosphere via either the ADS or the reactor vessel breach, the containment may be vented to the spent fuel pool via the residual heat removal suction lines. The manual valve from the spent fuel pool to the RNS pump suction would be opened and then the RNS hot-leg suction isolation valves operated remotely to control the vent process. The COL applicant, as part of COL Action Item 19.2.5-1 regarding accident management, will develop detailed procedures for use of the containment vent system.

19.2.3.3.9 Non-Safety-Related Containment Spray

Performance of numerous risk assessment studies over the past 20 years show that the risk to the public from severe accidents is usually dominated by accidents that result in early containment failure commensurate with a significant release of radioactive material. Many design features have been added to the AP600 design to reduce this risk. Examples include allowing for depressurization of the reactor coolant system, controlling hydrogen generation, and cooling of molten core debris in-vessel. The large passively-cooled AP600 containment provides significant benefit to cope with severe accident challenges because the failure modes of the containment heat removal system are independent of the scenarios that could lead to containment challenges and of the vulnerabilities associated with reliance on human actions. While the use of passive systems enhances the safety of the plant during early containment challenges, the ability to intervene and provide control over the course of a severe accident has significant benefit in terms of accident management. For existing plants an internal containment spray system and other features can accomplish this. However, the AP600 relies solely on enhanced natural processes for aerosol fission product removal. The state-of-the-science for evaluating the effectiveness of natural removal processes in harsh environments has uncertainty levels that are greater than those for current operating plants that do not credit these processes.

The concept of passive safety systems is appealing because the design relies primarily on gravity. Passive safety system designs are also attractive because they minimize the need for support systems and reduce reliance on human actions. However, there are uncertainties regarding the performance of passive safety systems. Net driving forces are small compared to active systems. For example, the reliability and functionality of check valves can no longer be taken for granted in passive designs. While a sticking check valve in an active system can be easily overcome by the forces developed by a pump, there is less assurance that the low driving head developed by gravity injection in a passive design will similarly overcome a sticky check valve. In addition, the parallel flow paths existing in the AP600, combined with the low driving heads, make calculation of flow distributions more uncertain. Although the staff is confident that, within the design basis, the testing program data and conservatisms inherent in design basis analyses bound these uncertainties, the uncertainties become much more significant when considering severe accidents.

In the unlikely event that a severe accident in the AP600 occurs, the cause is likely to be some combination of events and passive system failures that had not been specifically evaluated or assessed. Assuming the failure of the passive core cooling system features, the containment becomes the primary mitigation system to protect public health and safety. As with other passive systems, there are large uncertainties associated with the passive nature of the containment system design. Heat transfer and fission product removal from the AP600 containment atmosphere is dependent upon mass condensation onto cool surfaces, predominantly the walls inside containment. Given a severe accident, the long-term buildup and distribution of non-condensible gases within the containment and their effects (as a result of stratification and increasing concentration gradients within the inner containment boundary layer) cannot be assessed with existing analytical tools.

In view of the uncertainties associated with the reliance on passive systems in mitigating severe accidents and the advantages of having operator intervention as part of the design's accident

management strategy, the staff recommended to the Commission that the AP600 design should include additional system(s). The staff made this recommendation in SECY-96-128 and in a supporting clarification letter to the Commission that was dated November 12, 1996. The staff went on to say that one way to meet this position was through the incorporation of a containment spray system that injects internally to the containment.

The Commission, in its SRM, dated January 15, 1997, did not support the staff's request for the inclusion of additional system(s) for accident management and mitigation following a severe accident because the basic design and performance requirements had not been bounded or specified. The staff provided the Commission with additional information regarding the type of non-safety-related system that would achieve an appropriate balance between prevention and mitigation of severe accidents for the AP600 design in SECY-97-044. To achieve this balance, the staff envisioned a simple containment spray system, which injects into the containment without dedicated pumps and heat exchangers. In its SRM, dated June 30, 1997, the Commission approved the staff's recommendation that, on the basis of the impact of the uncertainties associated with the performance of passive safety systems, the AP600 include a containment spray system or equivalent for accident management following a severe accident.

In response to SECY-97-044, Westinghouse included a containment spray function for accident management following a severe accident as part of the AP600 fire protection system design. This design feature is not safety-related and is not credited in any accident analysis including the dose analysis provided in Section 15.6.5 of the SSAR. In Section 9.5.1 of the SSAR, Westinghouse provides a description of the fire protection system including equipment and valves that support the containment spray function.

The secondary fire protection system water tank provides the source of water for the containment spray function. Either the motor driven or diesel driven fire protection system pump may be used to deliver fire water to the containment spray header. The containment spray header consists of a single header that feeds two ring headers located above the polar crane. The ring headers and spray nozzles are oriented to maximize containment volume coverage. Figure 6.5.1 of the SSAR shows the cross sectional area of the containment building covered by the spray. The total free volume of the sprayed region is approximately 4.0E+04 $m^3$ (1.4E+06 $ft^3$) which represents approximately 83 percent of the total containment free volume.

Westinghouse states in Section 6.5.2 of the SSAR that the fire protection system header can provide the design flow rate of 57.5 L/min (15.2 gpm) to each spray nozzle at a containment backpressure of 20 psig for a total containment spray flow of approximately 3914.1 L/min (1034 gpm). The staff finds the assumed containment backpressure of 20 psig to be reasonable on the basis of Westinghouse's and the staff's analyses of severe accident sequences that show the long term containment backpressure is on the order of 10 to 20 psig. The fire protection system header has been designed to provide a containment spray nozzle differential pressure of 40 psid, which fixes the drop size distribution. Westinghouse assumes the mass mean drop size produced at this differential pressure to be 1000 microns.

Westinghouse estimates the aerosol removal coefficient for the containment sprays to be 2.6 $hr^{-1}$ in the sprayed volume on the basis of the equation given in SRP Section 6.5.2-III(4)(c)(4). Westinghouse assumed a nominal spray flow height of 100 feet, a nominal flow rate of 1,000 gpm, and a value for E/d of 3.05 $ft^{-1}$. E/d is the ratio of a dimensionless collection efficiency E to the average spray drop diameter. A value for E/d of 3.05 $ft^{-1}$ is only conservative

initially. The SRP states that E/d should change abruptly to .305 $ft^{-1}$ after the aerosol mass has been depleted by a factor of 50. The staff finds the use of 3.05 $ft^{-1}$ for E/d and this estimate acceptable because the sprays are expected to be pulsed over short time periods in order to limit their impact on the containment sump inventory.

The possibility of inadvertent actuations of the containment spray system is evaluated in Section 6.2.1.1.4, "External Pressure Analysis," of this report.

Use of the containment spray system requires multiple operator actions outside the main control room MCR. These actions include dispatching a crew to the auxiliary building, local alignment of certain valves, and starting the firewater system pumps. AS discussed in Section 6.5.2.1.1 of the SSAR the manual valves outside containment are located in valve piping penetration room 12306. The valves are located close to the entrance door such that radiation exposures to an individual required to enter the room and align the valves would not exceed the prescribed post-accident dose limits discussed in Section 12.4.1.8 of the SSAR.

The staff finds that the containment spray system proposed by Westinghouse provides the following benefits and, thereby, satisfies the staff's recommendation in SECY-97-044:

(1) the capability for site personnel upon recognition of elevated radiation levels in the containment atmosphere to quickly and substantially remove aerosol fission products following activation

(2) mixing the containment atmosphere following a severe accident, especially the boundary layer inside the containment shell

(3) short term pressure reduction upon injection because of the heat capacity of the subcooled spray water

19.2.4 Containment Performance Goal

The containment performance goal (CPG) is intended to ensure that the containment structure has a high probably of withstanding the loads associated with severe accident phenomena, and that the potential for significant radioactive releases from containment is small. The CPG includes both a deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges, and a probabilistic goal that the conditional containment failure probability (CCFP) be less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA. At the time of the DSER, the staff had not completed its evaluation of containment performance. Hence, this issue was identified as DSER Open Item 19.2.4-1.

In SECY-93-087, the staff recommended that the Commission approve the following deterministic containment performance goal for the passive ALWRs:

> The containment should maintain its role as a reliable, leak-tight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage

under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

In discussions during the Commission meeting on this subject, the staff informed the Commission that it also intends to continue to apply the probabilistic containment performance goal of 0.1 CCFP in implementing the Commission's defense-in-depth regulatory philosophy and the Commission's policy on Safety Goals. (The 0.1 CCFP goal had been proposed by the staff for evolutionary designs in SECY-90-016, and approved by the Commission in its SRM of June 26, 1990.)

In the SRM dated July 21, 1993, the Commission approved the staff's position to use the deterministic CPG in the evaluation of the passive ALWRs as a complement to the CCFP approach, subject to the staff's review and recommendations resulting from public comments on the "Advance Notice of Proposed Rulemaking on Severe Accident Plant Performance Criteria for Future ALWRs." In SECY-93-226, "Public Comments on 57 FR 44513 - Proposed Rule on ALWR Severe Accident Performance", the staff provided the Commission with a summary of public comments received regarding the ANPR, and recommendations regarding policy issues raised in these comments. On the basis of a review of these comments and experience gained from the evaluation of the evolutionary reactor designs, the staff concluded that use of both a deterministic and probabilistic containment performance goal should be pursued for the passive reactor designs. Accordingly, the staff has considered both the deterministic and probabilistic CPGs in assessing the performance of the AP600 containment.

Deterministic Containment Performance Goal

The staff used the deterministic containment performance criteria to confirm that an acceptable level of containment performance has been achieved. For purposes of this evaluation, containment failure was defined as events in which the containment fails to maintain its role as a reliable, leak-tight barrier for approximately 24 hours following the onset of core damage, or following this period, fails to continue to provide a barrier against uncontrolled release of fission products. Containment was assumed to fail if any of the following conditions occur (even if the conditions occur after 24 hours):

- internal pressure exceeds the value associated with ASME Code Service Level C Limits
- the containment is bypassed, such as in SGTR and ISLOCA events
- the containment fails to isolate
- containment seal materials fail as a result of over-temperature
- molten core debris melts through the concrete basemat into the subsoil

Controlled venting of containment would not constitute containment failure provided venting occurs after approximately 24 hours following onset of core damage.

On the basis of the Level 2 PRA results, the more likely severe accident challenges are defined by sequences in which the RCS is fully depressurized, the reactor cavity is flooded, the reactor vessel is reflooded and intact, the containment is isolated, and the PCS and hydrogen igniter systems are operable. (Such sequences represent more than 90 percent of the core damage frequency). Each of these sequence characteristics is directly attributable to corresponding safety-grade features incorporated in the AP600 design, and the very low contribution of station

blackout sequences to core damage frequency. Westinghouse predicted the peak containment pressure for these sequences to be on the order of 30 psig, and the long-term pressure to be on the order of 10 to 20 psig.

All relevant severe accident challenges were evaluated for the these sequences, including hydrogen combustion, high pressure melt ejection, temperature-induced creep rupture of steam generator tubes, fuel-coolant interactions, and core-concrete interactions. These phenomena do not contribute to containment over-pressure or over-temperature failure because of operation of the safety systems incorporated in the AP600 design. Specifically, operation of the hydrogen igniter system produces peak hydrogen burn pressures well below Service Level C, and eliminates the potential for deflagration-to-detonation transitions. RCS depressurization eliminates high pressure melt ejection and temperature-induced SGTR challenges, and terminates fission product releases to the environment in SGTR and ISLOCA events. Reactor cavity flooding, in conjunction with RCS depressurization, provides reasonable assurance that core debris will be retained within the reactor vessel, thereby preventing ex-vessel FCIs, core concrete interactions/basemat melt-through, and long-term over-pressurization of containment. The operation of PCS, in conjunction with reactor cavity flooding, maintains containment pressure below Service Level C and containment temperature below levels where over-temperature failure would be a concern. Finally, core damage events involving failure of containment isolation account for less than one percent of the total core damage frequency in the baseline and focussed PRA.

For the less likely events in which these safety-grade systems do not operate, the probability of containment failure from the associated severe accident phenomena is assessed in the Level 2 PRA and in separate deterministic calculations of each phenomena described elsewhere in Section 19.2 of this report, i.e., hydrogen combustion (Section 19.2.3.3.2), high pressure melt ejection (Section 19.2.3.3.4), ex-vessel FCI (Section 19.2.3.3.5.2), and core concrete interactions (Section 19.2.3.3.3). The results of these assessments indicate that the containment is generally capable of withstanding the challenges from these phenomena, with a small attendant probability of containment failure. The probability of containment failure is addressed below in the context of the probabilistic containment performance goal. The contribution of the various phenomena to the overall containment failure frequency is described further in Section 19.1.3.2.2 of this report.

On the basis of the availability of the severe accident mitigation design features in the majority of the core damage sequences, and the ability of the containment to accommodate the corresponding severe accident loads, the staff concludes that the AP600 containment will maintain its role as a reliable, leak-tight barrier for the more likely severe accident challenges, in accordance with the deterministic containment performance goal.

Probabilistic Containment Performance Goal

The staff used the probabilistic containment performance criteria to confirm that an acceptable level of containment performance has been achieved, and to identify important contributors to containment failure. For purposes of calculating containment failure frequency, containment failure was defined as above, with the exception that containment over-pressure failure was on the basis of a plant-specific containment failure probability distribution (containment fragility curve) rather than the Service Level C Limit. Using this approach, the probability of

containment failure reflects best-estimate structural capabilities and associated uncertainties rather than the more conservative assumption that containment failure occurs whenever Service Level C is exceeded. A large early release frequency goal of 1E-06/y and a conditional containment failure probability goal of 10 percent were used as points of reference for the probabilistic assessment. As described in Section 19.1.3.2, essentially all of the containment failure frequency (98 percent) is the result of either containment bypass or early containment failure. Thus, containment failure frequency and large early release frequency are equivalent in this application.

The containment failure frequency for internal events is 1.8E-08/y in the baseline PRA, which is nearly two orders of magnitude below the large early release goal. The corresponding CCFP is 10.8 percent, which is only slightly higher than the CCFP goal. In Section 19.1.3.2.4 the staff discusses the results of the probabilistic assessment and supporting sensitivity analyses. Through these analyses the staff concludes that for reasonable variations in Level 2 input assumptions and CET split fractions, increases in the containment failure frequency and CCFP are limited to a factor of 2 to 5, and the containment failure frequency remains below 1E-07/y. Also, modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency since the bulk of the containment failures in the existing analyses are driven by the frequency of events with failure of RCS depressurization or reactor cavity flooding, rather than the frequency at which containment pressure loads exceed the containment pressure capability.

The staff concludes that the AP600 containment design satisfies the Commission's probabilistic containment performance goal. Specifically, the estimated containment failure frequency in the baseline PRA is well below the large release frequency goal of 1E-06/y. The conditional containment failure probability is only slightly higher than the CCFP goal of 10 percent in the baseline PRA. Although CCFP is exceeded under certain alternative assumptions (e.g., if diffusion flames are assumed to produce containment failure) and in several sensitivity cases, these increases are modest, and the corresponding containment failure frequencies remain well below 1E-06/y. In view of the approximate nature of the containment performance goal, the recognition that PRA results contain considerable uncertainties, and the fact that under more realistic modeling assumptions a large fraction of the containment failures reflected in the calculated CCFP in the baseline PRA would actually involve late basemat melt-throughs (or no containment failures) rather than early releases to the atmosphere, the staff concludes that the AP600 design satisfies the Commission's goals for both large release frequency and CCFP. This resolves DSER Open Item 19.2.4-1.

### 19.2.5 Accident Management

Accident management (AM) encompasses those actions taken during the course of an accident by the plant operating and technical staff to (1) prevent core damage; (2) terminate the progress of core damage if it begins and retain the core within the reactor vessel; (3) maintain containment integrity as long as possible; and (4) minimize offsite releases. AM, in effect, extends the defense-in-depth principle to plant operating staff by extending the operating procedures well beyond the plant design-basis into severe fuel damage regimes, and by making full use of existing plant equipment and operator skills and creativity to terminate severe accidents and limit offsite releases. In the DSER the staff stated that it was still evaluating the issue of accident management for the AP600. This was identified as DSER Open Item 19.2.5-1.

On the basis of PRAs and severe accident analyses for the current generation of operating plants, the NRC staff concluded that the risk associated with severe accidents could be further reduced through improvements to utility accident management capabilities. Although future reactor designs such as the AP600 will have enhanced capabilities for the prevention and mitigation of severe accidents, accident management will remain an important element of defense-in-depth for these designs. However, the increased attention on accident prevention and mitigation in these designs can be expected to alter the scope, focus, and overall importance of accident management relative to that for operating reactors. For example, increased attention on accident prevention and the development of error tolerant designs, can be expected to decrease the need for operator intervention, while increasing the time available for such action if necessary. This will tend to relieve the operators of the need for rapid decisions, and permit a greater reliance on support from outside sources. For longer times after an accident (several hours to several days), human intervention and accident management will continue to be needed.

In SECY-88-147 and Generic Letter 88-20, the staff identified the development of an accident management plan by each operating reactor licensee as a key element of severe accident closure. A description of the major goals, framework, and elements of an accident management plan was subsequently provided in SECY-89-012, "Staff Plans for Accident Management Regulatory and Research Programs," and in an NRC letter to NUMARC dated July 29, 1991. The AM plan provides a framework within the licensee's organization for evaluating information on severe accidents, for preparing and implementing severe accident operating procedures, and for training operators and managers in these procedures.

The nuclear power industry initiated a coordinated program on accident management in 1990. This program involves the development of three major products as follows: (1) a structured method by which utilities may systematically evaluate and enhance their abilities to deal with potential severe accidents, (2) vendor-specific accident management guidelines for use by individual utilities in establishing plant-specific accident management procedures and guidance, and (3) guidance and material to support utility activities related to training in severe accidents. As described in SECY-97-132, "Status of the Integration Plan for Closure of Severe Accident Issues and the Status of Severe Accident Research," the industry accident management program is scheduled for completion in 1998. Using the guidance developed through this program, a plant-specific accident management plan is expected to be implemented at each operating plant as part of an industry initiative.

For both operating and advanced reactors the overall responsibility for AM, including development, implementation, and maintenance of the accident management plan, lies with the nuclear utility, since the utility is ultimately responsible for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. However, the development and implementation of accident management in future reactors involves both the reactor designer and the plant owner/operator, particularly in view of the fact that many of the design details are still to be developed (such as balance of plant equipment and final piping layout). The plant designer is responsible for developing the technical bases for the plant-specific accident management program or plan, whereas the owner/operator is responsible for developing and implementing the complete accident management plan, including those areas beyond the purview of the plant

designer, such as the content and techniques for severe training, and the delineation of decision making responsibilities at a plant specific level.

The COL applicant will develop and submit an accident management plan as part of the COL application. This was previously identified as COL Action Item 19.2.5-1. The plan will provide a commitment to perform a systematic evaluation of the plant's ability to deal with potential severe accidents, and to implement the necessary enhancements within the detailed plant design and organization, including severe accident management guidelines and training. General areas that will be addressed in the plan include the following five items: (1) accident management strategies and implementing procedures, (2) training in severe accidents, (3) guidance and computational tools for technical support, (4) instrumentation, and (5) decision making responsibilities.

All AP600 PRA insights and COL action items that fall within the scope of accident management should be specifically addressed as part of the COL applicant's accident management plan, including:

- development of detailed guidance and procedures for the use of the severe accident features in the AP600 design, including the ADS (manual actuation after core uncovery), the hydrogen igniter system, the reactor cavity flood system, the containment spray system, and containment venting

- development of guidance and procedures on protection of fission product barriers, including:

  - filling the SGs, and avoiding SG depressurization if water is not available, in order to prevent a thermally-induced SGTR

  - depressurizing the RCS and maintaining a secondary side water level covering the SG tubes in order to mitigate fission product releases from a SGTR event

  - using the containment spray system and associated water sources for containment fission product scrubbing in events with intact or vented containments

  - using containment venting to control fission product releases

- development of guidance and procedures for actions that are expected to be taken in the longer-term (post-72 hours), including:

  - using the ancillary ac diesel generators to power the post-accident monitoring system, main control room lighting, and the PCS recirculation pumps

  - aligning and using the PCS recirculation pumps to refill the PCCWST from a mobile water source using power from the ancillary diesel generators

  - changeover of the main control room habitability system from air bottles to circulation using diesel-powered ancillary fans

- water makeup to the spent fuel pool and containment
- reflooding a damaged core which is retained in-vessel

- development of guidance and procedures for actions that may need to be taken in events during shutdown operations, such as actions to flood the reactor cavity
- evaluation of information needed to implement the accident management guidelines, and plant instrumentation that could be used to supply the needed information considering instrumentation availability and survivability under severe accident conditions

Westinghouse has developed a framework to guide the COL applicant in the development of plant-specific AM guidance for the AP600 design. This guidance, documented in WCAP-13914, Revision 3, includes a discussion of severe accident management requirements, the anticipated structure for the decision making process, the goals that must be accomplished for severe accident management, a summary of possible strategies for AP600 severe accident management, and potential adverse impacts of AM strategies. The COL applicant is expected to follow the recommendations provided in WCAP-13914, Revision 3 in developing their plant-specific AM guidance. This is COL Action Item 19.2.5-1.

The staff will review the accident management plan at the COL stage to assure that the evaluation process and commitments proposed by the COL applicant provide an acceptable means of systematically assessing, enhancing, and maintaining AM capabilities, consistent with staff expectations. The COL applicant would subsequently implement the plan and submit the results for staff review before plant operation. This plan should be developed on the basis of the final, as-built plant, the accident management-related information developed by the plant designer, and the accident management program guidance developed for the current generation of operating reactors. As previously discussed this is COL action item 19.2.5-1. This resolves DSER Open Item 19.2.5-1.

19.2.6 Ultimate Pressure Capacity of the Containment

19.2.6.1 Introduction

In Section 3.8.2.4.2 of the SSAR, Revision 23, Westinghouse discussed the ultimate capacity of the steel containment. The purpose of this section of the FSER is to assess Westinghouse's determination of the performance for the AP600 steel containment vessel (SCV) under severe accident conditions against the containment performance criteria contained in SECY-93-087.

In SECY-93-087, the staff recommended that the Commission approve the deterministic containment performance goal that offers protection comparable to evolutionary advanced light water reactors (ALWRs) in the evaluation of passive ALWRs. The staff recommended the following general criterion for containment performance during a severe accident challenge for passive ALWRs:

> The containment should maintain its role as a reliable, leaktight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C Limits for

metal containments, or Factored Load Category for concrete containments) approximately 24 hours following the onset of core damage under the more likely severe accident challenges and following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

In the SRM dated July 21, 1993, the Commission approved the above deterministic containment performance goal in the evaluation of the passive ALWRs as a complement to the CCFP approach approved by the Commission in its SRM of June 26, 1990.

The staff has evaluated the containment ultimate capacity determinations as contained in the AP600 design certification documents, including Revision 23 of the SSAR, Westinghouse's responses to NRC RAIs and other submittals, which include the materials presented and discussed during NRC/Westinghouse meetings. The details of the staff's evaluation are provided as follows.

19.2.6.2 Deterministic Evaluation of Containment Capacity

The objective of this section is to assess the extent to which the AP600 SCV meets the deterministic containment performance goal of SECY-93-087.

19.2.6.2.1 Containment Description

The AP600 SCV is a cylindrical, welded steel, shell structure, designed in accordance with Subsection NE of Section III of the ASME Code. The AP600 SCV consists of a steel cylinder having a diameter of 39.62 m (130 ft) and height of 46.4 m (152 ft-2.5 in), an ellipsoidal upper head, and an ellipsoidal lower head that is fully embedded in concrete. It is constructed of steel plates with a nominal thickness of 4.13 cm (1.625 in). The plate thickness of 4.45 cm (1.75 in) is used to provide allowance for corrosion in the embedment transition region.

The material of construction is SA537, Class 2 carbon steel. Above elevation 30.48 m (100 ft), the containment is designed as an independent, free-standing structure. Below this elevation, the AP600 SCV is encased between the base slab of the internal structures and the shield building foundation. Near the top of the embedded concrete there is a flexible watertight and airtight seal. The AP600 SCV includes the shell, hoop stiffeners, crane girder, equipment hatches, personnel airlocks, penetration assemblies, and miscellaneous appurtenances and attachments. The polar crane is designed to handle loads up to 275 tons during normal refueling. The crane girder and wheel assemblies are designed to support a special 400-ton trolley to be installed and used in the event of steam generator replacement.

19.2.6.2.2 Deterministic Containment Performance Criterion Under Severe Accident Conditions

The staff used the following deterministic containment performance criteria of SECY-93-087 to determine its performance acceptability under severe accident conditions:

- For the first 24 hours after the onset of the core damage accident, Service Level C stress intensity (SI) limits in Subsection NE of Division 1 of Section III of the ASME Boiler and Pressure Vessel Code should not be exceeded.

- For the period 24 hours after the onset of the core damage accident, the ultimate containment capacity analysis will be used to demonstrate that the containment will neither rupture nor collapse under the prevailing accident environment which could lead to an uncontrolled release of radioactivity.

19.2.6.2.3 Containment Pressure Capacity Analysis

Design-Basis Pressure Capacity

On the basis of the evaluations described in the Section 3.8.2 of the SSAR, the AP600 design-basis accident pressure capacity for the containment internal pressurization was determined to be 411.62 kPa (45 psig). The differential pressure limit for containment external pressurization was calculated to be 20.68 kPa (3.0 psid) for normal operating conditions.

Deterministic Ultimate Capacity Analysis

In order to calculate the ultimate internal pressure capacity of the AP600 SCV under postulated severe accidents, Westinghouse evaluated each critical component forming the containment pressure boundary to estimate the maximum pressures at the ambient temperature within the limits of the following stress and buckling criteria:

- deterministic severe accident pressure capacity corresponding to the ASME Service Level C Limits

- best estimate yield capacity corresponding to gross membrane yield with the ASME Code specified minimum yield stress and the von Mises failure criterion and critical buckling for the equipment hatch covers and top head

The cylindrical shell, top head, equipment hatches and covers, personnel airlocks, and mechanical and electrical penetrations are critical SCV components evaluated in the AP600 SSAR for severe accident loadings. These components are evaluated below.

Tensile Stress Evaluation of Shell

Axisymmetric analyses of the cylinder and top head for dead load and internal pressure were performed to determine the pressure at which stresses reach yield at ambient temperature. The analyses assume that the shell is free standing and fixed at elevation 30.48 m (100 ft), where the bottom part of the shell is embedded in concrete. The allowable SI under the ASME Service Level C Limit is equal to yield. At the internal pressure of 411.6 kPa (45 psig), the maximum general membrane hoop stress is 148.9 MPa (21.6 ksi). For the ASME Service Level C SI Limit of 413.7 MPa (60 ksi) at ambient temperature, the maximum allowable pressure is 963.2 kPa (125 psig). This value is confirmed by the staff's independent calculation. The staff's pressure capacity assessment is on the basis of the maximum membrane stress value and does not incorporate detailed evaluation of localized stresses at points of change of geometry and discontinuities.

The critical section is in the cylinder where the general primary membrane SI is the greatest. As a result of the presence of the crane girder, the maximum hoop membrane stress occurring

in the portion of the shell between the tangent line of the top head and the crane girder is reported as 156.5 MPa (22.7 ksi). Under increasing pressure, yielding would initiate at this location at a pressure of 921.8 kPa (119 psig). However, this yielding is localized and would not result in excessive deformation. The ASME Service Level C allows a stress of 1.5 $S_y$ for primary local membrane stresses computed by elastic analyses. These local stresses do not control the maximum Service Level C pressure. As a result of the staff's independent calculations, the use of the pressure of 963.2 kPa (125 psig) at the ambient temperature for the ASME Service Level C Limit is, therefore, acceptable. At a higher temperature of 204.4 °C (400 °F), the corresponding pressure capacity will be 819.6 kPa (104.2 psig) as a result of the reduced yield stress of 344.47 MPa (50 ksi).

For the best estimate yield pressure computation, Westinghouse adopted the von Mises failure criterion instead of the ASME Code SI criterion because the difference between the two criteria is 15 percent when both principal stresses are in tension with the larger equal to twice the smaller. The best estimate yield pressure was calculated as 1.09 MPa (144 psig = 1.15 x 125 psig) at ambient temperature using the ASME Code specified minimum yield stress and the von Mises failure criterion. At the temperature of 204.4 °C (400 °F), the yield pressure was computed as 928.7 kPa (120 psig). Westinghouse used the results of tests of ductile steel materials, such as SA537 steel, to support the validity of the use of the von Mises failure criterion and to show that the ASME Code SI criterion is conservative (Joseph Marin, *Mechanical Behavior of Engineering Materials*, Prentice-Hall, Inc., 1962). It is generally accepted that only the von Mises failure criterion be adopted as a criterion of transition from the elastic to the plastic state (V. Feodosyev, *Strength of Materials*, Mir Publishers, 1968) and this agrees well with test results and is recommended for ductile materials (E. H. Baker et al., *Structural Analysis of Shells*, McGraw-Hill, 1972). Therefore, the use of the von Mises failure criterion with the ASME Code specified minimum yield stress for the calculation of the deterministic best estimate yield capacity of the AP600 SCV is acceptable.

Buckling Evaluation of Top Head from Internal Pressure

The top head is ellipsoidal with a major diameter of 39.6 m (130 ft) and a height of 11.5 m (37 ft-7.5 in). The thickness is 4.1 cm (1.625 in). Westinghouse analyzed the AP600 SCV for the theoretical buckling capacity using the BOSOR-5 computer code, which can treat both large displacement and material nonlinearity.

Using elastic-plastic material properties at the ambient temperature, i.e., a yield stress of 413.7 MPa (60 ksi), and the von Mises failure criterion, the best estimate yielding was determined to start at 1.11 MPa (146 psig) for the top of the crown, and at 1.15 MPa (152 psig) for the knuckle region. These values are confirmed by the staff's independent calculations using the equations given in Ugural, A.C., *Stresses in Plates and Shells*, pp. 211-212, McGraw-Hill, 1981. Therefore, the best estimate yield pressure at the ambient temperature for the top of the crown of 1.11 MPa (146 psig) and for the knuckle region of 1.15 MPa (152 psig) is acceptable.

Westinghouse determined that the theoretical elastic-plastic (or asymmetric) buckling due to internal pressure is 1.3 MPa (174 psig) at the ambient temperature, on the basis of Galletly, G.D., "Buckling and Collapse of Thin Internally Pressurized Dished Ends," Proceedings, Institution of Civil Engineers, Part 2, 1979, Volume 67, September, 607-626, without considering initial imperfection and residual stresses. However, the staff believed that the initial imperfections and residual stresses might reduce this value below 1.3 MPa (174 psig). The

staff requested in the DSER that Westinghouse discuss the basis for not considering the effect of initial imperfections and residual stresses in the determination of the buckling pressure. This was DSER Open Item 19.2.6.2-1.

The applicant responded by stating that the effect of residual stresses and imperfections on the buckling capacity is included in a single capacity reduction factor, which is intended to address all variables that reduce the theoretical buckling capacity. Using BOSOR-5 analysis with an elastic, perfectly-plastic, bi-linear stress-strain curve, the buckling capacity was found to be 1.3 MPa (174 psig) and the buckling occurred in the knuckle region.

The applicant performed an additional BOSOR-5 analysis with stress-strain curves accounting for the effects of residual stresses on the buckling of cylindrical shells as a result of axial compression and/or external pressure. The failure mode was found to be an axisymmetric plastic collapse resulting from excessive vertical displacements at the pole. The maximum displacement was 1.09 m (43 in) at 1.45 MPa (195 psig). This information was given in the Revision 23 to Section 3.8.2.4.2.2 of the SSAR.

The staff performed independent calculations on the basis of equations given in "Buckling and Collapse of Thin Internally-Pressurized Dished Ends," Proceedings, Institution of Civil Engineers, Part 2, Volume 67, September 1979, pp. 607-626 by Galletly, G.D., and found that the theoretical elastic-plastic buckling pressure would be 1.35 MPa (181.3 psig).

The value of 1.3 MPa (174 psig) is, thus, believed to be appropriate for the theoretical elastic-plastic buckling pressure. Therefore, DSER Open Item 19.2.6.2-1 is closed.

Table 19.2-5 of this report shows the meridional and hoop stresses in the knuckle region as obtained from Figure 3.8.2-5 of the SSAR and the January 14, 1993, response to Q220.12.

From Table 19.2-5, it appears that the meridional stresses (tensile) are shown to vary linearly with the pressures. However, this is not the case for the hoop stresses (compressive). In the DSER, the staff requested Westinghouse to discuss the technical basis for this apparent difference in the pressure-stress relationship between the meridional and hoop stresses. This was DSER Open Item 19.2.6.2-2.

Westinghouse responded that at the knuckle region of the dome, elastic analyses show that the meridional stress is tensile and the hoop stress is compressive. The compressive hoop stress occurs over a short length of the knuckle region. Once the material yields, the geometry changes as the shell deflects inward and the yield zone extends along the meridian. The extension of the yield zone increases the total hoop compressive force even though the hoop stress remains approximately constant. The meridional stress is uniform around the circumference of the vessel and continues to increase to remain in equilibrium. The staff finds that Westinghouse's explanation for the nonlinear variation of the hoop (compressive) stresses is reasonable and, thus, is acceptable. Therefore, DSER Open Item 19.2.6.2-2 is closed.

Using BOSOR-4, Westinghouse calculated the theoretical elastic buckling pressure utilizing an approach similar to that of the ASME Code Case N-284, Revision 0 as 3.8 MPa (536 psig) at the ambient temperature. A reduction factor (defined as the product of the capacity reduction factor and the plastic reduction factor) was established as 0.385 on the basis of the lower

bound curve of test results of 20 ellipsoidal and 28 torispherical test specimens. This resulted in a predicted buckling capacity of 1.52 MPa (206 psig) at the ambient temperature.

If one were to use Figure 1512-1 in ASME Code Case N-284, Revision 0, the capacity reduction factor should be 0.21. However, Figure 1512-1 can be used for both internally or externally stiffened shells as well as unstiffened shells. In case of internal pressure, ASME Code Case N-284, Revision 0 allows the use of higher values of capacity reduction factor since the influence of the internal pressure on a shell structure may reduce the initial imperfections. Therefore, the use of the reduction factor of 0.385 is judged to be reasonable and thus acceptable.

From the above analyses and the rationale used for capacity factor determination at the ambient temperature for the top head, the staff concludes that the theoretical elastic-plastic buckling pressure of 1,301 kPa (174 psig) and the elastic buckling pressure of 1.52 MPa (206 psig) are consistent with the staff's evaluation, and are therefore, acceptable. The corresponding allowable buckling pressures are 818.4 kPa (104 psig) and 951.5 kPa (123.3 psig) for the ASME Service Level C Limits with a factor of safety of 1.67 as specified in ASME Code Case N-284, Revision 0. The capacity of steel elements is reduced in proportion to the reduction attributable to temperature in yield stress, ultimate stress, or elastic modulus. At 204.4 °C (400 °F), the yield stress is reduced by 17 percent, and the corresponding pressures are reduced to 698.9 kPa (86.7 psig) and 809.8 kPa (102.8 psig), respectively, and are also acceptable.

The ultimate pressure capacity for the containment function is expected to be associated with leakage caused by excessive radial deflection of the containment cylindrical shell. This radial deflection may, in turn, cause distress to the mechanical penetrations, and potential leakage at the expansion bellows for the main steam and feedwater piping. There is high confidence that this failure would not occur before stresses in the shell reach the ASME Code specified minimum material yield.

Westinghouse considered the most likely failure mode to be that associated with gross yield of the cylindrical shell using the ASME Code specified minimum yield stress and the von Mises failure criterion. However, Westinghouse uses a 32 percent increase from the ASME Service Level C Limit (i.e., a 15 percent increase from the von Mises failure criterion and a 15 percent increase from the mean material strength). The staff does not accept Westinghouse's use of both the mean yield strength of SA 537, Class 2 material and the von Mises failure criterion for the best estimate failure pressure for the following four reasons:

(1) A comparison between experimental and theoretical yield stresses in *Engineering Design*, Faupel, J.H., pp. 249-258, John Wiley & Sons, 1964 shows that the von Mises failure criterion does not always give a failure stress 15 percent higher than the minimum material yield stress.

(2) The material test data uses only 122 specimen and they are not the same as the SA 537, Class 2 material nor as-built material.

(3) In the following references the membrane yielding for most of the tested cylinders occurre MARC FEM code using the large displacement and nonlinear material property options:

- Clauss, D.B. and Horschell, D.S., "Comparisons of Analytical and Experimental d at 5 to 14 percent lower than the predicted yield pressure determined by the Results from Pressurization of a 1:8 - Scale Steel Containment Model," Proceedings 8th International Conference on Structural Mechanics in Reactor Technology, August 19 - 23, 1985

- Clauss, D.B., "Comparison of Analytical Predictions and Experimental Results for a 1:8 - Scale Steel Containment Model Pressurized to Failure," NUREG/CR-4209, July, 1985.

The discrepancy between the observed and the predicted results is attributable to the following reasons: (a) strain rate effects (5 percent reduction), (b) Bauschinger effect (5 to 10 percent reduction) referring to the phenomenon whereby the yield stress in tension or compression is reduced if the material has been previously yielded in the opposite sense (when the plates comprising the cylinder were rolled into the cylindrical shape, the internal surface underwent compressive yielding and internal pressurization results in tensile yielding in the cylinder), and (c) difficulties in applying uniaxial data to multiaxial strain states.

(4) From an American Iron and Steel Institute (AISI) survey of test results for thousands of individual product samples, it has been found that strength levels vary as much as 20 percent from the certified material test reports (CMTR) test values. It has been the staff's position that minimum specified strength values (e.g., ASME Code minimum strength values) should be used as the basis for allowable stresses as described in the letter from G. Bagchi and C. Cheng to J. Stolz, Subject: Review of Oyster Creek Drywell Containment Structural Integrity, dated June 14, 1990.

In the DSER, the staff suggested that a 15 percent increase for the determination of the best estimate failure pressure (not a 32 percent increase) be used as the median pressure for the determination of the fragility curve. This was DSER Open Item 19.2.6.2-3. This is subsumed into question number 1 of the letter dated September 14, 1995. The closure of this open item is discussed in the "Fragility Assessment for Probabilistic Evaluation" section below.

As an alternative to the deterministic approach, the SECY-93-087 objective requires that the CCFP be less than or equal to 0.1. To compute CCFP, the best estimate values are used. For the best estimate values, the median values would be used. The staff finds the median fragility of the containment structure is an adequate criterion for satisfying the SECY-93-087 objective, provided the total leakage from penetrations and other bypasses are reasonably controlled. However, Westinghouse did not provide the leakage estimation through the penetrations. In the DSER, the staff requested that Westinghouse provide the leakage estimate through penetrations such as equipment hatches and personnel airlocks. This was DSER Open Item 19.2.6.2-4.

Westinghouse responded that the leakage area in the severe accident is equal to that corresponding to the specified containment leakage of 0.12 volume percent at design basis conditions. There is no increase in leakage area caused by containment pressurization. The ultimate pressure capacity for containment function is calculated to occur when the general membrane stresses in the shell reach the yield stress. Thus the general membrane shell remains elastic for pressures up to this ultimate capacity and increased leakage area is not expected as a result of pressure. The SCSB staff reviewed and evaluated this estimate in the FSER for SSAR Section 6.2.1. Therefore, DSER Open Item 19.2.6.2-4 is closed.

The considerations of (1) gross long-term temperature effects, and (2) transient temperature effects when the AP600 SCV is being cooled under severe accident conditions are evaluated in Section 19.2.6.4 of this evaluation report.

19.2.6.3 Evaluation of Containment Ultimate Capacity Via Use of Fragility Curve

In Chapter 42 of the AP600 PRA, Westinghouse describes the CCFP distribution. Westinghouse developed the probability distribution for containment failure as a result of internal pressurization of the containment vessel.

Five containment failure modes have been identified on the basis of the AP600 containment configuration and its structural material properties described in Section 3.8.2.4 of the SSAR: (1) general yielding of the cylindrical shell, (2) buckling of the ellipsoidal head, (3) buckling of the 6.7 m (22 ft) equipment hatch, (4) buckling of the 4.9 m (16 ft) equipment hatch, and (5) yielding of the personnel airlocks.

The overall uncertainty in the containment failure probability is derived from considering uncertainties in structural material properties, modeling assumptions and construction method. Considering uncertainties in structural material properties, modeling assumptions, and construction methods derived the uncertainty in the containment failure probability. Westinghouse assumed the coefficient of variation (COV) of material properties as 0.048 on the basis of a 122 specimen test. Westinghouse assumed that the overall uncertainty is dominated by the variances in structural properties. However, the staff raised several questions about this assumption as discussed below.

Generally, a modeling error would represent (1) the basic variability of the theoretical resistance model with respect to experimental results, and (2) the variability between experimental results and in-service conditions, which accounts for the imperfect experimental modeling of a real structure (variations in plate thickness, boundary conditions, welds, residual stresses, etc). From the staff's previous review of the ABWR and System 80+ designs, modeling uncertainties have been found to have a significant effect in establishing containment designs. NUREG/CR-2442 recommends that the COV be 0.12 for all practical instances of modeling error. The COV is defined as $(\exp(\beta^2) - 1)^{1/2}$, where $\beta$ is the logarithmic standard deviation for lognormal distribution. The common $\beta$ for material properties ranges from 0.06 to 0.08. The staff, in the DSER, requested Westinghouse to consider the modeling uncertainties and the realistic material uncertainties in the calculation of the containment failure probability distribution. This was DSER Open Item 19.2.6.3-1.

Westinghouse revised Chapter 42 of the AP600 PRA to consider uncertainties in geometric properties, structural analysis, material properties, and gross errors. The overall uncertainty in

the containment strength is generally insensitive to variations in geometric properties such as fabrication and erection tolerances on plate thickness, size, and dimensions, except for the buckling mode of failure (L. Greimann and F. Fanous, "Reliability of Containments under Overpressure," Pressure Vessel and Piping Technology, 1985, pp. 835 - 856). However, uncertainties for geometric properties are not given in the AP600 PRA. In a meeting at Chicago Bridge and Iron (CBI) Technical Services Company held on August 30 - 31, 1995, (see "Summary of Meeting on the Analysis and Design of the Westinghouse AP600 Containment Vessel," dated September 29, 1995), Westinghouse committed to revise the AP600 PRA to include the uncertainties in geometric properties for buckling. The Revision 8 to the AP600 PRA contains this commitment.

Gross errors in construction and design are not quantifiable because they can lead to catastrophic results that are not predictable by reliability methods. Thus, Westinghouse considers the subjective uncertainty associated with modeling and the random uncertainty in material properties. This is consistent with industry practice.

The pressure capacity for a given failure mode is described by $P = P_m \cdot M \cdot S$, where (1) $P_m$ is the median pressure capacity representing the internal pressure level for which there is a 50 percent probability of failure, (2) M is a lognormally distributed random variable having a unit median value and a logarithmic standard deviation, $\beta_M$, representing the uncertainty as a result of analytical modeling, and (3) S is also a lognormally distributed random variable having a unit median value and the logarithmic standard deviation, $\beta_S$, representing the uncertainty associated with the material properties. The staff finds Westinghouse's consideration of uncertainties in modeling and material properties to be appropriate and, thus, is acceptable. Therefore, DSER Open Item 19.2.6.3-1 is closed.

Westinghouse chose the Weibull distribution to represent the containment failure probability function. It is indicated that the Weibull distribution requires the definition of the mean containment failure pressure, the variance in the containment failure, and the cut-off containment pressure below which the failure probability is zero. However, the PRA did not explain how these values were used to develop the probability distribution function for each containment failure mode. In the DSER, Westinghouse was requested to discuss how values were used to develop the probability distribution function and provide the resulting mathematical expression, including scale and shape parameters for the Weibull distribution and a tabulation of failure probability against various pressure levels for each containment failure mode. Also, Westinghouse was requested to justify the adequacy of the use of Weibull distribution in conjunction with the use of the material and modeling uncertainties. This was DSER Open Item 19.2.6.3-2.

Westinghouse revised the AP600 PRA to consider the normal, the Gamma, the Gumbel, the lognormal, and the Weibull distributions to specify the probability density function and selected the lognormal distribution to construct the CCFP distribution.

The lognormal distribution is considered a reasonable distribution since the statistical variation of many material properties may be represented well by this distribution provided one is not primarily concerned with extreme tails of the distribution. In addition, the central limit theorem states that a distribution of a random variable consisting of products and quotients of several variables tends to be lognormal even if the individual variable distributions are not lognormal.

Because the pressure capacity for a given failure mode is described by $P = P_m \cdot M \cdot S$, the lognormal distribution is a reasonable selection and, thus, is acceptable. Therefore, DSER Open Item 19.2.6.3-2 is closed.

Westinghouse used the mean failure pressures at the temperature of 37.8 °C (100 °F). However, on the basis of Section 3.8.2.4.7 of the SSAR, 37.8 °C (100 °F) is the ambient temperature. Usually, the ambient temperature is 21.1 °C (70 °F). In the DSER, Westinghouse was requested to clarify this discrepancy. This was DSER Open Item 19.2.6.3-3.

Westinghouse revised Sections 3.8.2.4.1 and 3.8.2.4.7 in its SSAR, Revision 3 to use the terminology "ambient temperature of 100 degrees" to clarify that the ambient temperature is 37.8 °C (100 °F). On the basis of this clarification, DSER Open Item 19.2.6.3-3 is closed.

For the uncertainties in containment failure, Westinghouse used coefficients of variation as 0.11 and 0.12 for the material and the modeling uncertainties, respectively. They are acceptable on the bases of (1) "Development of a Probability Based Load Criterion for American National Standard A58," National Bureau of Standards Special Publication 577, US Government Printing Office, Washington, DC, 1980 and "Reliability of Containments Under Overpressure," L. Greimann and F. Fanous, *Pressure Vessel and Piping Technology,* 1985, pp. 835 - 856 for the material uncertainty and (2) NUREG/CR-2442, "Reliability of Steel Containment Strength," L. Greimann, et. al., for the modeling uncertainty.

For the containment cylindrical shell, Westinghouse used the pressure of 1.25 MPa (166 psig) at 37.8 °C (100 °F) as the mean failure pressure. The staff noted that this resulted from the adoption of both the mean yield strength of SA 537, Class 2 material and the von Mises failure criterion. Based on the discussion in Section 19.2.6.2 of this report, "Deterministic Evaluation of Containment Capacity," it was not acceptable. In the DSER, the staff stated that the best estimate yield pressure of 1.09 MPa (144 psig) should be used. This was DSER Open Item 19.2.6.3-4. This is subsumed by question number 1 of the letter dated September 14, 1995.

In the letter NTD-NRC-96-4617, dated January 4, 1996, Westinghouse stated for the von Mises failure criterion that the difference of 5 to 10 percent in the test results is small and is accounted for in the AP600 fragility estimates in the coefficient of variations (COVs) assigned to materials and modeling uncertainties. Accordingly, Westinghouse treated the von Mises failure criterion as a random variable having a median value of 1.15 with uncertainty for modeling. This is acceptable because of the small scatters from test results and the recommendation of using a median value of 1.15 with uncertainty specified in NUREG/CR-2442.

Also, Westinghouse used the median yield strength as the 10 percent increase above the ASME Code specified minimum yield strength with lognormal distribution. It is appropriate to use the expected, as-built material strength (could be 15 percent increase dependent on tests). However, it is not available for the AP600. Therefore, the 10 percent increase above the ASME Code specified minimum yield strength for the median yield strength is acceptable. Since the lognormal distribution is assumed for the CCFP, the median failure pressure with modeling and material uncertainties should be defined. The median pressure is equal to the product of the medians of lognormally distributed random variables as discussed above.

In Revision 8 to the AP600 PRA, Westinghouse used the median pressure of 1.19 MPa (158 psig = 1.15 [modeling with von Mises failure criterion] x 1.1 [material] x 125 psig [ASME Service Level C Limit]) at 37.8 °C (100 °F) (1 MPa [132 psig] at 204.4 °C [400 °F]). The staff concluded that the use of this pressure as the median failure pressure for the containment cylindrical shell is acceptable. This resolves question number 1 of the letter dated September 14, 1995. Therefore, DSER Open Item 19.2.6.3-4 is closed

For the ellipsoidal upper head, Westinghouse used the pressure of 1.3 MPa (174 psig) at 37.8 °C (100 °F) as the mean failure pressure. The staff found this to be unacceptable, because the best estimate yield pressures for the top head might be 1.1 MPa (146 psig). The buckling pressure is 1.3 MPa (174 psig). In the DSER, the staff recommended that a pressure of 1.1 MPa (146 psig) be used because the top head will yield before buckling could occur. This was DSER Open Item 19.2.6.3-5.

In the August 30 - 31, 1995 meeting at CBI, Westinghouse committed to clarify the pressures specified in the AP600 PRA Section 42.4.2 and revise the PRA to clarify that the failure mode at the top head is knuckle-region buckling instead of top head yield or axisymmetric plastic collapse (see "Summary of Meeting on the Analysis and Design of the Westinghouse AP600 Containment Vessel," dated September 29, 1995). Westinghouse considered buckling at the knuckle area as the failure mode because there is more space above the crown region than next to the cylinder. In that case, knuckle-region buckling will control the probability of failure of the top head. Therefore, the staff finds the use of 1.3 MPa (174 psig) at 37.8 °C (100 °F) (i.e., 1.2 MPa [160 psig] at 204.4 °C [400 °F]) for the median failure pressure for top head is appropriate and, thus, this is acceptable. Therefore DSER Open Item 19.2.6.3-5 is closed.

For the containment equipment hatches, Westinghouse used 150 percent of the critical buckling pressure as the best estimate failure pressure on the basis of the test data. In the DSER, the staff requested that Westinghouse clarify in the SSAR whether this 50 percent increment is founded on either the lower bound or the median value of test data and justify the applicability of these test data to the AP600 equipment hatches. This was DSER Open Item 19.2.6.3-6.

Westinghouse responded that the 50 percent increment of critical pressure for the best estimate failure pressure was based on the curve in ASME Code Case N-284, Revision 0 that was derived from the lower bound of tests. There was only one test specimen that was similar to the AP600 containment configuration ($M_i$ = 14.5). However, using test data points provided by Westinghouse, the staff performed a regression analysis on the basis of the methodology provided in NUREG/CR-4604, and found that the median point at $M_i$ of 14.5 is higher than 50 percent increment. Therefore, the 50 percent increment of critical pressure for the best estimate failure pressure is acceptable and, thus, DSER Open Item 19.2.6.3-6 is closed.

For the overall failure distribution, the staff requested in the DSER that Westinghouse describe the mathematical construction of the overall cumulative failure probability curve, and provide a tabulation of cumulative failure probability versus pressure. The staff requested that temperature be specified in Figure Q-1 of the PRA. Also, the definition of "mean containment failure internal pressure" should be provided in the PRA. This was DSER Open Item 19.2.6.3-7.

Westinghouse added Chapter 42 to the AP600 PRA to provide the mathematical construction of containment failure as a result of internal pressurization of the containment. On the basis of the inclusion of this information, DSER Open Item 19.2.6.3-7 is closed. However, the definition of mean containment failure internal pressure was not provided in the AP600 PRA. This is subsumed by the September 14, 1995 RAI (#9) for which Westinghouse had defined it as median internal pressure.

In the DSER the staff stated that it had not determined the acceptability of the internal containment pressure. It stated that the acceptance of the pressure would be determined on the basis of the resolution of the above DSER Open Items. This was DSER Open Item 19.2.6.3-8. On the basis of the staff's independent calculations, the overall failure distribution is acceptable. The median internal pressure for the AP600 is expected to be 0.99 MPa (129 psig) at 204.4 °C (400 °F). As discussed above DSER Open Items 19.2.6.3-1 through 19.2.6.3-7 are closed and the overall containment internal pressure failure distribution is acceptable. Therefore, DSER Open Item 19.2.6.3-8 is closed.

As a response to the staff's request for the PRA Level 2 analysis, Westinghouse was requested to provide, in the DSER, an assessment of the pressure capability of the main steamline and main feedwater line bellows, a corresponding failure probability distribution curve, and the impact to the overall cumulative failure probability curve. This was DSER Open Item 19.2.6.3-9. DSER Open Item 19.2.6.3-9 is closed on the basis of the discussion on mechanical and electrical penetrations in Section 19.2.6.4.4 of this report.

### 19.2.6.4 Evaluation of Localized Leakage

The containment function can be compromised if excessive leakage occurs before the containment ultimate capacity pressure is reached. The objective of this section is to ensure that significant localized leaks would not occur before reaching the containment ultimate capacity pressures. At pressures above the design allowable pressure, leakage from the containment can potentially occur from buckling at the transition area because of high temperature and at penetrations because of high temperatures and pressures. The leakage potential from thermal buckling of SCV and at containment penetrations is evaluated below.

#### 19.2.6.4.1 Thermal Buckling of Steel Containment Vessel

In the design basis evaluation, the ASME Service Level C Limit (Emergency Condition) does not require the consideration of temperature loading. This is founded on the assumption that the temperature loadings associated with LOCAs are short lived and would not affect the behavior of the steel shell. The temperature loadings associated with the severe accident sequences would last for a number of days. Thus, the effect of severe accident temperature loading needs to be evaluated to ensure that the expected compressive stresses resulting from the load at the transition region (along the entire periphery of the shell) do not lead to buckling of the containment shell causing a loss of containment function. In Q220.93, the staff requested that the buckling analysis of the containment shell under the severe accident temperature loading be performed and results be discussed in the SSAR. This was DSER Open Item 19.2.6.4-1.

In the DSER the staff also stated that it was reviewing the effect of asymmetric temperature distribution as a result of the thermal striping on the buckling behavior of the SCV. This was identified as DSER Open Item 19.2.6.4-2.

The applicant responded that local buckling in this area was investigated by using a BOSOR-5 model of the portion of the shell above elevation 30.48 m (100 ft) extending up to the horizontal stiffener at elevation 40.31 m (132 ft-3 in). Material yield and stiffness properties were contingent on properties at the design temperature of 137.8 °C (280 °F). Buckling occurred 50.8 cm (20 in) above elevation 30.48 m (100 ft) at a factor of 6.0 times the design differential temperature condition.

In an accident scenario, the containment emergency cooling system is activated letting water flow on the top of the containment dome and down the SCV walls to an elevation of 40.31 m (132 ft 3 in) to cool the vessel. Tests simulating this scenario showed that the flowing water or wet region covered about 70 percent of the surface (Gilmore, J. E., "AP600 Passive Containment Cooling System -- Phase II, Test Data Report," WCAP-13296, March 1992). The test results indicated the strips could be as narrow as 86.4 cm (34 in) and 38.1 cm (15 in) for wet and dry regions, respectively, and showed a maximum difference in temperature between wet and dry regions of 20 °C (68 °F).

In the August 30 - 31, 1995 meeting at CBI, an NRC contractor presented an analysis of this accident scenario with temperature difference between wet and dry regions of 26.8 °C (80 °F) and strips of wet (1.73 m [68 in] at 93.3 °C [200 °F]) and dry (76.2 cm [30 in] at 137.8 °C [280 °F]) regions (see the closure of the Open Item 3.8.2.4-6 in Section 3.8.2.4 of this report for the evaluation of the widths of these two strips acceptability) (see "Summary of Meeting on the Analysis and Design of the Westinghouse AP600 Containment Vessel," dated September 29, 1995). The failure mode was buckling as a result of compressive hoop stress near the base at load proportionality factor, $\lambda$, of 5.64. The load proportionality factor, $\lambda$, is defined as the ratio of the loads at which buckling occurs to initial input loads including dead weight, crane load, and temperature loading.

The thermally induced compressive stress encountered during the severe accident condition is strain-controlled, or strain-limited, rather than load-controlled. Load-controlled buckling is characterized by forces applications, such as external pressure and dead weight, that continue beyond instability into the post buckling region, resulting in gross deformation and loss of function. Strain-controlled buckling is characterized by loads that are strain limited, such as thermal loads, so that when buckling occurs, the strain is accommodated and the load is relieved. The process is self-limiting so that deformations are controlled without immediate loss or impairment of function. The essential difference between load-controlled buckling and strain-controlled buckling is recognized in ASME Code Case N-47, Appendix T-1500, by setting different design factors of safety for each case. The design factor of safety for load-controlled buckling is 3.0, consistent with the ASME Code Section III, whereas, for strain-controlled buckling, the design factor of safety is 1.67.

It is highly unlikely that thermal buckling could impair the function of this vessel since the factor of safety against buckling resulting from thermal striping is 5.64. The strain is limited and the material is ductile so that the shell will not rupture as a result of buckling. If there are no penetrations in the region of buckling that might distort appreciably, then there should be no

reason for loss of containment pressure because of buckling. The region where thermal buckling is most likely to occur is at the base of the containment where there are no containment penetrations. For the reasons stated above, Westinghouse's consideration of the thermal effect is acceptable, and DSER Open Items 19.2.6.4-1, and 19.2.6.4-2 are closed.

In the event of an accident, the PCS water is distributed onto the AP600 SCV in order to provide cooling, which is in addition to natural air circulation cooling. Consequently, the pressure and temperature inside containment will be lowered. In certain severe accidents, the PCS water may not initiate when called upon, but does initiate later in the scenario when the containment is hot and pressurized. Rapid cooling of the AP600 SCV in such a scenario is evaluated below.

On the basis of the January 22, 1993, and June 30, 1994, responses to RAI 252.1 and RAI 480.78 respectively, the stress in the top head is the result of the internal pressure of 708.1 kPa (88 psig) is 251 MPa (36.4 ksi). Reduction of the surface temperature from 148.9 ° to 4.4 °C (300 ° to 40 °F) results in a thermal strain of 0.16 percent. On the basis of elastic analysis assuming biaxial restraint of thermal expansion, the temperature changes produce a tensile thermal stress of 469.5 MPa (68.1 ksi). By combining the internal pressure stress and the thermal stress, a tensile stress of 720.5 MPa (104.5 ksi) results at the outside surface of the vessel.

The ASME Code (NE-3213.11) considers surface stresses produced by thermal shock as peak stresses. The ASME Code requires the evaluation of such stresses only for Service Level A and B loads (not for Service Level C or D). For Service Level A and B loads, the total stress is limited to the allowable stress ($S_a$) of 3,999 MPa (580 ksi) for 10 load cycles as shown in Figure I-9.1 of Appendix I of the ASME Code. The surface stress of 720.5 MPa (104.5 ksi) is small in comparison with the ASME Service Level A allowable stress ($S_a$ = 3,999 MPa [580 ksi]).

The staff concludes that rapid cooling of the AP600 SCV by addition of cold PCS water to a hot containment would not cause failure of the vessel because thermal strains are self-relieving and are small in comparison with the ultimate material strain. Therefore, the design of the AP600 SCV for the effects of the rapid cooling plus the internal pressure is acceptable.

19.2.6.4.2 Equipment Hatches

Westinghouse estimated the critical buckling pressures for equipment hatches as 1.45 MPa (196 psig) for a 6.7 m (22 ft) diameter hatch and 1.21 MPa (161 psig) for a 4.9 m (16 ft) diameter hatch founded on the classical buckling capacity of spherical shells subjected to external pressure and the capacity reduction factors specified in Baker et al., *Structural Analysis of Shells*, pp. 253-254, McGraw-Hill, 1972, and in ASME Code Case N-284, Revision 0. The corresponding ASME Service Level C Limits are 908 kPa (117 psig) and 763.2 kPa (96 psig) using the factor of safety (FS) of 1.67 as specified in ASME Code Case N-284, Revision 0, respectively.

For the FS to be applied to the Service Level C pressure capacity, Westinghouse considered the equipment hatch cover buckling attributable to external pressure as the local buckling (FS = 1.67 from ASME Code Case N-284, Revision 0). However, the staff considers it as the global

buckling (FS = 2.5 from NE-3222). The ASME Service Level C pressure capacity is 763.2 kPa (96 psig) with FS of 1.67 and 545.4 kPa (64.4 psig) with FS of 2.5.

On the basis of ASME Code Case N-284, Revision 0, the local buckling is defined as the buckling of the shell plate between stiffeners. The flange of the cover can act as a stiffening element around the periphery of the spherical cap. However, the stiffening effect is limited to $(Rt)^{½}$ of 35.3 cm (13.9 in) from the edge. The entire arc length from the center of the hatch cover to the flange is 255.3 cm (100.5 in). The remaining 218.4 cm (86 in) arc should be considered as unstiffened, therefore, the global buckling criteria should be applied to this unstiffened region. In the DSER, the staff noted that Westinghouse's assumption of local buckling for the equipment hatch cover under external pressure was not acceptable. The staff requested that Westinghouse increase the thickness or use stiffeners (e.g., ABB-CE System 80+ design) to meet the ASME Service Level C Limits at the ambient temperature of 908 kPa (117 psig) for a 6.7 m (22 ft) diameter hatch and 763.2 kPa (96 psig) for a 4.9 m (16 ft) diameter hatch. This was DSER Open Item 19.2.6.4-3.

The staff performed an independent analysis for the equipment hatch covers using ALGOR computer code with fixed boundary conditions and no imperfection. Using ALGOR, the staff predicted the buckling pressure, $P_{buckling}$, as 1.38 MPa (185.12 psig) and 1.57 MPa (212.96 psig) for 4.9 m (16 ft) and 6.7 m (22 ft) equipment hatch covers, respectively. In both cases, the buckling was predicted to occur near the top portion.

Even though the equipment hatch cover forms a portion of the containment boundary, structurally its behavior should be considered to be independent of the containment. The staff is concerned that with a global failure mode of the hatch, there is a potential for radioactive leakage through the equipment hatch sleeve/gasket once buckling occurs. Thus, the leaktight integrity of the containment is jeopardized. On this basis, the staff finds a higher FS of 2.5 founded on NE-3222 to be appropriate and should be applied.

Westinghouse requested the approval of ASME Code Case N-284, Revision 1 to be used for the design and analysis of hatch covers in a letter from Brian A. McIntyre of Westinghouse to T. R. Quay of NRC, Subject: ASME Boiler and Pressure Vessel Code Case N-284, Revision 1 for Use on the AP600, dated September 13, 1995. However, Westinghouse did not provide a comparison of the differences between Revisions 0 and 1 and the significance of these differences with respect to the design of the steel containment shell, stiffeners, penetrations, and equipment hatch covers. The staff sent its position to Westinghouse regarding the acceptability of Revision 1 of the ASME Code Case N-284 (see "Staff Response to Westinghouse Letter Dated February 12, 1996, Regarding ASME Code Case N-284, Revision 1, dated November 26, 1996). In response to the staff concern Westinghouse provided a SSAR revision. Specifically, in Revision 11 to Section 3.8.2.4.3 of the SSAR, Westinghouse provided two ASME Service Level C Limits for the 4.9 m (16 ft) equipment hatch cover at 37.7 °C (100 °F), i.e., 545.4 kPa (64 psig) using NE-3222 with FS of 2.5 and 763.2 kPa (96 psig) using N-284, Revision 0 with FS of 1.67.

The staff has determined that the ASME Service Level C Limit pressure for the 4.9 m (16 ft) equipment hatch cover at 37.7 °C (100 °F) is 545.4 kPa (64 psig) (527.4 kPa [62 psig] at 137.7 °C [280 °F]).

On the basis of the response to Q252.1, dated January 22, 1993, the postulated maximum containment internal pressure would rise to 708.1 kPa (88 psig) at 147.7 °C (296 °F). This is higher than the ASME Service Level C Limit pressure for the 4.9 m (16 ft) equipment hatch cover buckling. The staff believed that there would be a potential for radioactive leakage through the equipment hatch sleeve/gasket once buckling occurs. Thus, the leaktight integrity of the containment would be jeopardized. The staff believed, therefore, that Westinghouse needed to change the design of the equipment hatch cover either by increasing its thickness or by stiffening it. The staff discussed this concern in a letter to Westinghouse dated September 18, 1997.

For severe accident sequences involving failure of the passive containment cooling system (PCCS) as shown in Figure 34-160 of the AP600 PRA, the pressure inside containment starts to exceed ASME Service Level C Limit approximately 18 hours after accident initiation and reaches up to 613.7 kPa (74.3 psig) at 154.4 °C (310 °F) at the end of the first 24 hours. However, the failure modes of the PCCS are independent from those leading to core damage, therefore, the failure of the PCCS is not considered a likely severe accident sequence. Likewise, the containment failure as a result of hydrogen detonation is not considered a likely severe accident sequence because of the inclusion of the hydrogen igniter system. ASME Service Level C Limit was not exceeded for the other more likely severe accident sequences analyzed by the staff. The staff's evaluation of the ability of the AP600 to meet the containment performance requirement is described in Section 19.2.4 of this report. Therefore, DSER Open Item 19.2.6.4-3, and the item identified in the previous paragraph, are considered closed.

19.2.6.4.3 Personnel Airlocks

Westinghouse determined the capacity of the personnel airlocks by comparing the airlock design to that tested and reported in NUREG/CR-5118. Westinghouse stated in the SSAR that because critical parameters of the designed and the tested airlocks are the same, the test results can be applied directly. This approach is acceptable. In the tests, the inner door and end bulkhead of the airlock withstood a maximum pressure of 2.17 MPa (300 psig) at 204.4 °C (400 °F). The capacity of the airlock is, therefore, at least 2.17 MPa (300 psig) at the ambient temperature. The maximum pressure corresponding to the ASME Service Level C Limit is estimated by reducing this capacity in the ratio of the minimum specified material yield to ultimate, which gives 1.23 MPa (163 psig) at the ambient temperature. Because this capacity is greater than the ASME Service Level C Limit of 963.2 kPa (125 psig) for the cylindrical portion, the design of the airlocks is acceptable.

19.2.6.4.4 Mechanical and Electrical Penetrations

Seals around penetrations are designed to seat under internal containment pressurization to ensure minimal containment leakage at higher pressures.

In NUREG/CR-5334, the NRC reported results of tests that, during severe accident conditions, resulted in no leakage from any of the three currently used electrical penetration assemblies (EPAs), under the following conditions: (a) D. G. O'Brien EPA, 182.8 °C (361 °F), 1.07 MPa (155 psia) for 10 days, (b) Westinghouse EPA, 204.4 °C (400 °F), 517.1 kPa (75 psia) for 10 days, and (c) Conax EPA, 371.1 °C (700 °F), 930.8 kPa (135 psia) for 10 days.

However, the SSAR does not clearly indicate which EPA will be used in the AP600. In Q220.33, the staff requested a commitment in the SSAR that EPAs penetrating containment be at least as strong as the AP600 SCV.

In its response to RAI 220.33 dated April 26, 1994, Westinghouse stated that the EPAs are procured as equipment and the details are dependent on the supplier. The EPAs to be procured will be similar to one of those tested by Sandia as reported in NUREG/CR-5334 and will have ultimate capacities consistent with those demonstrated in the Sandia tests. The temperature primarily determines the ultimate capacity of the EPAs. The maximum temperature of the AP600 SCV below the operating deck during a severe accident is reported in the PRA Section 34 as 137.7 °C (280 °F). This is below the temperature of the assemblies tested from the three suppliers noted above. In the DSER, the staff requested that Westinghouse provide a commitment in Section 3.8.2.4.2.5 of the SSAR that the COL applicant will demonstrate that EPAs to be used in the AP600 plant shall be at least as strong as the AP600 SCV. This was DSER Open Item 19.2.6.4-4 and COL Action Item 19.2.6.4-1.

In Revision 3 to Section 3.8.6.1 of the SSAR, Westinghouse included a COL commitment to address ultimate capacities at the maximum severe accident temperature of 157.2 °C (315 °F) for EPAs and this commitment would resolve DSER Open Item 19.2.6.4-4 and COL Action Item 19.2.6.4-1. However, this commitment was dropped in Revision 11. Instead, Westinghouse added the design requirement for EPAs, i.e., ASME Service Level C stress limits under a pressure of 721.9 kPa (90 psig) at design temperature (137.7 °C [280 °F]) in SSAR Section 3.8.2.4.2.5. Consequently, the EPAs are at least as strong as the AP600 steel containment vessel and the EPAs will meet the containment performance goal requirement. This design commitment resolves the staff's concern and a COL action item is not needed because it would be redundant and unnecessary. Therefore, the staff considers DSER Open Item 19.2.6.4-4 closed and COL Action Item 19.2.6.4-1 dropped.

The survivalibility of EPAs under certain beyond design-basis accidents is addressed in the Appendix D to the AP600 PRA and evaluated in Section 19.2.3.3.7 of this report.

Containment penetration bellows, which are primarily used in steel containments, with only limited use in some concrete (reinforced and prestressed) containments, are an integral part of containment pressure boundary. Their performance during severe accident conditions must be evaluated in order to assess the pressure and temperature conditions at which a given containment would develop leakage.

The purpose of containment penetration bellows is to minimize the loading imposed on the containment shell caused by differential movements between the containment shell and the pipe to which the bellows are attached. Most bellows are connected to the outside of the containment shell, and would be subjected to internal pressure and axial compression, along with lateral deflection, in a severe accident.

In NUREG/CR-5561 and -6154, the NRC describes the response of typical expansion bellows to severe pressure and deformation. Recent testing has shown that the bellows remain leaktight even when subjected to large deflections sufficient to fully compress the bellows.

In response to RAI 720.206, Westinghouse stated that the bellows supplier performs design of the containment penetration. The specification for the containment penetration bellows requires that the bellows have an ASME Service Level C pressure capacity of 721.9 kPa (90 psig) at 137.7 °C (280 °F) as identified in Revision 23 to Section 3.8.2.4.2.5 of the SSAR. Therefore, the containment penetration bellows are at least as strong as the AP600 steel containment vessel, thus, this design commitment is acceptable.

Because the containment vessel will remain elastic under ASME Service Level C conditions, its deformation under such conditions should be expected to be within the limits specified for the bellows. Therefore, the specified ASME Service Level C design specification requirements for the containment penetration bellows are acceptable. Because of the small number of load cycles, fatigue is not believed to be an important issue in determining containment bellows capacity. However, corrosion could have a significant effect on bellows capacity. In Revision 3 to Section 3.8.2.7 of the SSAR, Westinghouse stated that testing of the containment vessel and the pipe assemblies forming the pressure boundary within the containment vessel will be performed in accordance with the provisions of ASME Section III, NE-6000 and Section XI, NC-600, respectively. Inservice inspection of the containment vessel will be performed in accordance with the ASME Code Section XI, Subsection IWE, and will be described in the Combined License application. With these testing and inservice inspection requirements and COL commitment specified in SSAR Section 3.8.2.7 to prevent corrosion and the specified ASME Service Level C design specification requirements, the staff believes that the bellows will remain leaktight under severe accident, therefore, the deterministic ultimate capacity of 721.9 kPa (90 psig) at 137.7 °C (280 °F) is reasonably achievable.

In Revision 8 to Chapter 42 of PRA, Westinghouse stated that failures of the mechanical penetration bellows, and leakage of the equipment hatches because of ovalization, do not occur before general yielding of the cylinder. For CCFP calculations, the probability of failure at the general yielding pressure of the cylinder is assumed to be 50 percent. After this pressure, the yielding of the cylinder is the prime contributor to the CCFP calculations, and the mechanical penetration failures would contribute only minimal increase in CCFP calculations. Therefore, the probability of failure calculations from mechanical penetrations would not be necessary, as requested in RAI 13 dated September 14, 1995.

In RAI 220.34, the staff raised a concern about nonmetallic items, such as gaskets, which are purportedly qualified to function at the design temperature. The staff requested in the DSER that a commitment be made in the SSAR to demonstrate the functionality of such items under severe accident conditions. In the response to Q220.34 dated March 24, 1994, Westinghouse stated that the AP600 SCV includes nonmetallic gaskets for the equipment hatches and the personnel airlock. The functionality of the personnel airlocks is discussed in the Section 3.8.2.4.2.4 of the SSAR. The functionality of the gaskets for the equipment hatches is addressed in Revision 23 to the SSAR by stating that the gaskets for the AP600 would be similar to those already tested with material such as Presray EPDM E603. For such gaskets, the onset of leakage occurred at a temperature of about 315.6 °C (600 °F), which is above the severe accident temperature. This response is, therefore, acceptable.

19.2.6.5 Conclusion

The SECY-93-087 and the corresponding SRM dated July 21, 1993, approve the deterministic containment performance goal by establishing ASME Service Level C Limits in the evaluation of the passive advanced light water reactors as a complement to the conditional containment failure probabilities (CCFP) approach.

In Section 3.8.2.4 of the SSAR, Westinghouse presented the ultimate capacity of the steel containment vessel (SCV). The staff performed independent evaluations and determined that the design of the AP600 SCV under severe accident phenomenology will meet the deterministic containment performance goals of SECY-93-087 and the corresponding ASME Service Level C Limit was determined as 545.4 kPa (64 psig) at 37.7 °C (100 °F) or 527.4 kPa (62 psig) at 137.7 °C (280 °F) on the basis of the 4.9 m (16 ft) equipment hatch cover buckling. The conclusion is founded on: (1) evaluation of capacity using the ASME Code Level C Service Limit and a 3-D finite element model analysis, (2) realistic failure assessments for various pressure ranges, (3) assessment of applicable components test data, and (4) due consideration of the effects of any potential localized leakage from thermal buckling at the transition area, at the penetrations, and at penetration seals.

In Chapter 42 of the AP600 PRA, Westinghouse discussed the CCFP distribution and the mathematical construction of containment failure as a result of internal pressurization of the containment. The median pressure capacity of the AP600 SCV should constitute a reasonable fragility value to determine the CCFP. The staff performed independent calculations and determined that the median internal pressure for the AP600 is expected to be 0.99 MPa (129 psig) at 204.4 °C (400 °F) and the overall failure distribution is acceptable.

On the basis of the deterministic containment capacity in conjunction with the fulfillment of the probabilistic containment performance, the AP600 SCV should provide a reliable barrier against uncontrolled release of fission products as long as the internal pressure generated by severe accident events is below the ultimate capacity of the containment. Localized leakage due to load induced deformation and/or thermal buckling of the AP600 SCV the transition area, the penetrations, and penetration seals are duly accounted for in determining the median capacity.

The failure probability of the pressure of 527.4 kPa (62 psig) at 137.7 °C (280 °F) for the ASME Service Level C Limit is determined to be less than 5E-5 from the containment fragility curve. Hence, the ASME Service Level C Limit pressure can be taken to represent the realistic lower bound containment failure pressure. Therefore, the staff concludes that the AP600 design has met the containment performance goal specified in SECY-93-087.

19.3 Shutdown Evaluation

19.3.1 Introduction

As part of the design certification process for the AP600 plant design, the NRC has determined, in accordance with SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993, that concerns about shutdown operations should be satisfactorily addressed before the FDA on the AP600

design is issued. The NRC requested the design certification applicant (Westinghouse) to perform a systematic assessment of the shutdown risk issue to address concerns identified in NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," as they are applicable to the AP600 design.

The assessment should include (1) an evaluation of risks associated with shutdown and low-power operation, including design specific vulnerabilities, weaknesses, and consideration of fire and floods with plant in Modes other than full power, and (2) a demonstration that these risks have been considered and that the design features that minimize shutdown and low power risk probability have been incorporated. The applicant has submitted its systematic evaluation of the shutdown operations, WCAP-14837, "AP600 Shutdown Evaluation Report," the most recent revision of which is Revision 3, March 30, 1998. Westinghouse evaluated the AP600 design for risks associated with plant conditions in Mode 4 (safe shutdown), Mode 5 (cold shutdown) and Mode 6 (refueling). Westinghouse concluded that the AP600 is designed to mitigate all design-basis events that can occur during shutdown modes, and the risk of core damage as a result of an accident that may occur during shutdown modes is acceptably low.

The staff based its review of this submittal on insights from NUREG-1449, from a number of studies documented in NRC Information Notice (IN) 91-54, "Foreign Experience Regarding Boron Dilution," September 6, 1991, and from a PRA of shutdown and low-power operating modes for PWRs to screen for important accident sequences. The purpose of the staff review is to ensure that the AP600 design has appropriately addressed the shutdown risk concerns on the basis of experience with operating plants, including appropriate vendor guidelines for COL applicants in areas of outage planning and control, fire protection, and instrumentation. Design improvements were reviewed to ensure insights from shutdown operation experiences were addressed and that the design improvements reduce the likelihood of core damage and enhance public health and safety. Also, the staff evaluated vulnerabilities that may result from new design features; decay heat removal capability using the normal residual heat removal system (RNS); treatment of fires and floods with the plant in modes other than full power; related technical findings discussed in NUREG-1449 and the effectiveness of the regulatory treatment of non-safety systems proposed by the design certification applicant. The following discussion documents the staff's evaluation and basis for resolving these DSER open items.

19.3.2 Design Features That Minimize Shutdown Risk

Westinghouse described the AP600 design features that minimize shutdown risk in WCAP-14837, Revision 3, "AP600 Shutdown Evaluation Report." These features are discussed in the following sections.

19.3.2.1 Decay Heat Cooling System

The AP600 design includes a redundant normal residual heat removal (RNS) system, which is used to perform normal plant cooldown. The RNS detailed design discussion is included in Section 5.4.7 of the SSAR. The RNS is a non-safety-related defense-in-depth system, which consists of two mechanical trains of decay heat removal. Each train includes a pump, a heat exchanger and the system piping and valves, and is located in the auxiliary building. The two RNS trains share a common suction line from the RCS and a common discharge header that splits inside containment to return flow to the RCS via the two PXS DVI lines. In the event that a loss of RNS cooling occurs during shutdown operations, an alternate core cooling capability is

provided by a passive safety-related injection system using the IRWST that injects water into the RCS via the DVI line. Other non-safety-related alternative core cooling capabilities can be achieved using the CVS, the CMTs, and the accumulators if they are made available. The WCAP-14837 report provides insights that can be used by the COL applicants to increase the availability of alternate decay heat removal capabilities during shutdown and refueling operations.

In Section 13.5.1 of the SSAR, Westinghouse includes insights from WCAP-14837 report, which provides that the COL applicant will address plant procedures for normal and abnormal operations, emergency operation, refueling and outage planning, alarm response, maintenance, inspection, test and surveillance as well as administrative controls.

19.3.2.2 Onsite Power Systems

The AP600 Onsite Power Systems (OPS) arrangement includes the following power supply sources:

- The preferred power supply is from the high-voltage switchyard through the plant main stepup transformers and two unit auxiliary transformers. Each unit auxiliary transformer supplies power to about 50 percent of the plant loads.

- A maintenance source is provided through a reserve auxiliary transformer.

- Two non-safety-related onsite standby diesel generators are furnished with their own support subsystems.

- A Class 1E dc power and uninterruptible power supply system provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed during shutdown operations.

This arrangement allows redundant power supplies to be maintained even during periods of electrical system maintenance. The details of the AP600 OPS design is discussed in Section 8.3 of the SSAR.

19.3.2.3 Decay Heat Removal Capabilities During Shutdown and Mid-Loop Operations

Westinghouse has incorporated into the AP600 several design features that address issues related to low-power and shutdown operations, especially during mid-loop operations. These design features include the following: (1) RCS loop piping offset, (2) RCS hot-leg level, and (3) RNS step-nozzle connection. These design features are discussed integrally in the shutdown operation discussions of the AP600 design.

While the RCS water level is lowered to within the hot leg (mid-loop) to allow maintenance and testing activities, the risk of losing decay heat cooling increases as a result of the increased likelihood of vortexing at the decay heat removal pump suction. Also, air entrained in the RNS piping may hinder the ability to provide adequate shutdown cooling during mid-loop operation. To address this concern, Westinghouse designed the RNS piping to each respective pump

suction in a continuously downward sloping path from the RCS connection, thereby creating a self venting path with no high point areas and no loop seals.

The staff verified the AP600 ITAAC design verification program to ensure that design improvements are implemented, and concluded that the verification requirements are adequate.

One of the design features that prevents air binding of the RNS pump during mid-loop operation is the step-nozzle connection to the RCS hot leg. The step-nozzle connection substantially reduces the critical RCS hot-leg level at which a vortex can occur in the RNS pump suction line because it reduces the fluid velocity in the hot-leg nozzle, and limits the amount of air entrainment into the pump suction, should a vortex occur, to no greater than 5-percent while continuing to provide decay heat cooling. The staff requested (RAI 440.133) that Westinghouse provide a discussion of the actual design configuration of the AP600 step-nozzle connection, and experimental data, as well as an analysis that demonstrated the adequacy of this design to minimize vortex formation and air entrainments into the pump suction. Westinghouse provided a test report APWR-045, "AP600 Vortex Mitigation Development Test for RCS Mid-Loop Operation," dated July 6, 1994, for staff review. The report describes experimental-scaled tests, which investigate the vortex behavior at the RNS line and hot-leg junction of AP600 during mid-loop operation. Various nozzle geometries were tested to assess the formation of vortices that result in void injection into the pump suction. The test program also identified the optimal nozzle geometry that permits the lowest fluid velocity in the hot leg with the formation of vortices. The staff reviewed the test report and found that test data indicate that the step-nozzle geometry has significantly reduced the potential vortex formation with a maximum of no more than five percent air entrainment into the pump suction, while maintaining the pump in operation. The staff considers a step nozzle is an improvement in the AP600 design to minimize the potential air entrainment of the RNS during midloop operation, and therefore, acceptable.

Table 2.3.6-4 of the AP600 ITAAC program verifies the acceptance criteria of the step-nozzle configuration.

19.3.2.4 Containment

Westinghouse addressed the containment-related aspects of the AP600, needed for shutdown operations, in Section 2.6 of WCAP-14837, "AP600 Shutdown Evaluation Report". During shutdown operations, Westinghouse identified the need for the containment and containment cooling during shutdown operations to maintain cooling water inventory, following a loss of the normal residual heat removal system. Following loss of the normal residual heat removal system, the reactor coolant system will heat up and release steam to the containment environment. If the containment is closed and sufficient cooling is provided through the containment shell to condense the steam, the condensate will eventually drain back to the reactor coolant system, providing a long term decay heat removal path. A closed containment, also known as containment closure, for shutdown operations is not the same as containment integrity normally associated with power operations. For example, containment closure relies upon a single barrier in each penetration and leak testing of the containment or the containment penetrations is not required.

Westinghouse committed to providing the ability to achieve containment closure, during shutdown operations, for events that may result in a steam release to the containment.

Containment closure consists of the ability to establish a single pressure resistant barrier in penetrations providing a direct release path to the atmosphere, before the time that steam would be released to the containment. The pressure resist barriers will have a design pressure equivalent to the containment design pressure of 411.2 kPa (45 psig). If the large equipment hatches are open during shutdown operations, a self-contained power source will be provided to ensure that the hatch can be closed when needed. In addition, when the decay heat is greater than 6 MWt, the passive containment cooling system will be available. For the reasons set forth above, the staff finds the proposed containment-related aspects of the AP600 needed to maintain cooling water inventory during shutdown operations to be acceptable.

19.3.2.5 RCS Piping Layout

The layout of the RCS hot-leg piping and the steam generator channel head allows the hot leg to be drained to a level that is much higher than existing operating reactor designs for nozzle dam installation. In Table 2.1-1 of the WCAP-14837, Westinghouse provides a comparison between a nominal water level for mid-loop operation and a RCS hot-leg centerline. The AP600 RCS loop piping offset provides a higher margin of operation to prevent vortex formation in the RNS pump suction during mid-loop operation. The plant procedures require that ADS first, second and third stage valves be open and fourth stage valves be operable, whenever the CMTs are blocked during shutdown conditions with the reactor vessel upper internals are in place. This provision establishes an RCS vent path that precludes inadvertent repressurization of the RCS during shutdown conditions in the event of a loss of decay heat removal, and also allows the IRWST to inject water into the RCS following a sustained loss of decay heat removal. The staff finds the layout of the RCS hot-leg piping provides a large margin of available water in the RCS that would minimize the potential loss of RNS cooling during midloop operation due to air entrainment. Also, the availability of ADS for RCS venting would minimize inadvertent repressurization of the RCS. Therefore, the staff considers Westinghouse's design improvement for the RCS piping layout acceptable.

19.3.2.6 Reactor Cavity Seal

Current plants use temporary reactor cavity seals to flood the refueling cavities. Failure of these seals can divert water to the reactor pit, and subsequently to the reactor floor drains, and may result in a loss of shielding and fuel cooling during spent fuel assembly movement. The staff requested that (RAI 440.706 and 440.710) Westinghouse address the ability to quickly move and safely store fuel assemblies during a seal failure event. Westinghouse replied that AP600 uses a seismic, Class I, permanently welded seal ring design to provide the seal between the vessel flange and the refueling cavity floor. The permanent cavity seal is designed to accommodate thermal transients associated with the reactor vessel during heatups and cooldowns and alleviate the potential temporary seal failures. In Section 1.2.1.2.1 of the SSAR and Section 2.8.2.1 of the WCAP-14837 report, Westinghouse discusses the permanent reactor cavity seal. In addition, other potential loss of refueling water scenarios associated with the spent fuel pool and fuel transfer canal are discussed in Section 9.1 of the SSAR. During refueling operations, there are three connections to the refueling cavity that could drain the filled refueling pools. These connections are shown on Figure 9.1.6 of the SSAR. The first connection is the 15.2-cm (6-in.) line from the refueling cavity to the containment sump, which is isolated by a manual isolation valve. This manual isolation valve is normally locked-open during power operation to prevent significant holdup of coolant inventory during an accident that

requires containment recirculation. During refueling operations, this valve is locked-closed to allow the refueling cavity to be filled with refueling water and to prevent its inadvertent misalignment.

The other connections are used to transfer water between the refueling cavity and the IRWST. If the spent fuel cooling system pump is inadvertently aligned to divert flow to the IRWST during refueling operations, the spent fuel pool low water alarms would alert the operators to a drop in the fuel pool water level. At the design water transfer flow rate of 3.22 kL/m (850 gpm), if no operator actions were assumed for 30 minutes, the water level in the refueling pools would drop approximately 0.4 m (1.3 ft). Since there is at least 7.0 m (23 ft) of water above the top of the reactor vessel flange during refueling, and there is at least 3.05 m (10 ft) of water above the fuel during fuel movement, sufficient time exists for the operator to prevent fuel uncovery from an inadvertent draining of the refueling pools. The staff concludes that sufficient time exists for operators to take actions to isolate inadvertent loss of refueling water and that refueling pool low-water alarms would provide sufficient warning to operators of the loss of spent fuel pool cooling. Therefore, the staff considers the design of the reactor cavity seal acceptable.

19.3.2.7 Spent Fuel Pool Cooling

The staff reviewed the spent fuel pool cooling and purification system (SFPCPS) in accordance with Section 9.1.3 of the SRP. The staff's acceptance of the SFPCPS design is contingent on whether the design complies with the requirements of GDC 2, 4, 5, 44, 45, 46, 61, 63, and 10 CFR 20, paragraph 20.1(c) as discussed in Section 9.1.3 of this report.

The AP600 spent fuel cooling system is a non-safety-related system. The system is not required to operate to mitigate design-basis events. In the event the spent fuel cooling system is unavailable, spent fuel cooling is provided by the heat capacity of the water in the pool. Connections to the spent fuel pool are made at an elevation to preclude the possibility of inadvertently draining the water in the pool to an unacceptable level. In the event of loss of normal spent fuel pool cooling, a 7-day supply of safety-related makeup is available.

The spent fuel pool cooling system consists of two mechanical trains of equipment. Each train consists of one spent fuel pool pump, one spent fuel pool heat exchanger, one spent fuel pool demineralizer and one spent fuel pool filter. The two trains of equipment share common suction and discharge headers. In addition, the spent fuel pool cooling system comprises piping, valves, and instrumentation necessary for system operation. Either train of equipment can be operated to perform any of the functions required of the spent fuel pool cooling system independently of the other train. One train is continuously cooling and purifying the spent fuel pool while the other train is available for water transfers or in-containment refueling water storage tank (IRWST) purification, or is aligned as a backup to the operating train of equipment.

Both trains are designed to process spent fuel pool water. Each pump takes suction from the common suction header and discharges directly to its respective heat exchanger. The outlet piping branches into parallel lines. The purification branch is designed to process one third of the cooling flow while the bypass branch passes the remaining two thirds. Each purification branch is routed directly to a spent fuel pool demineralizer. The outlet of the demineralizer is routed to a spent fuel pool filter. The outlet of the filter is then connected to the bypass branch, which forms a common line that connects to the discharge header.

The staff completed its review of the spent fuel cooling system and concluded that the design is acceptable, and has provided an evaluation as Section 9.1.3 of this report.

19.3.3 Temporary RCS Boundaries

In Section 6.7 of NUREG-1449, the NRC describes instances in which the failure of temporary RCS boundaries (such as freeze seal, which is used to temporarily isolate fluid systems, temporary plugs for neutron instrument housing, and nozzle dams installed in the hot-leg and cold-leg penetrations to steam generators) can lead to a rapid non-isolable loss of reactor coolant. The staff requested that Westinghouse address this concern with respect to failure of temporary boundaries in the AP600 design.

The AP600 design uses passive safety systems to provide the safety-related means for protecting the plant during all modes of operation including shutdown and refueling. The passive safety systems are designed to either automatically mitigate events that occur during shutdown, or are available for manual actuation. The AP600 technical specifications identify when the various portions of passive safety system are required to be available.

In addition, Westinghouse provided the following design features that reduce risks associated with temporary RCS boundaries for AP600:

- Reduced reliance on freeze seals - Freeze seals are used for repairing and replacing components such as valves, pipe fittings, pipe stops and pipe connections when it is impossible to isolate the area of repair any other way. Industrial experience indicates that some freeze seals have failed in nuclear power plants and resulted in significant events. To address the issue of freeze seals failure, the AP600 design reduced the potential applications of freeze seals by reducing the number of lines that connect to the RCS and by providing the ability to perform inservice tests (ISTs) on many valves that connect to the RCS pressure boundary. The IST program reduces the requirements for disassembling of RCS pressure boundary valves to perform operability tests. The use of freeze seals during a forced outage will typically occur in cold shutdown, when passive core cooling is required to be available.

  This is a COL action item and the COL applicant will develop plant specific guidelines that would reduce the potential for loss of RCS boundary and inventory when using freeze seals. Section 13.5 of the SSAR contains COL information items requiring plant procedures, including those related to the use of freeze seals.

- Elimination of temporary plugs for nuclear instrumentation - The AP600 design does not contain removable bottom mounted nuclear instruments that require temporary plugging during shutdown and refueling. The AP600 design uses a fixed incore system.

- Steam generator nozzle dams - Steam generator nozzle dams are often used to isolate steam generators during refueling outages to allow maintenance and inspection of the steam generator tubes. The nozzle dams will fail if the RCS pressure exceeds the nozzle dam design pressure without a pressure vent/release pathway, thus creating a direct RCS drain path to the containment through an open SG primary manway. The AP600 nozzle dams are designed to withstand to a RCS pressure of 220.6 kPa

(32 psia), compared to the typical pressure of 137.9-172.4 kPa (20-25 psia). The refueling procedures will require that stages 1, 2 and 3 of the ADS valves are open to ensure that an RCS vent path is established and to preclude potential RCS repressurization that results in a loss of RCS boundary.

The staff finds that the reduction of RCS penetrations, the ability to perform inservice tests, the use of fixed incore system, and higher nozzle dam design pressure, together will reduce the risks associated with the loss of temporary RCS boundaries. Therefore, the staff considers the design relative to temporary RCS boundaries acceptable.

19.3.4 Instrumentation and Control During Shutdown Operation

In NUREG-1449, the NRC describes inadequate instrumentation and incomplete operating procedures, especially during periods of reduced inventory operations that have contributed to several loss-of-shutdown-cooling events at operating plants. Consequently, the staff has recommended that PWRs of advanced designs include enhanced instrumentation capabilities to enable the operator to continuously monitor key plant parameters during reduced inventory operations. Also, the operator must be able to detect the onset of a loss of decay heat cooling early enough that mitigation actions can be taken to restore shutdown cooling capability. As a minimum, this instrumentation should be available to provide visible and audible indications of abnormal reactor vessel level, temperature, and RNS heat-removal performance.

Westinghouse addressed the instrumentation and control systems in Sections 2.1 and 2.3 of WCAP-14837.

19.3.4.1 Level Instrumentation

The AP600 design employs two redundant differential-pressure (dP)-based safety-related RCS hot-leg level channels, which consist of separate pressure taps that connect to the bottom of the hot leg, and to the top of the hot-leg bend leading to the steam generator. Other level tap connections are located between the reactor vessel and RNS step-nozzle suction line and at the high point of the steam generator tubing run. These channels provide signals for alarm and isolation protection on low RCS level in the event that the operator fails to take action and continues to drain coolant from the RCS. The RCS level indicators are provided primarily to monitor the RCS water level during mid-loop operation. In the event that a loss of RNS occurs and the RCS water level drops to the bottom of the hot leg, the passive safety-related IRWST will automatically inject water into the RCS to maintain core cooling. In addition, the operators can manually initiate IRWST injection if the automatic function is not available.

In Table 2.1-1 of WCAP-14837, Westinghouse describes various RCS water level stages associated with isolation protection and safety injection. The offset design of the AP600 RCS hot-leg and cold-leg piping provides an approximately 30.5-cm (12-in.) margin for mid-loop operation as compared with the hot-leg centerline. Additionally, the hot-leg level system is designed to provide accurate water level measurement within ±3 percent of the measured level.

On this basis, the staff finds that the additional water level margin and the accuracy of the hot-leg level indication during mid-loop operation reduces the potential for loss of RNS from air-entrainment into the pump suction. The low-level alarm and automatic isolation prevents the operator from over-draining the RCS coolant during a draindown evolution. Safety injection

from IRWST provides and maintains core cooling in the event of a loss of RNS. The staff, therefore, concludes that the AP600 level instrument design is acceptable.

19.3.4.2 Temperature Instrumentation

The AP600 design includes two safety-related hot-leg wide-range thermowell-mounted resistance temperature detectors (RTDs) and incore thermocouples that are used to measure RCS temperature. The incore thermocouples are used to measure core exit temperature, which is the indicative of the RCS temperature, and they are only available when the reactor vessel head is in place. This capability is no longer available when the reactor vessel head is detensioned and the instruments are disconnected in preparation for refueling activities. In this condition, the ability to measure the RCS temperature is the RCS wide-range hot-leg RTDs. The staff was concerned that the RTD detector's accuracy is highly flow dependent and asked (RAI 440.690) that Westinghouse address the ability of the RTDs to accurately detect incremental changes in temperature under no flow condition. Westinghouse replied that the wide-range RTDs provide a backup indication of RCS coolant temperature when the RNS is operating because the RNS heat changer inlet and outlet temperatures, and the RNS pump flow indications would show adequate RCS cooling. The wide-range RTDs provide the primary indication in the event that the RNS pumps become inoperable. The RTDs do not require flow to provide an accurate temperature measurement of the stagnant water in the hot legs under these conditions because they are inserted into the bottom of the hot legs. This configuration provides trending capability of the RCS temperature. as long as there is water in the loop piping.

Upon detection of the loss of RNS cooling, the operators are required by emergency response guidelines (ERGs) to verify ADS vent paths and IRWST injection capability if the RNS cooling is not recovered and the reactor coolant level has dropped to the bottom of the RCS hot leg. The safety-related IRWST injection in conjunction with the shutdown ERGs give the operators sufficient tools to maintain core cooling. The staff, therefore, considers this approach acceptable.

19.3.4.3 RNS Performance

Several instruments are available to monitor the normal residual heat removal system (RNS) performance. As described in Section 5.4.7.7 of the SSAR and Section 2.4.2.1 of WCAP-14387, the following system parameters are monitored for system operation:

- RNS pump flow/discharge pressure
- RNS heat exchanger inlet/outlet temperature
- RNS valve status
- RCS wide range pressure

The staff requested that Westinghouse (RAI 440.700) discuss the net positive suction head (NPSH) requirements for the RNS pump to enable the pumps to operate during mid-loop conditions with saturated fluid in the RCS without throttling the RNS flow. Westinghouse replied that Section 5.4.7.2.1 of the SSAR discusses the AP600 configuration and that the RNS pumps can operate at full design flow with saturated conditions in the RCS, and that this requirement provides adequate assurance that the RNS pump can be operated following loss of RCS heat

sink events during shutdown. The RNS pump minimum NPSH requirement is approximately 3.05 m (10 ft) at design flow. The staff verified the AP600 ITAAC design verification program to ensure that adequate RNS flows were implemented and concludes that the verification requirements are adequate.

The staff concludes that the available instrumentation is also adequate for the operator to monitor the performance of the RNS and to ensure the heat removal capability during shutdown and low-power operations.

19.3.5 Technical Specifications

In NUREG-1449, the NRC reported that current standard technical specifications (STS) for PWRs are not sufficiently detailed to address several risk-significant RCS configurations during shutdown and refueling operations. The safety margin that is available during these modes of operation is significantly influenced by the time it takes to uncover the core following an extended loss of residual heat removal capability. The staff found that the conditions that affect this safety margin include the decay heat level, the initial reactor vessel water level, the status of reactor vessel head, the number and size of openings in the cold legs, the existence of hot-leg vents, and availability of alternate methods of decay heat removal in case of loss of decay heat removal systems. The staff requested (RAI 440.58) that Westinghouse describe the TS provisions that deal with shutdown and refueling operations. Westinghouse summarized the TS requirements for shutdown operations in Table 2.3-1 of WCAP-14837. For events that occur in Mode 4, safe shutdown, the TSs require that the full complement of passive safety-related systems be available to mitigate an event. For events that occur in Mode 5, cold shutdown conditions with the RCS pressure boundary intact, the passive safety-related ADS, CMT and PRHR HX as well as IRWST injection will be available. The accumulators, however, will not be available.

For events that occur in Mode 5 with the RCS pressure boundary open and the plant in reduced inventory conditions, the PRHR HX, accumulators, and core makeup tanks are not effective. The ADS first, second and third stage valves are open and the fourth stage valves are required to be operable. The IRWST gravity injection, containment recirculation paths and containment closure capability must be available. However, TSs do not include the RNS in the AP600 in this mode.

In Section A of the SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety-Related Systems (RTNSS) in Passive Plant Designs" dated March 28, 1994, the staff discusses the processes used (1) to develop insights regarding the importance of non-safety-related systems to the overall safety of the AP600 design, and (2) to determine what, if any, additional regulatory controls should be implemented for those non-safety-related systems determined to be important to safety. In Chapter 22 of this report, the staff discusses the RTNSS process in detail.

Westinghouse's evaluation of the RTNSS implementation is discussed in WCAP-13856 (Revision 1) "AP600 implementation of the Regulatory Treatment of Non-Safety-Related Systems Process." In addition, the focused PRA sensitivity study that forms a major part of the RTNSS process is contained in Chapter 52 of the AP600 PRA. The original RTNSS evaluation

in WCAP-13856 (Revision 0) identified only two conditions requiring regulatory controls on non-safety-related systems:

(1) the reactor trip function on the DAS for mitigation of ATWS

(2) the RNS and supporting fluid and ac electrical systems for operations during mid-loop conditions

However, after extensive discussions with the staff, Westinghouse agreed to expand the number of SSCs covered by RTNSS and to expand the modes during which RTNSS controls apply, as discussed in the attachment to Westinghouse letter NSD-NRC-97-5485, dated December 12, 1997. RTNSS oversight is accomplished through administrative controls on the identified SSCs, which specify operability requirements are not met, surveillance requirements, and the bases for the controls. However, there are no limiting conditions for operation associated with these RTNSS controls.

The staff reviewed the administrative controls related to shutdown operations (Modes 5 and 6), and identified a concern related to the allowed completion time for required actions during periods of reduced inventory. The proposed administrative control for RNS during Modes 5 and 6 specify that both RNS pumps should be available before entry into Mode 5 with the pressure boundary open or Mode 6 with upper internals in place or the cavity less than full. If one RNS pump subsequently fails, the operators is permitted up to 72 hours to remove the plant from the mode in which these controls are applicable. The staff concluded that the time, with no other mitigation actions, would be excessive when the plant is operating in a reduced-inventory condition. The short refueling schedules proposed for the AP600 mean the plant could be in reduced-inventory conditions for a relatively short time. Thus, it could be possible to enter reduced-inventory operations, then have the RNS or one of its supporting SSCs become inoperable, but with the 72-hour action completion time, necessary work could be completed and the plant could exit the mode within the time specified for operator action (The same action times are specified for RNS support systems, such as component cooling water, service water, and on-site ac power). Thus, for the originally proposed control for reduced-inventory operations in the applicable modes, the 72-hour completion time effectively served no safety purpose.

The staff concluded that the administrative controls on RNS and supporting SSCs for reduced-inventory operations during Modes 5 and 6 were not consistent with the safe shutdown objective. In the January 15, 1998 meeting with Westinghouse, the staff discussed the basis for the 72-hour completion time and appropriate action completion times when operability requirements are not met. As a result of the discussions, Westinghouse agreed to reduce to 12-hour action completion time for the operators to initiate actions to increase the RCS water level, especially during mid-loop conditions.

The staff reviewed Westinghouse letter DCP/NRC 1271, dated February 27,1998, which revises the AP600 investment protection short-term availability controls for the RNS and supporting SSCs and concluded that the proposed revision adequately addresses the agreement with the staff as discussed in the January 15, 1998 meeting. The proposed required action A.1 states that if one RNS pump is found inoperable, the operator is required to take actions to increase the water inventory above the core and that this action must be completed

within 12 hours. The administrative control bases clarifies that by 12 hours, if the control is still applicable, actions shall be initiated to increase the RCS water level to 20 percent pressurizer level or to a full refueling cavity (whichever is applicable). The staff considers this acceptable.

19.3.6 Transient and Accident Analysis

The applicant discussed applicable SSAR Chapter 15 non-LOCA and LOCA transients postulated to occur in shutdown operations in Section 4.0 of WCAP-14837. The applicant identified the limiting case for each event category discussed in Chapter 15 of the SSAR and evaluated the effects of plant control parameters, neutronic and thermal hydraulic parameters, and engineering safety features on plant transients. For those cases that are bounded by the corresponding cases presented in Chapter 15 of the SSAR, the applicant provided supporting rationales. For those cases that are more limiting than the corresponding SSAR cases, the applicant provided quantitative analyses results for the staff to review and approve. The following discussion documents the staff's evaluation.

19.3.6.1 Feedwater System Malfunctions

Feedwater system malfunctions can result in a decreased feedwater temperature or an increased feedwater flow. The events decrease RCS temperature, which causes power to increase because of the effects of the negative moderate coefficient of reactivity. The analyses of the feedwater system malfunction initiated from Modes 1 and 2 are discussed in Sections 15.1.1 and 15.1.2 of the SSAR. For a decreased feedwater temperature event, the maximum change in feedwater temperature occurs when the plant is operating at full-power. Also, feedwater flow is reduced as plant load is reduced. Because of lower feedwater temperature changes caused by the feedwater system malfunctions and lower feedwater flow rates, the event has less effect on power increase at lower power levels or in Modes 2, 3 and 4.

In modes other than Mode 1, feedwater entering the steam generator is routed through the startup feedwater control valves, which restrict feedwater flow to be less than the flow through the main feedwater control valves. Therefore, a failure of a main feedwater control valve in Modes 2, 3 and 4 is unlikely. The assumption of a failed open startup feedwater control valves, in Modes 2, 3 and 4, results in a relatively slow transient because of a lower feedwater flow rate. Modes 5 and 6 are bounded by Mode 1 because the initial RCS temperatures are reduced and the core is subcritical. Therefore, the analyses for Modes 1 and 2 in Sections 15.1.1 and 15.1.2 of the SSAR bound the events initiated from shutdown modes. The staff has reviewed and approved the analysis for the limiting feedwater system malfunction events and provided its evaluation in Sections 15.2.1.1 and 15.2.1.2 of this report.

19.3.6.2 Excessive Increase in Secondary Steam Flow

Excessive load increase events decrease RCS temperature, which causes an increased power because of the effects of the negative moderate coefficient of reactivity. The excessive load increase event initiated from full-power conditions is discussed in Section 15.1.3 of the SSAR. Since the initial power at Mode 2 is low, the event results in a lower power level than that from full-power conditions. In Modes 3 through 6, the excessive load increase event may be considered to be a steam release because there can be no load when the turbine is off-line and the core is subcritical. Modes 3 through 6 are bounded by Mode 2 because the initial RCS temperatures and pressures are reduced and the core is subcritical. The excessive load events

at low powers and shutdown modes are bounded by the cases at full power conditions. The staff has reviewed and approved the analysis for the limiting excess load initiated from full-power and provided its evaluation in Section 15.2.1.3 of this report.

19.3.6.3 Steamline Breaks

Steamline breaks (SLBs) are analyzed for Mode 1 and 2 conditions and the results are provided in Section 15.1.5 of the SSAR. The steam released from a steamline break causes a decrease in the RCS temperature, and in the presence of a negative moderator temperature coefficient, the decreased RCS temperatures result in a positive reactivity addition. If the resulting positive reactivity is greater than the negative reactivity from the inserted control rod worth and from the borated water injected from the CMTs, the core may return to criticality for a post-trip core. In Section 15.1.5 of the SSAR, Westinghouse shows that if the event occurs in Mode 2, it results in a more severe post-trip transient than that initiated from Mode 1 because the decay heat level for Mode 1 is higher and reduces the effect of cooldown.

An SLB initiated from Mode 3 is not worse than that from Mode 2 because the pressure, temperature, and steam flow through the broken steamline are less limiting. Mode 4 is bounded by Mode 2 because of its lower initial RCS temperature and an effective decoupling of the secondary system from the primary system as the reactor coolant pumps are removed from services and the RNS is started. Automatic safeguards actuation signal are available through Mode 3, until the RCS is borated to meet shutdown margin requirements at cold shutdown 93°C (200°F) and safeguards signals are blocked. Both CMTs continue to be available for automatic actuation on low-2 pressure level or manual actuation through Mode 4 with the RCS not being cooled by the RNS (per TS LCO 3.5.2).

The RCS temperatures in Modes 5 and 6 are low (below 93°C (200°F)), and the cooldown effect resulting from the SLB is insignificant. Therefore, the SLB initiated from Mode 2 bounds the cases at full power and shutdown modes. The staff has reviewed and approved the analysis for the limiting SLB initiated from Mode 2 condition is discussed in Section 15.2.1.5 of this report.

19.3.6.4 Inadvertent PRHR HX Operation

Inadvertent actuation of the PRHR HX causes an injection of a relatively cold water into the RCS, and produces a positive reactivity addition in the presence of a negative moderator temperature coefficient. The analysis of this event for Modes 1 and 2 is discussed in Section 15.1.6 of the SSAR. The PRHR HX heat transfer rate is a function of the heat exchanger's inlet temperature and flow rate. PRHR HX heat transfer rate is higher with high flow rates and high inlet temperatures. The maximum heat removal rate occurs when the plant is at full-power with forced RCS flow. With the maximum heat removal rate, the event which occurs at the full-power condition results in a higher power than that from Mode 2. In Modes 3 and 4, because the reactor is subcritical, the event produces lower power increases than that from Mode 1. For Modes 5 and 6, the cooldown effect resulting from the inadequate PRHR HX operation is insignificant because the RCS temperatures are low. Therefore, the inadvertent actuation of the PRHR HX initiated from full power conditions is the limiting case. The staff has reviewed and approved the analysis for the limiting case and provided its evaluation in Section 15.2.1.6 of this report.

19.3.6.5 Decreased Heat Removal by the Secondary System

The consequences of a decrease in heat removal by the secondary system are discussed in Section 15.2 of the SSAR. The following seven events are analyzed: (1) loss of load, (2) turbine trip, (3) inadvertent closure of main steam isolation valves, and (4) loss of condenser vacuum, (5) loss of ac power, (6) loss of normal feedwater, and (7) feedwater system pipe breaks. These events are characterized by rapid reductions in heat removal capability of the steam generators. The loss of heat removal capability results in a rapid rise in the steam generators' secondary system pressure and temperature and a subsequent increase in the RCS pressure and temperature. Reactor trip and actuation of secondary and primary safety valves mitigate the effects of the primary to a secondary power mismatch during these events. The severity of these events is increased if the primary to a secondary power mismatch is increased. The occurrence of the event at full-power produces a greater and more rapid power mismatch than at lower power or operations below Mode 2 because of a higher initial power and a higher decay heat level. Therefore, the worst cases are the events initiated from full-power conditions.

For operations other than Mode 1, Cases 1 through 4 listed above are not considered credible because the turbine is off-line and the transients resulting from a turbine related faults cannot occur.

Decay heat removal can be accomplished by the SGs through SG safety valves, which are available through Mode 4 (per TS LCO 3.7.1) and the PRHR HX, which is available through Mode 5 with the RCS intact (per TSs LCO 3.5.4 and 3.5.5).

For operations in Mode 4 or 5 with the RNS in operation, the plant response to a loss of ac power is the same as the loss of RNS cooling event (see Section 19.3.6.20 of this report). In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used. Loss of feedwater events and feedwater line break events will not caused a heatup of the RCS.

The staff has reviewed and approved the analyses for the limiting cases for these events and provided its evaluation in Section 15.2.2 of this report.

19.3.6.6 Decrease in Reactor Coolant Flow

The consequences of a decrease in reactor coolant system (RCS) flow are discussed in Section 15.3 of the SSAR. The following four events are analyzed: (1) partial loss of forced RCS flow, (2) complete loss of forced RCS flow, (3) reactor coolant pump shaft seizure, and (4) reactor coolant pump shaft break. For these events, a loss of RCS flow can reduce heat removal from the primary to the secondary system and cause a heatup in the RCS. The RCS heatup results in an increase in the RCS pressure and a decrease in the departure from nucleate boiling ratios (DNBRs). The occurrence of the event at full-power produces a greater and more rapid heatup than at lower power or operations below Mode 2. Therefore, the cases initiated from full-power are the limiting cases, resulting in a maximum peak RCS pressure and a minimum DNBR. The staff reviewed and approved the analyses for the limiting events and provided its evaluation in Section 15.2.3 of this report.

19.3.6.7 Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition

An uncontrolled rod control cluster assembly (RCCA) bank withdrawal from a subcritical condition causes power to increase. An increase in power results in a decrease in DNBR if it is not terminated by a reactor trip. The analysis of this event for Mode 2 is discussed in Section 15.4.2 of the SSAR. In the analysis, the most limiting operating conditions required by the TSs were used to bound the event from Modes 2 through 5. The assumptions related to the limiting operating conditions include (1) the power range (low setting) high neutron flux is credited for the reactor trip to delay the trip, (2) the flow from three reactor coolant pumps are credited to calculate the minimum DNBR and (3) the RCS temperature at Mode 2 is used to calculate the minimum DNBR and core kinetics feedback. The staff has reviewed and approved the limiting case and provided its evaluation in Section 15.2.4.1 of this report.

19.3.6.8 Uncontrolled RCCA Bank Withdrawal at Power

The analysis for this event is discussed in Section 15.4.2 of the SSAR. This event is not applicable to Mode 2 and below because this event occurs only at power.

19.3.6.9 RCCA Misalignment

The following three events are considered RCCA misalignment: (1) one or more dropped RCCAs, (2) statistically misaligned RCCA and (3) withdrawal of a single RCCA. The analyses of these events for full-power conditions are discussed in Section 15.4.3 of the SSAR. These events result in core radial power distribution perturbations. The radial power changes cause the calculated DNBRs to decrease. Therefore, these events are significant only at power, and the severity increases at higher power. For operations below Mode 2, the reactor is subcritical, the events do not result in a significant decrease in DNBRs and are bounded by Mode 1 conditions. The staff has reviewed and approved the analysis for the limiting events initiated from full-power and provided its evaluation in Section 15.2.4.3 of this report.

19.3.6.10 Startup of an Inactive Reactor Coolant Pump at Incorrect Temperature

Starting an idle reactor coolant pump (RCP) increases the circulation of cold water into the core from the stagnant RCS loop. This results in an increase in positive reactivity in the presence of a negative moderator coefficient and thus, causes power to increase. The analysis of the event for Mode 1 is initiated from 70 percent power (maximum allowable power for conditions with three RCPs operating) and is discussed in Section 15.4.4 of the SSAR. The consequences of this event are directly related to the temperature difference between the cold-leg temperature in the loop with the inactive pump and the core inlet. Initial RCS conditions at power maximize the inlet temperature differences and thus, bound operations in Mode 2 and subcritical modes. Therefore, the 70-percent power case is the limiting case. The staff has reviewed and approved the analysis for the 70-percent power case and provided its evaluation in Section 15.2.4.4 of this report.

19.3.6.11 Chemical and Volume Control System Malfunction

Chemical and volume control system (CVS) malfunctions result in a decrease in boron concentration in the reactor coolant. The analyses of the boron dilution event in Modes 1

through 6 are provided in Section 15.4.6 of the SSAR. The staff has reviewed and approved the analyses for the CVS malfunction events and provided its evaluation in Section 15.2.4.6 of this report.

19.3.6.12 Inadvertent Loading of a Fuel Assembly in an Improper Position

Fuel loading errors may result in a core power-shape exceeding its design values. The core power-shape changes cause the calculated DNBRs to decrease. The severity of this case increases as the power level increases. The results discussed in Section 15.4.7 of the SSAR for Mode 1 at full-power conditions bound that for Mode 2 and subcritical modes. The staff has reviewed and approved the analysis for the limiting event initiated from full-power conditions and provided it evaluation in Section 15.2.4.7 of this report.

19.3.6.13 RCCA Ejection

RCCA ejections in Modes 1 and 2 are the most limiting cases because during Modes 3 through 6, the plant technical specifications require the maintenance of adequate shutdown margin. The required shutdown margin is determined by assuming that the most reactive RCCA is fully withdrawn from the core. Ejection of a single RCCA initiated form the subcritical conditions would not cause the core to be critical. The staff has reviewed and approved the analysis for the limiting cases at Modes 1 and 2 and provided its evaluation in Section 15.2.4.8 of this report.

19.3.6.14 Inadvertent Actuation of the CMTs

The analysis of the inadvertent actuation of the CMTs is performed with the plant initially in Mode 1, full-power condition and is discussed in Section 15.5.1 of the SSAR. The reactor trip and the PRHR HX actuation are actuated on the Hi-3 pressurizer level trip setpoint. During the event, the CMTs inject cold borated fluid into the RCS. The injected fluid expands as the decay heat heats it in the RCS. The expansion is counteracted by the heat removal from the PRHR HX. The applicant stated that the severity of the fluid expansion increases with higher decay heat levels and claimed that the case at full-power (producing maximum decay heat) bounds the results initiated from conditions below Mode 1. The staff notes that the injection rate, the core decay heat level and the heat removal rate controls the fluid expansion. At shutdown operations, while decay heat levels are lower, heat removal from the PRHR HX is also lower. In the absence of analyses to quantify the total effect of the injection rate, decay heat levels and the heat removal rate from the PRHR HX on the fluid expansion, it is not clear that the full-power case bounds conditions below Mode 1. In RAI 440.769F, the staff requested the applicant to analyze the CMT malfunction event at shutdown modes. In response, the applicant presented the results of analyses for the following four cases:

(1) Case 1 - spurious "S" case from 102 percent power
(2) Case 2 - spurious "S" case from HZP conditions (285°C (545°F), Mode 2)
(3) Case 3 - spurious "S" case from 215.5°C (420°F, Mode 3)
(4) Case 4 - spurious "S" case from 176.6°C (350°F, Mode 4)

In the analyses, the CMT malfunction event was assumed to be initiated by a spurious "S" signal. The "S" signal tripped the reactor and RCPs, and actuated the PRHR. To maximize the fluid expansion, Cases 2 through 4 were initiated from a power of 1 percent rated power. The

results showed that for Case 1, the pressurizer level increased after the CMTs were actuated. Since the decay heat following a reactor trip was greater than the heat removal capability of the PRHR, the injected CMT fluid adsorbed the excess decay heat and expanded. The expansion of the injected CMT fluid resulted in an increase in the pressurizer water level. For Cases 2 through 4, the heat removal capability of the PRHR was lower because of the lower initial inlet temperatures. However, the heat removal capability of the PRHR was greater than the decay heat produced and resulted in a shrinkage of the RCS fluid. The results have demonstrated that Case 1 at full power bounds Cases 2 through 4 in lower modes.

For the CMT malfunction caused by the inadvertent opening of the CMT discharge valves, the limiting SSAR case considers consequential LOOP following a turbine trip. A LOOP causes a loss of power to the RCPs. When the reactor coolant flow changes from forced flow to natural circulation flow, the CMT flow increases while the PRHR heat removal capability decreases. The applicant's analyses showed that the assumption of a LOOP following a turbine trip causes the inadvertent opening of the CMT discharge valves to be more limiting than the spurious "S" signal case at full power conditions. In the lower modes, the turbine/generator is offline and the power to plant auxiliaries is supplied by offsite power sources. A consequential LOOP is not a credible event because there is no disruption of the grid. For the CMT malfunction that occurred in lower modes and caused by the inadvertent opening of CMT discharge valves, the pressurizer water level increases until the high-3 pressurizer level setpoint is exceeded and the PRHR is actuated. Pressurizer level will then decrease at a rate greater than that observed in Cases 2 through 4 discussed above because the RCPs are operating and the PRHR heat removal capability is at a higher rate. The applicant's scoping analyses demonstrated that the SSAR case at full power bounds the results for the cases initiated from lower modes. Since the applicant uses the acceptable method and the values for input parameters are conservative, the staff concludes that the scoping analyses are acceptable. The staff has also reviewed and approved the analysis for the limiting case initiated from full-power condition and provided its evaluation in Section 15.2.5.1 of this report.

19.3.6.15 CVS Malfunction

The analysis of CVS malfunction is performed with the plant initially in Mode 1, full-power conditions, and is discussed in Section 15.5.2 of the SSAR. In the full power analysis, a worst combination of makeup boron concentration, feedback conditions, and plant system interactions is used for the limiting case. For this case, the CVS malfunction can cause a slight boration of the RCS. As a result, the core power decreases, which in turn causes actuation of an "S" signal on low cold-leg temperature. The "S" is generated before the pressurizer water increases to the high-2 pressurizer level signal that actuates isolation of the CVS makeup and terminates the transient. The "S" signal actuates the CMTs and PRHR. The reactivity effects of the CVS malfunction that causes an "S" signal for the at-power cases does not occur at shutdown because the core is subcritical with a sufficient shutdown margin. In shutdown modes, the CVS malfunction results in the pressurizer water level increasing to the high-2 level setpoint. As a result, the PMS isolates the CVS makeup valves. Because the isolation of the CVS makeup flow occurs earlier and the CMTs are not actuated (resulting in a smaller increase in the RCS inventory), the events initiated from operations at shutdown modes are bounded by the full-power case. The staff has reviewed and approved the analysis for the limiting case and provided its evaluation in Section 15.2.5.2 of this report.

19.3.6.16 Inadvertent Opening of Pressurizer Safety Valves or the ADS Valves

The analysis of inadvertent opening of pressurizer safety or ADS valves with the plant initially at full-power conditions is discussed in Section 15.6.1 of the SSAR. During the transient, the RCS pressure decreases rapidly. These depressurization events, which occur at power, result in deceased DNBRs. For subcritical modes, violation of DNB safety limits is not of concern because of low decay power levels. Therefore, the events discussed in Section 15.6.1 of the SSAR bound events for operating modes other than full-power conditions. The staff has reviewed and approved the analysis for the limiting case initiated from full-power and provided its evaluation in Section 15.2.6.1 of this report.

19.3.6.17 Failure of Small Line Carrying Primary Coolant Outside Containment

The analyses of radiological consequences for breaks of small lines carrying primary coolant outside containment are discussed in Section 15.6.2 of the SSAR. The analyses performed in Mode 1 are bounding because the coolant temperature and iodine concentrations at Mode 1 bound those that would exist in the other modes. The staff has reviewed and approved the analysis for the limiting case initiated from Mode 1, and provided its evaluation in Section 15.2.6.2 of this report.

19.3.6.18 Steam Generator Tube Rupture in Lower Modes

The analyses of the steam generator tube rupture (SGTR) events with the plant initially at full-power conditions are discussed in Section 15.6.3 of the SSAR. At full-power conditions, the SGTR event results in maximum offsite doses. The offsite doses drop significantly at lower power levels and in lower modes of operation because the break flow from the primary to secondary sides and the steam release from the faulted steam generator, major factors to determine dose releases, are less limiting. In Section 15.6.3 of the SSAR, Westinghouse indicates that an analysis at full-power was performed to demonstrate margin to SG overfill and thus, to assure that the SG safety valves can reseat after opening. The dose calculations for the SGTR event are on the basis of the assumption that the SG safety valve will reseat after opening.

The applicant asserted in Section 4.7.3 of WCAP-14837 that the margin to the SG overfill would be maintained for SGTR events initiated at lower power levels even with a higher initial SG inventory corresponding to the lower initial power level. The staff notes that margin to SG overfill depends on parameters such as initial SG water inventory, time to actuate the PRHR HX and termination of the CVS flow. In the absence of a quantitative analysis for SG overfill, it is not clear that the margin to SG overfill can be maintained for SGTR events initiated at lower power levels and shutdown modes. In RAI 440.771F, the staff requested that Westinghouse perform SG overfill analyses initiated from lower mode conditions and show that the analytical results are acceptable. In its response, the applicant performed the analyses for the following three cases: (1) Mode 3 with the RCS at no-load conditions, (2) Mode 4 with the RCS at 215°C (420°F) and 13.3 MPa (1900 psig ), and (3) Mode 4 with the RCS at 157°C (350°F) and 7 MPa (1000 psig).

Case 1 bounds the highest RCS pressure and temperature that may exist during shutdown modes. In addition, the analysis assumed that the low RCS pressure and temperature

safeguards actuation signals were blocked and the CMTs and PRHR were actuated on low pressurizer water level.

Case 2 represents the lowest expected RCS temperature that may exist while the accumulators are aligned. At the RCS temperature of 215°C (420°F), the initial pressure of 13.3 MPa (1900 psig ) is the maximum RCS pressure on the basis of the required primary to secondary pressure differential specified in operating procedures. The low RCS temperature will reduce the effectiveness of the PRHR HX and the highest RCS pressure will maximize the leakage flow from the primary to the secondary sides. Both assumptions minimize the margin to SG overfill.

Case 3 represents the lowest RCS temperature where a credible SGTR is postulated. The initial pressure of 7 MPa (1000 psig) is the maximum RCS pressure expected when the RCS temperature is at 157°C (350°F).

The results of the analyses showed that although the initial mass of water in the SG is higher in lower modes, PRHR HX actuation may be delayed until the low pressurizer level setpoint is reached and accumulator injection may occur, the margin to SG overfill is maintained. The values used for input parameters are conservative, and the results show that the consequences of the SGTR events are bounded by the SSAR results for SGTRs at full-power conditions. Therefore, the staff considers that the analyses are acceptable.

19.3.6.19 Loss-of-Coolant Accident

The analyses of loss-of-coolant accidents (LOCAs) are performed with the plant initially at full-power conditions and are discussed in Section 15.6.5 of the SSAR. With other parameters being the same as assumed for LOCAs at full-power conditions, the reduction in decay heat levels associated with shutdown modes would make all LOCA events less limiting than those analyzed at full-power conditions. To assess the effects of LOCAs with various PXS equipment removed from service in shutdown modes, the applicant analyzed the following LOCA cases that initiated from Mode 3 conditions:

- Large-break LOCA (LBLOCA) - Double-ended cold-leg guillotine (DECLG) break, which is identified in SSAR 15.6.5.4A of the SSAR as the limiting LBLOCA event.

- Small-break LOCA (SBLOCA) - Two SBLOCA cases, an inadvertent actuation of ADS valve and a double-ended direct vessel injection line (DEDVI) break, which are identified in Section 15.6.5.4B of the SSAR as limiting SBLOCAs with respect to ADS depressurization capability to achieve IRWST injection and providing safety injection delivery to limit core uncovery, respectively.

During Mode 3 operations, the accumulators are allowed to be removed from the service by the technical specifications once the pressurizer pressure has been reduced to less than 7 MPa (1000 psig). Before the accumulators are disabled, the consequences of a postulated LOCA event in Mode 3 are less limiting than for full-power cases discussed in Section 15.6.5 of the SSAR because of the lower decay heat levels. In LOCA analyses initiated from Mode 3 conditions, the applicant assumed that the initial pressurizer pressure and hot-leg temperature were (7 MPa (1000 psig) and 218°C (425°F)), respectively. The accumulators were assumed to be isolated. 218°C (425°F) is the highest expected hot-leg temperature when the pressure

is 7 MPa (1000 psig) and the accumulators are removed from service. In RAI 440.713, the staff asked the applicant to address the effect on the Mode-3 LOCA analyses when the initial hot-leg temperature is higher than 218°C (425°F) and accumulators are isolated. In response, the applicant stated that AP600 analyses are insensitive to initial RCS fluid temperate. The applicant's study shows that the sensitivity of the peak clad temperature (PCT) to the RCS initial temperature is about 0.23°C (0.5°F) increase in PCT per degree F increase in initial RCS temperature. Because (1) the calculated PCT of the Mode-3 DECLG break is less than 649°C (1200°F), (2) this result is relatively insensitive to the initial RCS temperature, and (3) the possibility that the RCS hot-leg temperature at the time of accumulator isolation may on occasion exceed 218°C (425°F) is remote for LOCA analyses performed in Mode 3, the staff concludes that the assumption of 218°C (425°F) for the initial hot-leg temperature used in the analyses is acceptable.

The decay heat level is determined at 2.78 hours after reactor shutdown. The cooldown time of 2.78 hours is on the basis of the time estimated to cool down the plant from full-power operation to 218°C (425°F) at a cooldown rate of 27.8°C (50°F) per hour. The cooldown time assumed in the analyses is shorter than the expected time to reach the point to isolate the accumulators during a plant outage. Selection of an earlier time after shutdown will be non-limiting relative to the Section 15.6.5 of the SSAR analyses because the accumulators remain available. Furthermore, a precaution was added to Section 3.1.3.1 of the AP600 shutdown evaluation report (WCAP-14837, Revision 2) to highlight the assumption (the cooldown time of 2.78 hours) of the shutdown LOCA analyses.

For a LBLOCA single failure consideration, the limiting fault is a failure of one CMT discharge valve to open while for the SBLOCA event, the limiting fault is a failure of one of the four fourth-stage ADS valves to open on demand.

In its response to RAI 440.713, the applicant stated that the LOCA analyses performed in Mode 3 bound events that may occur during both Modes 3 and 4 because after accumulator isolation and before normal residual heat removal system (RNS) operation, the decay power drops relative to the Mode-3 LOCA analysis conditions, and there is no reduction in safety-related systems that are available to mitigate the event.

In Modes 4 and 5, once the RCS pressure is reduced to 3 MPa (450 psig) to permit operation of the RNS, the likelihood of breaks in the RCS is extremely low. Therefore, the applicant did not analyze LOCA events at low pressures. However, leaks can occur as a result of operator misalignment of valves. In addition, the TS LCO 3.5.3 permits isolation of one CMT for Mode 4, once the RNS is aligned, and for Mode 5 with the RCS intact. The applicant assessed the consequences of leaks in the RCS. The results show that the consequences of RCS leaks are bounded by the Mode 3 LOCA analyses. Specifically, the results of the double-ended break of a DVI line in Mode 3 credit only one CMT and bound RCS leaks that may be postulated in Modes 4 and 5 when only one CMT is aligned.

The applicant used the WCOBRA/TRAC code to analyze the LBLOCA case and the NOTRUMP code to analyze the SBLOCA cases. The results show that (1) for the limiting LBLOCA case, the maximum PCT is 649°C (1200°F), which is less than the SSAR DECLG break value and (2) for the two limiting SBLOCA cases, the minimum RCS inventories of 54,000 kgs (119,000 lbs) for the ADS valve opening case, and 66,400 kgs (146,000 lbs) for the DEDVI break are greater than the corresponding SSAR values for full power. The values used for the

input parameters are conservative, and the results show that the consequences of the LOCAs are bounded by the SSAR results for LOCAs at full-power conditions. Therefore, the staff concludes that the analyses are acceptable.

19.3.6.20 Loss of RNS Cooling

During shutdown modes of operation, the RNS is used to remove decay heat when the RCS temperature and pressure are reduced to less than or equal to 178°C (350°F) and 3 MPa (450 psig), respectively. A-loss-of-electrical-power event can result in a loss of flow through the RNS and a subsequent loss of RNS cooling event. The applicant performed analyses to determine the plant response to loss of RNS cooling events for two cases initiated from Mode 4 with the RCS intact, and Mode 5 with the RCS open.

For Case 1, under Mode 4 conditions, the analysis uses an initial decay heat level for at time four hours after reactor shutdown. This cooldown time is on the basis of an expected cooldown rate of 27.8°C (50°F) to cool the RCS to the entry conditions for the RNS operation. The RCS is assumed to be 178°C (350°F) and 3 MPa (450 psig). To be consistent with the requirements of TS 3.5.3, one CMT is assumed to be available. To bound Mode 5 with the intact RCS, only three of the fourth-stage ADS valves are assumed to be operable. For consideration of the worst single failure, one of three available fourth-stage ADS valves is assumed to fail to open on demand. The RNS relief valve setpoint is assumed to be 3.98 MPa (578 psia) with corresponding relief capacity of 35 L/s (555 gpm). Since the above assumptions are more limiting than Mode 5 conditions, the analysis for Case 1 is applicable to the loss of RNS cooling event in Mode 5 with the RCS intact.

For Case 2, in Mode 5 with the RCS open, the RNS is initially operating in Mode 5 at 24 hours after reactor shutdown with the ADS stage 1, 2, and 3 valves open (meeting the TS 3.4.13 requirements) and one of IRWST injection paths available (meeting the TS 3.5.8 requirements). The RCS temperature and pressurizer pressure are assumed to be at 70.5°C (160°F) and at atmospheric pressure plus the elevation head in the IRWST, respectively. To be consistent with the TS requirements, both CMTs and PRHR are assumed to be not available. Two of fourth-stage ADS valves are assumed operable (meeting the requirements of TS 3.4.14). For the consideration of the worst single failure, one of two available fourth-stage ADS valves is assumed to fail to open on demand. Since the above assumptions are more limiting than Mode 5 conditions with reduced RCS inventory (mainly because of a higher decay heat level), the analysis for Case 2 is also applicable to the loss of RNS cooling event in the reduced inventory condition.

The applicant used an NRC-approved code, NOTRUMP, to analyze loss of RNS cooling events. The sequences of the events are discussed in Sections 4.8.5.1 and 2 of WCAP-14837. The input parameters are representative of the plant conditions at shutdown modes. The results show that the minimum RCS inventories are 54,500 kgs (120,000 lbs) for Case 1, a loss of RNS cooling at Mode 4, and 77,300 kgs (170,000 lbs) for Case 2, a loss of RNS cooling at Mode 5 with the RCS open. The analyses have demonstrated that the calculated core mixture water levels remain above the top of the active fuel during the event, thus preventing fuel failure. Therefore, the staff concludes that the analyses are acceptable.

The applicant stated in its response to RAI 440.773 that the analysis of a loss of the RNS performed in Mode 5 bounds events that may occur during Mode 6 because of the higher heat power levels. In Mode 6, the water in the refueling cavity provides a large heat sink. Following a loss of the RNS, the water in the refueling cavity can heat up and begin to boil in several hours. The applicant stated that, before boiling occurs, the operators are required to close containment. If no operator actions are taken, the water in the refueling cavity could fall below the top of the core within several days. The applicant stated that, before this time, the operators are required to align the IRWST injection and eventually containment recirculation to provide long-term cooling. In the AP600 Emergency Response Guidelines (ERG), Westinghouse provides guidance for the required operator actions to close containment (Guidance SDG-02, Step 20) , align IRWST injection, and establish containment recirculation (Guidance SDG-02, Step 7) for removal of the decay heat. The staff concludes that the ERG instructions are adequate to insure that the results of a loss of the RNS during Mode 6 will be bounded by that for Mode 5 conditions.

19.3.6.21 *Effects of PWR Upper Internals*

In NUREG/CR-5820, "Consequences of the Loss of the Residual Heat Removal System in Pressurized Water Reactors" dated May 1992, the NRC and its contractor analyzed a loss of residual heat removal event with the vessel upper intervals in place to determine whether it would be possible to uncover the core because of a lack of coolant circulation flow. Such conditions could occur during the flooding of the refueling pool cavity while preparing for fuel shuffling operations. Under these conditions, the vessel upper internals may provide sufficient hydraulic resistance to natural circulation flow between the refueling pool and the reactor, and may prevent the refueling water from cooling the core if the residual heat removal cooling is lost.

In its response to RAI 440.774F, the applicant stated that the AP600 ADS valves are required to be available in Mode 6 until the refueling cavity is filled and the upper internals are removed. Specifically, TS 3.4.14 requires the following: (1) all ADS Stages 1-3 to be open in Mode 6 until the reactor vessel upper internals are removed, and (2) two of four ADS Stage 4 valves to be operable in Mode 6 until the reactor vessel upper internals are removed. As shown in the loss of the RNS analyses for Mode 5, which is discussed in Section 19.3.6.20 of this report, the applicant demonstrated that the ADS valves provide sufficient venting capacity during a loss of the RNS event. In addition, the AP600 upper support plate contains open flow holes similar to that assumed for the Case 1 analysis discussed in NUREG/CR-5820. The consequences of the loss of the RNS would be similar to that presented for Case 1. In the NUREG/CR-5820 analysis, the NRC showed that early core uncovery does not occur for Case 1 with open flow holes through the SG upper support plate. Because the AP600 ADS valves are required to be available for Mode 6 and the SG upper support plate contains open flow holes, the staff concludes that AP600 design is adequate to provide sufficient vent paths to preclude pressurization of the RCS in Mode 6 following a loss of the RNS event.

19.3.7 Fire Protection

The staff reviewed the AP600 fire protection design for shutdown and refueling operations against applicable portions of Section 9.5-1 of the SRP (Revision 2 to BTP CMEB 9.5-1) and NUREG-1449. In Section 6.10 of NUREG-1449, the NRC identified that a postulated fire could potentially damage the operable train or trains of decay heat removal systems during shutdown

conditions. In addition, plant configurations can further complicate the plant's ability to remove decay heat. The portions of the SRP that are applicable pertain to administrative controls.

In Section 3.5 of the AP600 Shutdown Evaluation Report, Westinghouse specifies that the AP600 Fire Protection Analysis demonstrates the ability to achieve or maintain safe-shutdown conditions following a fire in any fire area that occurs during shutdown modes. In Section 2.1.3.2 of the AP600 Shutdown Evaluation Report, Westinghouse defines plant shutdown as "the operation that brings the reactor plant from no-load operating temperature to cold shutdown conditions." Plant shutdown (Modes 3-6) consists of two distinct cooldown stages. The first cooldown stage consists of lowering the RCS temperature from 550°F and no-load operation (Mode 3) to RCS temperature of 350°F and 450 psig (Mode 4). One of the steam generators transfers heat from the reactor coolant system to the steam supply system. The steam supply system transfers heat to the condenser. This heat removal process will continue to remove heat as long as a vacuum is maintained in the condenser. In the event that a fire damages this heat removal process and the normal residual heat removal system (RNS) or its support equipment, the PRHR HX will be available to remove decay heat. Should a fire occur inside containment, the PRHR system is provided with fire protection features that provide reasonable assurance that one passive shutdown path will be available.

The PRHR will be available during Mode 4 and Mode 5 with the RCS closed. If loss of RNS occurs during Mode 4, the PRHR will maintain the reactor in a stable shutdown condition for a long period of time. If loss of RNS occurs during Mode 5 with the RCS closed, the RCS will reheat to 420°F. The PRHR is available to maintain the reactor at stable shutdown conditions and allow sufficient time for operators to recover RNS. In-containment refueling water storage tank (IRWST) gutter isolation air-operated valves (V130 A/B) will be closed to direct IRWST condensate from the containment shell gutters back to the IRWST. In this configuration, PRHR will remove decay heat from the reactor coolant system for a long period of time.

Westinghouse incorporated design features in the AP600 plant that limit fire damage to the RNS system. This was accomplished by separating the redundant RNS components. RNS pumps and their associated cabling are located in separate fire areas. RNS pump A is located in fire area 1204 AF 01 and RNS pump B is located in fire area 1200 AF 01. RNS support equipment includes the component cooling water system and the service water system. In the event the component cooling water system, the service water system, and the fire protection water supply system are not available, a water connection is provided for fire truck pumpers to supply water to the secondary side of the RNS heat exchangers. The water connection is shown in Revision 18 to Figure 9.5.1-1, Sheet 2 of 3 of the SSAR. This configuration will allow RNS to continue to remove decay heat without the component cooling water system, the service water system, or the fire protection water supply system.

In SECY 94-084, the staff specifies that although these systems (RNS pumps and associated cabling) are not safety-related, a high level of confidence that active systems that have a safety role are available when challenged is expected. Therefore, applicants are to maintain the integrity of these fire protection features (such as fire barriers, sprinkler systems, location of storage and amount of transient combustibles). Applicant's administrative controls of combustibles procedures are to include limitations on the amount of combustibles in areas with redundant RNS cabling to ensure survivability of these systems. This is COL Action Item 9.5.1-4 (refer to Section 9.5.1 of this report).

The second cooldown stage is initiated at RCS temperatures less than 350°F (Mode 4) using RNS pumps and their support equipment to continue plant cooldown. At RCS temperatures below 200°F and 0 psig (Mode 5), the RCS may be opened for refueling or other maintenance activity. In the event RNS system is lost because of a fire in this plant configuration, IRWST can supply water for decay heat removal. Containment will be closed and if boiling occurs in the RCS, the steam will be condensed on the inner containment shell, and drained back into IRWST. In this configuration, the plant will remain in a stable condition until RNS can be placed back into service.

Based on Westinghouse meeting the guidance of NUREG 1449, the applicable portions of the SRP, and SECY-94-084 as it pertains to the RNS pumps and associated cabling, the staff concludes that the AP600 fire protection design for shutdown and refueling operations is acceptable.

19.3.8 Flood Protection

In NUREG-1449, the NRC stated that the safety significance of flooding or spills during shutdown depends on the equipment affected by the spills and that such spills are most often caused by human error. In Section 3.4.1 of the SSAR, Westinghouse discusses the flood protection measures that are applicable to the AP600 plant for postulated external flooding and internal flooding from plant system and component failures. In Section 6.2 of WCAP-14837, Revision 2 Westinghouse discusses the risk from internal flooding at shutdown.

All safety-related systems for the AP600 design are housed in the seismic Category I containment and auxiliary buildings. Seismic Category I structures are located such that the land slopes away from the structures. This assures that external flood water will drain away from the building and prevent pooling near the building. In addition, the actual grade is a few inches lower than building entrances to prevent surface water from entering doorways.

The AP600 design minimizes the number of penetrations through exterior walls below grade. Penetrations below the maximum flood level will be watertight and any process piping penetrating an exterior wall below grade either will be embedded in the wall or will be welded to a steel sleeve embedded in the wall. Exterior walls are designed for maximum hydrostatic loads as are penetrations through the wall.

One of the acceptable methods of flood protection incorporates a special design of walls and penetrations. The AP600 walls are reinforced concrete designed to resist the static and dynamic forces of the design-basis flood and incorporate water stops at construction joints to prevent in-leakage. Penetrations are sealed and also capable of withstanding the static and dynamic forces of the design-basis flood. The AP600 design has incorporated these protective features.

Redundant safety-related systems and components are physically separated from each other as well as from non-safety-related components. Therefore, the failure of a system or component may render one division of a safety-related system inoperable while the redundant

division is available to perform its safety function. Other protective features used to minimize the consequences of internal flooding include:

- structural enclosures
- structural barriers
- curbs and elevated thresholds
- leakage detection systems
- drainage systems

The flood sources that were considered in the internal flooding analysis included:

- high-energy piping (breaks and cracks)
- moderate-energy piping (through-wall cracks)
- pump mechanical seal failures
- storage tank ruptures
- actuation of fire suppression systems
- flow from upper elevations and adjacent areas

In the SSAR, Westinghouse identifies seven compartments inside containment which are subject to full or partial flooding. These are the reactor vessel cavity, two steam generator compartments, a vertical access tunnel, the chemical and volume control system (CVS) compartment and two passive core cooling system (PXS) compartments (PXS-A and PXS-B). Of these compartments, only the two PXS compartments contain safe-shutdown equipment. The PXS-A and PXS-B compartments and the CVS compartment inside containment are physically separated and isolated from each other by a structural wall so that flooding in one compartment cannot cause flooding in the other compartment. Inside these compartments, all the automatically actuated containment isolation valves (CIVs) are located above the maximum flood height with the exception of one normally closed CIV for the spent fuel pit cooling system in PXS-A and three normally closed CIVs for the normal residual heat removal (RHR) system in PXS-B. However, these CIVs are not required for safe shutdown operation and will not fail open under flooded conditions.

In the SSAR, Westinghouse identifies safety-related equipment in the auxiliary building that requires flood protection on a room-by-room basis, depending on the relative location of the equipment. The auxiliary building is separated into radiologically controlled areas (RCAs) and nonradiologically controlled areas (NRCAs). On each floor, structural walls and floor slabs 0.61- to 0.91-m (2- to 3-ft) wide areas separate these areas. The structures are designed to prevent floods which may occur in one area from propagating to another area. The NRCA is divided into a mechanical equipment and an electrical equipment area. The electrical equipment area is further divided into an area housing Class 1E electrical equipment and non-Class 1E electrical equipment.

The safe-shutdown equipment located in the NRCA is associated with the protection and safety monitoring system (I&C cabinets), the Class 1E dc system (Class 1E batteries and dc electrical equipment), and containment isolation. NRCAs are also designed to provide maximum separation between Class 1E and non-Class 1E electrical equipment. The AP600 design minimizes water sources in those portions of the NRCA housing Class 1E electrical equipment.

The main control room (MCR) and the remote shutdown workstation (RSW) are also located in the NRCA. The MCR and RSW are adequately protected from flooding as a result of limited sources of flood water, pipe routing, and drain paths.

The AP600 flooding protection scheme provides separation of the equipment and cabling for each of the four divisions of safe-shutdown equipment using 3-hour-fire-rated structural barriers. Areas containing safety-related equipment are physically separated from one another and from areas that do not contain safety-related equipment by sealed 3-hour-fire-rated barriers with no openings in the barriers. This defense-in-depth feature results in a small probability that flooding would affect more than one safety-related system or division. In addition, the design minimizes location of potential flood sources in safety-related equipment areas to the extent possible.

Flood detection and mitigation capability is provided in the AP600 design and is maintained during shutdown, even when parts of the automatic systems are rendered unavailable for preventive maintenance and testing. This is because compensatory measures are expected to be taken to maintain the detection and mitigation capability.

In the AP600 probabilistic risk assessment (PRA), Chapter 56, Westinghouse provides an evaluation of plant risk associated with the internal floods at shutdown. The objective of these analyses was to confirm that the design incorporates adequate capability to achieve safe shutdown following these events, by showing that the associated plant risk is sufficiently small. Deterministic criteria were used to screen out any areas in which the risk from flooding is clearly insignificant, on the basis of the lack of flood initiation sources or absence of equipment important to safe shutdown, as modeled in the internal events PRA. Because the plant is already in shutdown, an initiating event for the shutdown analysis was considered an event leading to a threat to equipment needed for the normal decay heat removal function through water submergence or spray.

The results from the shutdown flooding analyses confirmed that the inherent design characteristics of the AP600 provided an effective barrier against potential internal flooding hazards. This is true even considering several conservative assumptions used in the study, such as assuming total system failure for non-safety-related fluid systems if they are affected by flooding in any area and taking no credit for operation of sump pumps to mitigate the consequences of flooding.

The analysis identified eight internal flooding scenarios at shutdown. The total calculated contribution to core damage frequency (CDF) from internal flooding during safe shutdown is estimated to be 5E-11 per year. (The calculated contribution to CDF from internal flooding during mid-loop operation is estimated to be 1.5E-9 per year.)

The results of the AP600 analyses for internal flooding show that the AP600 design is adequate such that internal floods during shutdown do not represent a significant risk contribution. The results also show that safe shutdown following internal floods can be achieved, and an acceptably low level of risk attained, using only safety-related equipment. Therefore, the staff concludes that the AP600 design provides adequate flood protection for systems and components required to achieve and maintain safe shutdown, and is acceptable.

19.3.9 Outage Planning and Control

The technical findings of NUREG-1449 supported the determination that a comprehensive program for planning and controlling outage activities would reduce risk during shutdown by reducing the frequency of precursor events. The staff realizes that the ultimate responsibility for outage planning and control is within the scope of the plant owners and considers this a COL action item.

In Section 13.5.1 of the SSAR, Westinghouse includes insights from WCAP-14837, which requires the COL applicants to address plant procedures for normal and abnormal operations, emergency operation, refueling and outage planning, alarm response, maintenance, inspection, test and surveillance as well as administrative controls.

The staff will review the COL applicants' outage planning and control program and the COL applicants will have appropriately addressed the factors that improve low-power and shutdown operations. As a minimum, these factors will include the following important elements:

- an outage philosophy which includes safety as a primary consideration in outage planning and implementation
- separate organizations responsible for scheduling and overseeing the outage; provisions for an independent safety review team that would be assigned to perform final review and grant approval for outage activities
- control procedures which address both the initial outage plan and all safety-significant changes to schedule
- provisions to ensure that all activities receive adequate resources
- provisions to ensure defense in depth during shutdown and ensure that margins are not reduced; an alternate or backup system must be available if a safety system or a defense-in-depth system is removed from service
- provisions to ensure that all personnel involved in outage activities are adequately trained; this should include operator simulator training to the extent practicable; other plant personnel, including temporary personnel, should receive training commensurate with the outage tasks they will be performing

This is COL Action Item 19.3-1.

19.3.10 Operator Training and Emergency Response Guidelines

The staff determined in Chapter 2 of NUREG-1449 that it is important to have adequate procedures that give detailed guidance concerning responses to a loss of reactor vessel inventory or shutdown cooling capability. Also, the alternate strategies for recovery are important to reduce risk during shutdown conditions. During the course of its reviews, the staff requested that Westinghouse provide a description of the emergency response guidelines (ERGs) for the AP600 design for development of emergency operating procedure (EOPs) for

conditions including shutdown and mid-loop operations. Westinghouse submitted the report GW-GJR-100 "AP600 ERGs SHUTDOWN, Revision 1," July 28, 1995, as supplemented by GW-GJR-100 "AP600 ERGs SHUTDOWN, Revision 2," July 31, 1996, for staff review and approval. The detailed discussion of the AP600 ERGs, including shutdown condition is discussed in Section 18.9.3 of the SSAR. The staff's evaluation for this item can be found in Section 18.9.3 of this report.

## 19.4 Consideration of Potential Design Improvements Under Requirements of 10 CFR 50.34(f)

### 19.4.1 Introduction

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to "perform a plant/site specific probabilistic risk assessment, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant." In accordance with 10 CFR 52.47(a)(1)(ii), Westinghouse addressed 10 CFR 50.34(f)(1)(i) as documented in Appendix 1B of the SSAR. The staff's evaluation is presented below.

Westinghouse made extensive use of the results of the PRA to arrive at a final AP600 design. As a result, the estimated CDF and risk calculated for the AP600 is very low, both relative to operating PWR plants and in absolute terms. The low CDF and risk for the AP600 are a reflection of Westinghouse's efforts to minimize the effect of initiators/sequences that have been important contributors to CDF in previous PWR PRAs. This was done largely through incorporation of several passive design features and other design changes intended to make the plant safer, more available, and easier to operate. The design includes features to prevent the occurrence of core damage, as well as features to mitigate the progression and consequences of a core damage event, should one occur. The major preventive features and mitigative features which contribute to low CDF and low risk for the AP600 are discussed in Sections 19.1.2.1 and 19.1.2.2 of this report.

In response to 10 CFR 50.34(f)(1)(i), Westinghouse provided an evaluation of the AP600 design improvements in Appendix 1B of the SSAR. The Westinghouse evaluation of design alternatives was limited to internal events. On the basis of this evaluation, Westinghouse concluded that because of the small risk associated with the AP600 design (estimated at approximately 0.4 person-rem over a 60-year plant life) none of the design improvements considered were cost beneficial.

### 19.4.2 Estimate of Risk for AP600

#### 19.4.2.1 Westinghouse Estimates

Risk was defined in terms of person-rem, and was calculated by multiplying the yearly frequency of an event by its consequences. The consequences were defined as the effective whole body equivalent dose (50 year committed) to the total population within a 50-mile radius of the plant assuming a 24 hour exposure following the onset of core damage. Westinghouse used the MELCOR Accident Consequence Code System (MACCS), Version 1.5.11.1 to estimate accident consequences. Effective doses were estimated for each of six different release categories (RCs). The AP600 Level 1 and Level 2 PRA models were used to provide pertinent data related to accident sequences, accident progression, and source terms. The

ALWR site information described in the ALWR Requirements Document, Volume III, Annex B of Appendix A to Chapter 1, revision 5 and 6, was used to provide the meteorological and population data for the analysis. The ALWR reference site data were developed by EPRI to conservatively represent, that is, bound, the consequences at approximately 80 percent of the reactor sites in the United States. Because the EPRI URD did not provide sufficient topographical data to define the MACCS site input file, the site land use and crop data are on the basis of representative site data provided in the MACCS manual (NUREG/CR-4691, MELCOR accident consequence code system (MACCS) users guide, Volume 1).

The Westinghouse estimate of the offsite risk to the population within 80.5 km (50 mi.) of the site is provided in Table 1B.6-1 of Appendix 1B of the SSAR. The total risk for at-power internal events (excluding seismic, fire and flood events) is 7.3E-03 person-rem per year for the AP600 plant. This extremely low level of risk calculated by Westinghouse is primarily because of the low value predicted for the internal events CDF, specifically 1.7E-07 per reactor-year. Risk assessment studies for operating commercial PWRs typically estimate core damage frequencies that are one to two orders of magnitude higher than the AP600 CDF. These same commercial reactor studies typically predict large release frequencies (LRFs) that are one to two orders of magnitude larger than the Westinghouse LRF estimate for AP600 of 1.8E-08 per reactor-year.

Consistent with typical reactor PRA studies, the Westinghouse AP600 PRA and Westinghouse design alternative analyses are on the basis of an accident mission time of 24 hours. However, Westinghouse also estimated the population dose risk for a 72-hour PRA mission time. The 72-hour point-estimate population dose risk of 8.1E-03 person-rem/reactor-year is about 10 percent higher than the corresponding 24-hour dose risk of 7.3E-03 person-rem/reactor-year. These 24- and 72-hour dose risks are on the basis of the sum of risks associated with six individual RCs. For five of the six RCs, the risk increases ranged from 4 percent to 13 percent as the mission time was increased from 24 to 72 hours. In the remaining release category, late containment failure (CFL), the risk increased by about a factor of almost 13 as result of the mission time increase. However, release category CFL represents a negligible portion of the total risk (less than a 0.01 percent contribution to the risk) regardless of assumed mission time.

The staff's evaluation of AP600 design alternatives is on the basis of a 24-hour accident mission time. Per the discussion in the preceding paragraph, use of a more restrictive 72-hour mission time for the design alternative evaluations would not impact the cost/benefit calculations by more than about 10 percent. Given that the overall uncertainty in the PRA results is much greater than 10 percent, it was judged that the 24-hour mission time basis would be adequate for the design alternative evaluations.

Westinghouse, as part of their risk assessment sensitivity studies for the AP600, developed insights related to the reliability of the passive systems proposed for this design. The reliability of passive system components was varied and the change in the CDF was assessed. This analysis indicated that if the reliability of passive system check valves is assumed to decrease by a factor of 10 (increased failure probability), the total internal events CDF would only increase by a factor of about three (from 1.7E-07/reactor-year to 5.3E-07/reactor-year). The passive system check values included in this sensitivity analysis are associated with the following: core makeup tanks, accumulators, and the in containment refueling water storage

tank injection and recirculation functions. This result demonstrates that passive safety-related systems dependent on successful check valve operation will still provide substantial core protection, even if pessimistic check valve reliabilities are assumed.

19.4.2.2 Staff Review of Westinghouse Estimates

The staff reviewed the major models and assumptions entering into Westinghouse's risk estimate. Westinghouse based its risk estimate on three major elements: (1) the mean value CDF estimates from the Level 1 PRA; (2) the MAAP computer code and supporting deterministic analyses for evaluating accident progression, containment performance, fission-product releases (source terms); and (3) the MACCS computer code, combined with meteorology and population data for a bounding reactor site, for estimating offsite consequences.

As discussed in Section 19.1 of this chapter, the staff finds the approach used by Westinghouse for assessing CDF and containment performance to be logical and sufficient for describing and quantifying potential core damage sequences. Westinghouse also estimated the uncertainty inherent in the CDF estimate, which has been considered by the staff in assessing the merit of the design alternatives. The NRC staff has also performed a number of severe-accident confirmatory calculations, as described in Section 19.2 of this report. On the basis of Westinghouse and NRC calculations described therein, the staff concludes that Westinghouse's characterization of accident progression and containment performance is acceptable.

As part of the review of issues related to the level 2 PRA (Section 19.1.10 of this report) the staff reviewed Westinghouse's source term estimates for the major RCs and compared these predictions with estimates from NUREG-1150, where available. The staff found the source term estimates in reasonable agreement and concludes that the process for assigning source terms is acceptable. The staff also considered Westinghouse's use of the MACCS code in conjunction with the bounding site data in the EPRI requirements document, and concluded that this provides an acceptable basis for estimating the consequences associated with severe-accident releases for the AP600 design.

In summary, the staff considers Westinghouse's overall approach for quantifying the risk of severe accidents to be acceptable. Accordingly, the staff has based its assessment of the risk reduction potential for potential design improvements on Westinghouse's estimate of risk (0.4 person-rem over a 60-year plant life for internally initiated events). However, in view of the significant uncertainties inherent in risk estimates, the validity of the conclusions of this analysis were tested by considering the uncertainties in CDF and containment performance, as well as the potential for core damage from external events. This aspect of the review is discussed further in Section 19.4.7 of this report.

19.4.3 Identification of Potential Design Improvements

Westinghouse's process for identifying potential design enhancements and resulting set of potential enhancements is described in Section 19.4.3.1 of this report. The staff's review of Westinghouse's set of design alternatives is provided in Section 19.4.3.2 of this report.

19.4.3.1 Potential Design Improvements Identified by Westinghouse

The process used by Westinghouse to identify candidate design alternatives included a review of design alternatives for other plant designs, specifically Limerick, Comanche Peak, and the CE System 80+. Westinghouse also reviewed the results of the AP600 PRA to assess possible design alternatives. Other design alternatives came from suggestions from AP600 design personnel.

Documentation in Appendix 1B of the SSAR does not explicitly state whether plant improvements considered as part of the NRC's Containment Performance Improvement (CPI) program were included within Westinghouse's evaluation. However, in response to RAI 100.17 Westinghouse states that the types of design changes identified in the CPI program have already been considered as design alternatives or have been incorporated into the AP600 design. The improvement concepts identified in the CPI program were also evaluated in other documents reviewed by Westinghouse, specifically the CE System 80+ design alternative evaluations.

Westinghouse eliminated certain design improvements from further consideration on the basis that they are already incorporated into the AP600 design. Examples of design features already included in the design are:

- Hydrogen ignition system
- Reactor cavity flooding system
- Reactor coolant pump seal cooling (AP600 has canned motor pumps)
- Reactor coolant system depressurization
- External reactor vessel cooling
- Non-safety-grade containment sprays

On the basis of this screening, 14 potential design improvements were retained for further consideration. The design improvements are described in Section 1B.7 of the SSAR, and are summarized below.

(1) Upgrade the CVCS for Small LOCAs: The CVCS is currently capable of maintaining the RCS inventory for LOCAs for effective break sizes up to 0.97 cm (3/8 in.) in diameter. This design alternative would extend the capability of the CVCS so that it could maintain RCS inventory during small and intermediate size LOCAs (up to an effective break size of 15.2 cm (6 in.) in diameter). Implementation of this design alternative would require installation of IRWST and containment recirculation connections to the CVCS, as well as the addition of a second line from the CVCS pumps to the RCS. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 5.5E-04 person-rem/yr.

(2) Filtered Vent: This design alternative would involve the installation of a filtered containment vent, including all associated piping and penetrations. This modification would provide a means to vent containment to prevent catastrophic overpressure failures, as well as a filtering capability for source term release. The filtered vent would reduce the risk associated with late containment failures that might occur after failure of the passive containment cooling system (PCS). Note, however, that even if the PCS

fails, it is expected that air cooling will limit the containment pressure to less than the ultimate pressure. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 1.0E-03 person-rem/reactor-year.

(3) Self-Actuating Containment Isolation Valves: Self-actuation of containment isolation valves could be used to increase the likelihood of successful containment isolation during a severe accident. This design alternative would involve the addition of a self-actuating valve or enhancement of the existing containment isolation valves on normally-open containment penetrations (specifically those penetrations that provide normally-open pathways to the environment during power and normal shutdown conditions). The design alternative would provide for self-actuation in the event that containment conditions are indicative of a severe accident. Closed systems inside and outside containment, such as RNS and component cooling, would be excluded from this design alternative. The actuation of containment isolation valves would be automatically initiated in the event containment conditions are indicative of a severe accident. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 7.4E-04 person-rem/yr, which represents elimination of the containment isolation release category.

(4) Passive Containment Sprays: Installation of a passive safety-grade containment spray system could result in the following risk benefits: (1) scrubbing of fission products, primarily for containment isolation failure, (2) alternative means for flooding the reactor vessel (in-vessel retention) and (3) control containment pressure for cases in which the PCS has failed. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 6.9E-03 person-rem/yr, which represents elimination of all release categories except containment bypass.

(5) Active High Pressure Safety Injection System: A safety-related, active high pressure safety injection system could be added that would be capable of preventing a core melt for all events except excessive LOCA and ATWS. Note, however, that this design alternative is not consistent with the AP600 design objectives, in that the AP600 would change from a plant with passive systems to a plant with passive and active systems. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 6.1E-03 person-rem/yr.

(6) Steam Generator Shell-Side Heat Removal System: This design alternative would involve the installation of a passive safety-related heat removal system to the secondary side of the steam generators. This enhancement would provide closed loop secondary system cooling via the use of natural circulation and stored water cooling, thereby preventing loss of the primary heat sink given loss of startup feedwater and the passive RHR heat exchanger. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 5.3E-04 person-rem/yr.

(7) Direct Steam Generator Relief Flow to the IRWST: To prevent or reduce fission product release from bypassing containment during an SGTR event, flow from the steam generator safety and relief valves could be directed to the IRWST. An alternative, lower cost option of this design alternative would be to redirect flow only from the first stage safety valve to the IRWST. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 4.2E-04 person-rem/yr.

(8) Increased Steam Generator Pressure Capability: As an alternative to design alternative (8) above, another method could be used to prevent or reduce fission product release from bypassing containment during an SGTR event. This alternative method would involve an increase of the steam generator secondary side and safety valve set point to a level high enough so that an SGTR will not cause the secondary system safety valve to open. Although detailed analyses have not been performed, it is estimated that the secondary side design pressure would have to be increased by several hundred psi. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 4.2E-04 person-rem/yr.

(9) Secondary Containment Filtered Ventilation: This design alternative involves the installation of a passive charcoal and HEPA filter system for the middle and lower annulus region of the secondary concrete containment (below Elevation 135'-3"). Drawing a partial vacuum on the middle annulus via an eductor with motive power from compressed gas tanks would operate the filter system. This design alternative would reduce particulate fission product release from any failed containment penetrations. Westinghouse estimated that implementation of this design alternative would reduce plant risk by at most by 7.4E-04 person-rem/yr.

(10) Diverse IRWST Injection Valves: In the current design, a squib valve in series with a check valve isolates each of the four IRWST injection paths. To provide diversity, a modification could be made so that a different vendor provides the valves in two of the lines. This enhancement would reduce the likelihood of common cause failures of the four IRWST injection paths. Westinghouse estimated that implementation of this design alternative would reduce plant risk at most by 5.3E-03 person-rem/reactor-year, which represents elimination of all core damage sequences resulting from a failure of IRWST injection (3BE sequences).

(11) Diverse Containment Recirculation Valves: In the current design, a squib valve isolates each of the four containment recirculation paths. In two of the four paths, each of the squib valves is in series with a check valve. In the remaining two paths, each squib valve is in series with a motor-operated valve (MOV). To provide diversity, a modification could be made so that a different vendor provides the squib valves in two lines. This enhancement would reduce the likelihood of common cause failures of the four containment recirculation paths. Westinghouse estimated that implementation of this design alternative would reduce plant risk at most by 1.5E-04 person-rem per reactor-year, which represents elimination of all core damage sequences resulting from a failure of containment recirculation (3BL sequences).

(12) Ex-Vessel Core Catcher: This design alternative would inhibit core-concrete interaction (CCI), even in cases where the debris bed dries out. The enhancement would involve the design of a structure in the containment cavity or use of a special concrete or coating. The current AP600 design incorporates a wet cavity design in which ex-vessel cooling is used to maintain core debris within the vessel. In cases where reactor vessel flooding has failed, the PRA assumes that containment failure occurs from an ex-vessel steam explosion or CCI. Westinghouse estimated that implementation of this design alternative would reduce plant risk at most by 6.1E-03 person-rem/reactor-year.

(13) High Pressure Containment Design: A high-pressure containment design would prevent containment failures from severe accident phenomena such as steam explosions and hydrogen detonation. This proposed containment design would have a design pressure of approximately 300 psi, and include a passive cooling feature similar to the existing containment design. The high-pressure containment would reduce the likelihood of containment failures, although it would not reduce the frequency or magnitude of releases from an unisolated containment. Westinghouse estimated that implementation of this design alternative would reduce plant risk at most by 6.1E-03 person-rem/reactor-year.

(14) Increase Reliability of Diverse Actuation System: This design alternative involves an improvement in the reliability of the DAS. The DAS is a non-safety system that can automatically trip the reactor and turbine and actuate certain engineered safety features equipment if the protection and safety monitoring system is unable to perform these functions. In addition, the DAS provides diverse plant monitoring of selected plant parameters to guide manual operation and confirm reactor trip and ESF actuations. Westinghouse estimated that implementation of this design alternative would reduce plant risk at most by 2.2E-04 person-rem/reactor-year.

19.4.3.2 Staff Evaluation

The staff reviewed the set of potential design improvements identified by Westinghouse and finds it to be reasonably complete. The activity was accomplished by reviewing design alternatives associated with the following plants: Limerick, Comanche Peak, CE System 80+, Watts Bar (NUREG-0498), and the ABWR. Also surveyed were accident management strategies (NUREG/CR-5474), and alternatives identified through the Containment Performance Improvement (CPI) Program (NUREG/CR-5567, -5575, -5630, and -5562). The results of this assessment are summarized in Appendix A of "Review of Severe Accident Mitigation Design Alternatives (SAMDAs) for the Westinghouse AP600 Design", Science and Engineering Associates Inc., SEA 97-2708-010-A;1, August 29, 1997. That appendix briefly summarizes each of the design alternatives identified in the foregoing references. Also included are the Westinghouse AP600 design alternatives, which are discussed in Appendix 1B of the SSAR. More than 120 possible design alternatives were reviewed by the staff. The list includes most improvements identified as part of the NRC CPI program, and the improvements considered are a filtered containment vent and a flooded rubble bed core-retention device, two improvements specifically mentioned in NUREG-0660 for evaluation as part of TMI Item II.B.8 that would be applicable to the AP600. The list also includes potential design improvements oriented toward reducing the risk from major contributors to risk for AP600, including SGTR events.

Although several design alternatives were not included in the Westinghouse analysis, in most instances these design alternatives are either (1) already included in the AP600 design, or (2) bounded in terms of risk reduction by one or more of the design alternatives that were included in the Westinghouse analysis. In some other cases, design alternatives were pertinent only to boiling water reactors. The staff's preliminary review did not reveal any additional design alternatives that obviously should have been given consideration by Westinghouse. Also, Westinghouse considered some of the potential design alternatives identified in the above references to be considerations for accident management strategies rather than as design alternatives. The staff notes that the set of design improvements is not all inclusive, in that

additional, perhaps less-expensive design improvements could be postulated. However, the benefits offered by any additional modifications would not likely exceed those for the modifications evaluated, and the costs of alternative improvements are not expected to be less than those of the least expensive improvements evaluated, when the subsidiary costs associated with maintenance, procedures, and training is considered. The discussions in Appendix 1B of the SSAR do not provide the basis or the process used by Westinghouse for screening the many possible design alternatives to arrive at the final list of 14 selected for evaluation. Similarly, the RAI responses from Westinghouse provided little additional insights into the process used. Although the information provided does not demonstrate that the Westinghouse search for design alternatives was necessarily comprehensive, as noted above, the staff's review of the more than 120 candidate designs did not identify any new alternatives more likely to be cost-beneficial than those included in the AP600 design alternative evaluations. On this basis, the staff concludes that the set of potential design improvements identified by Westinghouse is acceptable.

19.4.4 Risk Reduction Potential of Design Improvements

19.4.4.1 Westinghouse Evaluation

Westinghouse assumed that each design alternative would work perfectly and completely eliminate the accident sequences that the design alternative addresses. This assumption is conservative, as it maximizes the benefit of each design alternative. The design alternative benefits were on the basis of the reduction of risk expressed in terms of whole body person-rem per year received by the total population within a 80.5-km (50-mi.) radius of the AP600 plant site. Each of the 14 design alternatives was evaluated separately. Westinghouse used analysis models and results contained in the AP600 PRA to estimate the risk reduction for each design alternative.

Westinghouse's risk reduction estimates for each potential design improvement are reported in Table 19.4-1 of this report. The bases for these estimates is provided in section 1.B.7 of the SSAR.

19.4.4.2 Staff Evaluation

The staff reviewed Westinghouse's bases for estimating the risk reduction associated with the various design improvements. Westinghouse conservatively assumed that each design alternative is completely effective in eliminating all risk associated with the sequences that the design alternative is intended to address. For example, the risk reduction assigned to passive containment sprays assumes that all release categories except containment bypass are eliminated. The staff concludes that the rationale and assumptions on which the risk reduction estimates for each design improvement are based are reasonable, and generally conservative.

The level of risk reduction estimated for the various design improvements is driven by two underlying assumptions in the methodology. Specifically, the Westinghouse risk reduction estimates reflect only the contribution from internal events initiated at power, and are on the basis of point estimate (mean) values without consideration of uncertainties in CDF or offsite consequences. Although this is consistent with the approach taken in previous design alternative evaluations, further consideration of these factors could lead to significantly higher

risk reduction values, given the extremely small CDF and risk estimates in the baseline PRA for internal events.

In assessing the risk reduction potential of design improvements for AP600, the staff has based its evaluation on Westinghouse's risk reduction estimates for the various design alternatives, in conjunction with supplementary parametric analyses in which the potential impact of external events and uncertainties were evaluated. These analyses are discussed further in Section 19.4.7 of this report.

### 19.4.5 Cost Impacts of Candidate Design Improvements

Capital cost estimates for the design alternatives evaluated by Westinghouse for the AP600 are discussed in Sections 1B.4.2, 1B.4.3, and 1B.8 of the SSAR. The results of the cost evaluations are presented in Table 1B.8-1 of the SSAR. In Table 1B.8-1, Westinghouse lists, for each design alternative, the potential risk reduction, the capital benefit assuming the design alternative was highly effective in reducing accident risks, the capital cost, and the net capital benefit. The cost evaluations did not account for factors such as design engineering, testing, and maintenance associated with each design alternative. These factors, if included, would increase the overall costs and decrease the capital benefits of each alternative. Thus, this approach is conservative.

The staff compared the capital costs for the AP600 design alternatives with those evaluated for the ABWR and CE System 80+. This comparison was performed in order to gauge the reasonableness of the cost estimates presented by Westinghouse in the SSAR. There is not an exact match in the design alternatives among the reactor designs, so only rough comparisons are possible - for example, the AP600 "Active High Pressure Safety Injection System," which is estimated to cost $20 million. This design alternative adds an active high pressure safety injection pump and associated piping, valves and supports to the AP600, and thus adds a complete new safety-related system. It can be compared to the "Alternative High Pressure Safety Injection" for the CE System 80+, which is estimated to cost $2.2 million. However, the design alternative for the CE System 80+ simply adds parallel piping and valves to an existing system, which would be expected to cost only a fraction of the total system cost. The "Filtered Containment Vent" for the AP600 can be compared to systems with similar functions for the ABWR and the CE System 80+. The estimated costs for the three venting systems are $5 million, $3 million, and $10 million, respectively, for the AP600, ABWR, and CE System 80+. These costs are in reasonable agreement with each other. The costs for "non-safety grade containment spray" for AP600, which was evaluated in an earlier version of SSAR Section 1B prior to its incorporation into the AP600 design, can be compared to the "Reactor Building Sprays" for the ABWR and the "Alternative Containment Spray" for CE System 80+. This AP600 design alternative consists of the addition of piping and spray headers inside containment, and connects to an existing fire water system. For the ABWR, similarly, the existing in-containment fire spray system would be modified to provide sprays in areas vulnerable to fission product release. The ABWR modification would thus be limited to providing sprays only to selected areas of containment. This design alternative for CE System 80+ consists of the addition of piping to connect to the existing in-containment spray system, together with new pumps to supply the water. Estimated costs for these three spray systems were $415,000 for AP600, $100,000 for the ABWR, and $1.5 million for CE System 80+. In light of the scope differences among these design alternatives, the estimates for the AP600 spray system appear to be reasonable. These comparisons indicate that the cost estimates for

several of the AP600 design alternatives are in reasonable agreement with the costs for roughly similar design alternatives evaluated for the ABWR and the CE System 80+.

A further check of the reasonableness of the AP600 design alternative cost estimates was performed by developing independent cost estimates for one particular design alternative, the active, non-safety-related containment spray system. This analysis was performed prior to the incorporation of the non-safety-grade spray system into the AP600 (and the deletion of this design alternative from SSAR Section 1B). The first assessment assumed the addition of fire protection system grade spray headers and supply piping inside containment (carbon steel), and the addition of control valves and piping outside containment which would connect to the existing fire water supply system. The resulting costs for containment spray system ranged from about $300,000 to $350,000 (1996 dollars), depending on the assumptions made on the required pipe size. These independent estimates did not include design engineering or first-of-a-kind costs, nor did they include allowances for associated personnel training, procedure development, or recurring operations and maintenance costs. This approach is similar to that used by Westinghouse for cost estimation. Thus, the Westinghouse estimate of $415,000 for this design alternative is in reasonable agreement with the independent estimate. An additional independent cost estimate was also developed for a containment spray system similar to that described above, but which included increased pumping capacity. The increased pumping capacity is needed since the Westinghouse letter of March 13, 1997, indicated the currently-designed fire water supply system is capable of delivering less than 1.89 kL/min (500 gpm) to the proposed containment spray system. The system evaluated for this alternative would increase the fire water pump capacity so that each pump was capable of delivering 11.36 kL/min (3000 gpm) to the containment sprays against a containment pressure of 310.3 kPa (30 psig). The currently-included piping supplying fire water to the containment would be increased in size to reduce the flow resistance. This modification to the AP600 was estimated to cost about $370,000 (1996 dollars). As with the foregoing estimate, no allowance was made for personnel training, procedure development, or recurring operations and maintenance costs.

On the basis of the staff's audit the staff views Westinghouse's approximate cost estimates as adequate, given the uncertainties surrounding the underlying cost estimates, and the level of precision necessary given the greater uncertainty inherent on the benefit side, with which these costs were compared.

### 19.4.6 Cost-Benefit Comparison

A cost-benefit comparison was performed to determine whether any of the potential severe-accident design features could be justified. Westinghouse assessed the benefits of each design alternative in terms of potential risk reduction, which was defined as the reduction in whole body person-rem per year received by the total population within a 80.5-km (50-mi.) radius of the AP600 plant site. One person-rem of averted offsite exposure was assigned a value of $1,000, and was assumed to account for both health effects and offsite property damage. This value was treated as the annual levelized benefit for averted risk. To determine the maximum expenditure justified by a given reduction in risk ("maximum capital benefit"), Westinghouse divided the annual levelized benefit by the annual levelized fixed charge rate. The annual levelized fixed charge rate was determined to be 15.7 percent in current U.S. dollars on the basis of factors and methods provided in EPRI and DOE documents

(EPRI P-6587-L and DOE/NE-0095). The Westinghouse approach that was used in calculating the fixed charge rate employed a component "book life" of 30 years. The use of this high charge rate tends to minimize the capital benefit associated with each design alternative. The 30-year life that was used in the calculations makes little difference in the economic benefit compared to the more typical 60-year life, particularly when the high levelized annual fixed charge rate of 15.7 percent is used.

The Westinghouse approach for calculating the benefits or reduced risk from each individual design alternative also does not give any credit for averted onsite property damage and replacement energy costs which are realized through a reduction in accident frequency. The onsite property damage and replacement energy costs may have been neglected because estimated CDF is very low. However, as indicated below, these on-site considerations can add substantially to the benefits achievable with design alternatives. Westinghouse's cost-benefit estimates for each potential improvement are reported in Table 19.4-1 of this report using a screening criterion of $1,000/person-rem-averted to identify whether any of the design improvements could be cost effective. As shown in Table 19.4-1, the highest capital benefit calculated by Westinghouse for any design alternative is about $50, whereas the capital cost for the least expensive design alternative is $33,000. On this basis, Westinghouse concluded that no additional modifications to the AP600 design are warranted.

The NRC recently updated its recommended approach for the monetary conversion of radiation exposures. Previous guidance specified that one-person rem of exposure should be valued at $1,000. This conversion factor for offsite doses was intended to account for both health effects and offsite property damage, and exposures incurred in future years were not to be discounted. The recent guidance given in NRC's regulatory analysis guidelines (NUREG/BR-0058 Revision 2), recommends the use of $2,000 per person-rem of exposure as the monetary conversion factor. For assessing values and impacts, future exposures are to be discounted to arrive at their present worth. In addition, offsite property damage from nuclear accidents is to be separately valued and is not part of the $2,000 per person-rem value.

Evaluations recently performed by Brookhaven National Laboratory for the NRC assessed total costs associated with offsite releases, including both health effects and property damage/loss effects (NUREG/CR-6349). Costs were assessed for each of the five NUREG-1150 plants, Grand Gulf, Peach Bottom, Sequoyah, Surry and Zion. The results indicated that overall costs associated with offsite releases of radioactive materials, presented on a cost per person-rem of exposure to the public, ranged from about $2,000 to more than $5,000 per person-rem, depending on factors such as the assumed interdiction criteria. A criterion of $3,000 per person-rem averted was added to account for offsite property damage and other related costs for severe accidents. Thus, the Westinghouse cost/benefit evaluation approach used for AP600 design alternatives is not consistent with the approach recommended in NUREG/BR-0058 Revision 2. The key differences are summarized in Table 19.4-2 of this report. The staff's independent evaluation is found below.

The NRC's recommended approach in NUREG/BR-0058 Revision 2 was applied to the design alternatives identified for the AP600 to arrive at a baseline potential benefit from the reduction in offsite risk. This assessment used a discount rate of 7 percent and assumed a reactor life of 60 years. The averted risk for each design alternative was taken from Table 1B.8-1 of the SSAR. Two monetary conversion factors for radiation exposures have been used in the staff's assessment. The first is the $2,000/person-rem recommended in NUREG/BR-0058 Revision 2.

The second is $5,000/person-rem, and is intended to account for offsite property damage as well as offsite health effects. The results for each design alternative are shown in columns 5 and 6 of Table 19.4-1. For comparison purposes, Westinghouse's estimate of the capital cost, averted risk, and capital benefit for each design alternative is also presented (columns 2, 3, and 4 of Table 19.4-1). A perfect design alternative would reduce the CDF to zero and/or reduce offsite releases to zero. Estimated benefits from a perfect design alternative are also shown for each of the alternative cost bases (last row of Table 19.4-1).

The results shown in Table 19.4-1 indicate that the benefits calculated using a 7 percent discount rate, a 60-year plant life, and a $2,000/person-rem conversion factor is about a factor of four higher than those calculated by Westinghouse. The benefits calculated using $5,000/person-rem are about a factor of 10 higher than those estimated by Westinghouse. The highest capital benefit shown in Table 19.4-1 amounts to less than $500, whereas the capital cost for the least expensive design alternative is $33,000. Thus, even with the highest benefit basis ($5,000/person-rem, 7 percent discount rate, 60-year life), the calculated benefits are almost two orders of magnitude too small to justify the addition of any of the design alternatives listed. It should be noted, however, that the above assessment neglects the benefits from averted onsite costs which are relevant for design alternatives that reduce core damage frequency. Dollar savings derived from averted onsite costs are treated as an offset or reduction in the capital cost of the design alternative in the staff's analysis. Averted onsite costs are significant for certain design alternatives and are considered further below.

19.4.7 Further Considerations

The estimates of potential design alternative benefits listed in Table 19.4-1 of this report are all on the basis of the Westinghouse estimates of averted risk and neglect the benefits from averted onsite costs. As mentioned in Section 19.4.4.2 of this report, the Westinghouse estimates of risk do not account for uncertainties either in the CDF or in the offsite radiation exposures resulting from a core damage event. The uncertainties in both of these key elements are fairly large since key safety features of the AP600 design are unique, and their reliability has been evaluated through analysis and testing programs rather than operating experience. In addition, the estimates of CDF and offsite exposures do not account for the added risk from external events such as earthquakes.

The staff performed a screening of the candidate design improvements to determine whether any of the design alternatives could be cost-beneficial when uncertainties, the added risk from external events, and averted onsite costs are incorporated into the cost-benefit analysis. A more detailed assessment was then performed for those design alternatives having potentially favorable cost-benefit factors under these more limiting considerations. These analyses are discussed in the sections below.

Uncertainties in Core Damage Frequency and Accident-Related Exposures

The uncertainty in the estimated CDF for the AP600 plant was provided in Revision 8 to the PRA. The CDF uncertainty distribution was characterized by an error factor (EF) of about 5.7. Assuming a log normal distribution, the error factor is the ratio of the 95th percentile to the median, and also the ratio of the median to the 5th percentile. Thus, the CDF for internal events could be a factor of six higher or lower than assumed in the above analysis.

Additional factors that could substantially increase the estimated CDF for the AP600 plant are the contributions from events and accident sequences not yet accounted for in the PRA. These include both accident sequences that have not yet been identified and identified sequences that have not yet been analyzed. An example of the latter is external events such as fire and earthquake. External events contributions to CDF are not included in the base estimate of 1.7E-07/reactor-year. In the PRA, Westinghouse indicated that external events, in particular internal fires, are estimated to increase the CDF by about a factor of four. The potential contributions from seismic events were not defined in the PRA available for this study. However, earthquakes could readily increase the CDF by an order of magnitude or more. These external events can also degrade the containment performance so that the releases from containment may also be higher than for accidents from internal events.

The potential increases in CDF because of accident sequences not yet identified is very difficult to estimate. Presumably the contributions from as-yet unknown sequences should be small if the PRA has been performed in a thorough and systematic manner. For the purposes of the present analysis the effects of these sequences are assumed to be captured by the potential increase in CDF because of external events.

Westinghouse presented offsite exposures for the major RCs defined for the AP600 plant in the Section 1B.6 of the SSAR. On the basis of the CDF reference value of 1.7E-07/reactor-year and the total risk of 7.3E-03 person-rem/reactor-year, the "average" offsite exposure is estimated to be on the order of 50,000 person-rem per core damage event. The uncertainty in the estimated releases was not provided in the Westinghouse documentation.

The average offsite exposure of 50,000 person-rem per AP600 core damage event as estimated by Westinghouse is a factor of 2.7 lower than the average public exposures calculated for the five NUREG-1150 current-generation nuclear plants (after adjusting the NUREG-1150 plant releases to that of a 600-Mwe size plant). The better performance of the AP600 may be due, in part, to the high likelihood of successful RCS depressurization and in-vessel retention of damaged fuel in the AP600 design and to methods and assumptions for defining source terms.

Uncertainties in the offsite exposure estimates for AP600 are significant. As described in Section 19.1.3.3.3 of this report, the AP600 risk profile is shaped by several major assumptions regarding containment failure modes and release characteristics including: (1) conservative assumptions regarding early containment failure from ex-vessel phenomena, (2) optimistic assumptions that external reactor vessel cooling will always prevent reactor pressure vessel breach, and (3) substantial credit for additional aerosol removal in SGTR events. If early containment failure is avoided (as suggested by deterministic calculations performed subsequent to the PRA) and reactor pressure vessel breach instead results in a more benign release (e.g., a containment failure in the intermediate time frame), overall risk for internal events would be reduced by about a factor of two. If credit for external reactor vessel cooling (ERVC) is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption that ERVC always fails and leads to early containment failure, the containment failure frequency would approach the core melt frequency and risk would increase by a factor of 20 (to about 0.16 person-rem/y). If the decontamination factor (DF) of 100 applied to the MAAP-predicted aerosol release fractions for SGTR events (to account for fission product removal by impaction on steam generator tubes) is not realized,

offsite risk can be significantly impacted. With this credit for aerosol removal, the risk contribution from a containment bypass is minimal (6 percent of the total). Without this credit, overall risk for internal events would increase by a factor of seven and would be dominated by bypass releases. Finally, the impact of the non-safety containment spray system on fission product releases was not credited in the PRA. Containment sprays could significantly reduce the estimated risk in the baseline PRA (by perhaps a factor of 2) since the sprays would be effective in reducing the source terms in the risk-dominant RCs, i.e., early containment failure (CFE) and containment isolation failure (CI). However, sprays would not impact releases from SGTR events.

In summary, the actual offsite exposure could range from a factor of two lower to an order of magnitude higher than the Westinghouse estimate, given the uncertainties in the underlying analyses of containment performance. This uncertainty range was factored into the staff's reassessment discussed below.

Reassessment of Design Alternative Benefit-Cost Relationships in Light of Uncertainties

Analyses were performed to assess AP600 design alternative benefits taking into account the uncertainties in estimated CDF, offsite releases of radioactive materials given a severe accident, and the effects of external events. Estimates were made of the maximum benefits that can be achieved with AP600 design alternatives, assuming a design alternative can either completely eliminate all core damage events or completely eliminate offsite releases of radioactive materials if a severe accident does occur. The estimates of benefits were calculated using the NRC developed FORECAST code (NUREG/CR-5595, Revision 1, "FORECAST: Regulatory Effects Cost Analysis Software Manual, Version 4.1", Science and Engineering Associates, Inc., July 1996). FORECAST allows the use of uncertainty ranges for all key parameters and provides a means for combining uncertainties in these parameters. It also provides a distribution for the bottom line costs or benefits, and thus presents a picture of the uncertainty on the bottom line figures. Key parameters used in evaluating the maximum potential benefit are provided in Table 19.4-3

For the purposes of estimating the maximum potential benefit from AP600 design alternatives, external events and accident sequences not yet accounted for in the PRA were assumed to increase the reference CDF by two orders of magnitude, i.e., a factor of 100. An error factor of six was used for this higher CDF. Cases were evaluated assuming the reference value of 50,000 person-rem per accident. The results of the analysis are presented in the Table 19.4-4 of this report.

The entries in Table 19.4-4 indicate that design alternatives which prevent accidents (reduce the accident frequency to zero) are much more cost effective than design alternatives which reduce or eliminate offsite releases but which have no effect on accident frequency. This is because of the fairly large benefits associated with averted onsite cleanup and decontamination costs, and with avoided replacement energy costs, neither of which are assumed to be impacted by design alternatives which do not reduce accident frequency.

Case 1 is the reference case utilizing the base CDF and Westinghouse-estimated offsite exposures. The estimated benefits are considerably higher than those cited in Table 19.4-1 of

this report, primarily because of the inclusion of averted onsite cleanup and decontamination costs and averted replacement energy costs.

Cases 2 and 3 show the effects of the higher CDF associated with external events, but they do not include the effects of possible higher releases from containment because of such events (base offsite exposure of 50,000 person-rem/event retained). These cases may be used as the basic benefits including external events and further assuming that containment performance would not be impacted by external events. Case 2 shows the potential benefit range for a design alternative which could reduce the accident frequency to zero. Case 3 applies to a design alternative which would eliminate all offsite releases but which would not impact the CDF.

Table 19.4-5 of this report combines the information in Tables 19.4-1 and 19.4-4 to estimate the total benefit possible from specific design alternatives. The design alternatives are divided between those that impact the CDF and those that impact containment performance but not the CDF. Benefits have been estimated by taking the fractional reduction in risk for each design alternative (compared to the AP600 baseline risk as defined by Westinghouse) and applying that fraction to the mean benefits displayed in Table 19.4-4. Design alternatives that reduce the CDF were applied to the Case 2 mean benefit, while those that only effect containment performance were applied to the Case 3 mean benefit.

The first sets of values shown in Table 19.4-5 (Columns 4 through 7) are on the basis of benefits calculated using the mean values. The second set of values (Columns 8 through 11) was calculated using the 95$^{th}$ percentile value. The latter set shows the potential design alternative benefits at which there is only a 5 percent chance that the benefits will be greater than the values shown.

The use of the maximum benefits typically improves the cost/benefit ratio by a factor of approximately five, but does not alter any of the overall conclusions about design alternatives that have acceptable cost/benefit ratios.

Further Evaluation of Design Alternatives With Potentially Favorable Benefit -Cost Factors

Design alternatives that are within a decade of meeting the benefit-cost criteria of $5,000/person-rem were to be subjected to further probabilistic and deterministic considerations, including a qualitative assessment of the following:

- the impact of additional benefits that could accrue for the design alternative if it would be effective in reducing risk from certain external events, as well as internal events
- the effects of improvements already made at the plant
- any operational disadvantage associated with the potential design alternative

None of the design alternatives have a cost benefit ratio of less than $5,000/person-rem. The only design alternatives which come within a decade of the $5,000/person-rem standard are the diverse IRWST valves at $19,800/person-rem and the self-actuating containment isolation valves at $33,700/person-rem.

Diverse IRWST Injection Valves

In the current AP600 design, a squib valve in series with a check valve isolates each of four IRWST injection paths. This design alternative would reduce the likelihood of common cause failures of IRWST injection to the reactor by utilizing diverse valves in 2 of the 4 lines. This design alternative, if it functioned perfectly, could potentially reduce the CDF by about 72 percent. When taking into account external events, other accident sequences not yet included in the AP600 PRA, and other uncertainties, this design alternative is estimated to be highly cost effective. In the absence of a comprehensive external events PRA for the AP600 plant, it is difficult to estimate the effectiveness of this design alternative in reducing the risk from such events. However, it appears likely that failure to inject coolant to the reactor would remain a prominent contributor to the CDF from external events, in which case diversity in the IRWST injection valves should help to reduce the risk from external events as well as internal events.

For the check valves, alternate vendors are available. However, it is questionable if check valves of different vendors would be sufficiently different to be considered diverse unless the type of check valve was changed from the current swing disk check to another type. The swing disk type is preferred for this application and other types are considered less reliable.

Adding diversity to the injection line squib valves would require additional spares at the plant, and some additional training for plant operations and maintenance staff, but would not appear to add significantly to the operational aspects of the AP600. However, a greater issue concerns the availability and costs of acquiring diverse valves from a second vendor. Squib valves are specialized valve designs for which there are few vendors. Westinghouse claims that a vendor may not be willing to design, qualify, and build a reasonable squib valve design for this AP600 application considering that they would only supply two valves per plant. The cost estimate for this design alternative assumes that a second squib valve vendor exists and that vendor only provides the two diverse IRWST squib valves. The cost impact does not include the additional first time engineering and qualification testing that will be incurred by the second vendor. Westinghouse estimated that those costs could be more than a million dollars. As a result, Westinghouse concluded that this design alternative would not be practicable because of the uncertainty in availability of a second squib valve design/vendor and because of the uncertainty in reliability of another check valve type. The staff considers the rationale set forth by Westinghouse regarding the potential reductions in reliability and high costs associated with obtaining diverse valves to be reasonable. On the bases of these arguments the staff concludes that this design alternative need not be further pursued.

Self-Actuating Containment Isolation Valves

This design alternative would reduce the likelihood of containment isolation failure by adding self-actuating valves or enhancing the existing containment isolation valves for automatic closure when containment conditions indicate a severe accident has occurred. Conceptually, the design would either be an independent valve or an appendage to an existing fail-closed valve that would respond to post-accident containment conditions within containment. For example, a fusible link would melt in response to elevated ambient temperatures resulting in venting the air operator of a fail-closed valve, thus providing the self-actuating function. This design alternative is estimated to impact releases from containment by only 10 percent. It has

a cost-benefit ratio of $33,000/person-rem, and achieves this ratio primarily because of its low capital costs.

This improvement to the containment isolation capability would appear to be effective in reducing off-site releases for accidents involving external events as well as internal events. Also, the effectiveness of this design alternative would not be affected by the design changes made as a result of the AP600 PRA.

The addition of this design alternative would impose minor operational disadvantages to the plant in that the operations and maintenance staff would require some additional training. In addition, these automatic features would require periodic testing to assure that they are functioning properly.

Perhaps the biggest question regarding this design alternative is whether or not it can be implemented for a cost of only $33,000. The cost estimate does not appear to include the first time engineering and qualification testing that would be required to demonstrate that the valve would perform its intended function in a timely and reliable manner. The costs associated with periodic testing and maintenance also do not appear to have been included. The staff believes that the actual costs of this design alternative would be substantially higher than Westinghouse's estimate (perhaps by a factor of 10) when all related costs are realistically considered. On the basis of the unfavorable cost-benefit ratio, and the expectation that actual costs would be even higher than estimated by Westinghouse, the staff concludes that this design alternative is not cost beneficial and need not be further evaluated.

### 19.4.8 Conclusions

As discussed in Section 19.1 of this report, Westinghouse made extensive use of the results of the PRA to arrive at a final AP600 design. As a result, the estimated CDF and risk calculated for the AP600 plant are very low both relative to operating plants and in absolute terms. The low CDF and risk for the AP600 plant are a reflection of Westinghouse's efforts to systematically minimize the effect of initiators/sequences that have been important contributors to CDF in previous PWR PRAs. This has been done largely through the incorporation of a number of hardware improvements in the AP600 design. These and additional AP600 design features which contribute to low CDF and risk for the AP600 are discussed in Section 19.1 of this report.

Because the AP600 design already contains numerous plant features oriented toward reducing CDF and risk, the benefits and risk reduction potential of additional plant improvements is significantly reduced. This is true for both internally and externally initiated events. Moreover, with the features already incorporated in the AP600 design, the ability to estimate CDF and risk approaches the limitations of probabilistic techniques. Specifically, when CDFs of 1 in 100,000 or 1,000,000 years are estimated in a PRA, it is the area of the PRA where modeling is least complete, or supporting data is sparse or even nonexistent, that could actually be the more important contributors to risk. Areas not modeled or incompletely modeled include human reliability, sabotage, rare initiating events, construction or design errors, and systems interactions. Although improvements in the modeling of these areas may introduce additional contributors to CDF and risk, the staff does not expect that additional contributions would change anything in absolute terms.

In 10 CFR 50.34(f)(1)(I), the NRC requires an applicant to perform a plant/site-specific PRA, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant. The staff concludes that the AP600 PRA, and Westinghouse's use of the insights of this study to improve the design of the AP600 meet this requirement. The staff concurs with the Westinghouse conclusion that none of the potential design modifications evaluated are justified on the basis of cost-benefit considerations. It is further concluded that it is unlikely that any other design changes would be justified on the basis of person-rem exposure considerations, because the estimated CDFs would remain very low on an absolute scale.

Table 19.1-1 Comparison of Core Damage Frequency Contributions by Initiating Event

| **Initiating Event** | AP600 (CDF/yr) | Operating PWRs (CDF range/yr) IPE results [NUREG-1560] |
|---|---|---|
| LOCAs (Total) | 1.5E-7 | 1E-6 to 8E-5 |
| - Large | 5.0E-8 | |
| - Safety Injection Line Break | 4.0E-8 | |
| - Intermediate | 3.0E-8 | |
| - Medium | 6.0E-9 | |
| - Small | 4.0E-9 | |
| - CMT Line Break | 4.0E-9 | |
| - RCS Leak | 3.0E-9 | |
| Steam Generator Tube Rupture (SGTR) | 6E-9 | 9E-9 to 3E-5 |
| Transients | 6E-9 | 5E-7 to 3E-4 |
| Loss of Offsite Power/Station Blackout | 1E-9 | 1E-8 to 7E-5 |
| Anticipated Transient Without Scram (ATWS) | 1E-8 | 1E-8 to 4E-5 |
| Interfacing System LOCA | 5E-11 | 1E-9 to 8E-6 |
| Vessel Rupture | 1E-8 | 1E-7 |
| Total | 2E-7 | 4E-6 to 3E-4 |

Table 19.1-2 Level 1 Accident Class Functional Definitions and Core Damage Frequencies

| Accident Class | Definition | RCS Pressure at Uncovery | CDF | % of Total CDF |
|---|---|---|---|---|
| 1A | Core damage with RCS at high pressure following transient or RCS leak | >1100 | 1.83E-9 | 1.1 |
| 1AP | Core damage with no depressurization following small LOCA and RCS leak with passive RHR operating, or intermediate LOCA | ~1100 | 3.20E-9 | 1.9 |
| 3A | Core damage with RCS at high pressure following ATWS or main steamline break inside containment | >1100 | 1.01E-8 | 6.0 |
| 3BR | Core damage following large LOCA with full RCS depressurization, but accumulator failed | ~0 | 7.68E-9 | 4.5 |
| 3BE | Core damage following large LOCAs or other event with full depressurization | ~0 | 7.79E-8 | 46.0 |
| 3BL | Core damage at long term following failure of water recirculation to RPV after successful gravity injection | ~0 | 4.35E-8 | 25.7 |
| 3C | Core damage following vessel rupture | ~0 | 1.0E-8 | 6.0 |
| 1D | Core damage with partial depressurization of RCS following transient | <150 | 6.23E-9 | 3.7 |
| 3D | Core damage following LOCA (except large) with partial depressurization | | | |
| 6E | Core damage following SGTR or ISLOCA. Early core damage (loss of injection) | Sequence Specific | 8.71E-9 | 5.1 |
| 6L | Core damage following SGTR. Late core damage (loss of recirculation) | | | |
| TOTAL | | | 1.69E-7 | 100.0 |

Table 19.1-3 Conditional Containment Failure Probability by Accident Class

| Accident Class | CCFP (%) |
|---|---|
| 1A | 97.3 |
| 1AP | 33.1 |
| 3A | 41.7 |
| 3BR | 0.2 |
| 3BE | 7.1 |
| 3BL | 0.2 |
| 3C | 10.3 |
| 3D/1D | 5.2 |
| 6E/6L | 48.4 |
| Weighted Average* | 10.8 |

*Weighted on the basis of core damage frequencies provided in Table 19.1-2

Table 19.1-4 Containment Release Categories and Associated Frequencies

| Containment Release Category | Frequency | % of CDF | % of LRF |
|---|---|---|---|
| Intact Containment (IC) | 1.5E-7 | 89 | NA |
| Early Containment Failure (CFE) | 6.6E-9 | 4 | 36 |
| Intermediate Containment Failure (CFI) | 1.3E-11 | <0.1 | <0.1 |
| Late Containment Failure (CFL) | 1.5E-11 | <0.1 | <0.1 |
| Containment Isolation Failure (CI) | 3.6E-10 | 0.2 | 2 |
| Containment Bypass (BP) | 1.1E-8 | 7 | 62 |
| Total | 1.7E-7 | 100 | 100 |

Table 19.1-5 Contribution to Risk from Various Release Categories, as Reported by Westinghouse (72 Hour Mission Time)

| Containment Release Category | Frequency | P-Rem/Event | P-Rem/y | % Risk |
|---|---|---|---|---|
| Intact Containment (IC) | 1.5E-7 | 3.3E2 | 5.0E-5 | 0.6 |
| Early Containment Failure (CFE) | 6.6E-9 | 1.0E6 | 6.8E-3 | 83.9 |
| Intermediate Containment Failure (CFI) | 1.3E-11 | 3.5E5 | 4.6E-6 | 0.06 |
| Late Containment Failure (CFL) | 1.5E-11 | 1.5E4 | 2.2E-7 | -- |
| Containment Isolation Failure (CI) | 3.6E-10 | 2.1E6 | 7.7E-4 | 9.6 |
| Containment Bypass (BP) | 1.1E-8 | 4.2E4 | 4.7E-4 | 5.8 |
| Total | 1.7E-7 | | 8.1E-3 | 100 |

Table 19.2-1 Treatment of Intangible Parameters for AP600

| Intangible Parameter | Prescription in the Report |
|---|---|
| Location of Failure | Single location argued based on melt relocation scenario (sideways failure) |
| Release Rates | Release rates of 100, 200, and 400 kg/s used; rates comparable to TMI-2 |
| Melt Length Scale | Initial melt length scales of 20 mm, 40 mm, and 80 mm; smaller than 20 mm length scales considered through breakup rate variation |
| Breakup Rate (Parameter) | Rapid, intermediate, and slow (i.e., virtually no) breakup rates considered |
| Trigger Strength | Sufficient strength (~ 100 bar) considered for triggering an explosion |
| Trigger Timing and Location | Several trigger times considered for different breakup rates; trigger locations varied (extent unspecified) |

Table 19.2-2 Input Parameters for Westinghouse TEXAS Calculations

| Input Parameter | Hinged Mode | Localized | Sensitivity |
|---|---|---|---|
| Melt Composition | Steel | Steel | Steel |
| Melt Density ($kg/m^3$) | 7800 | 7800 | 7800 |
| Melt Temperature (°K) | 1890 | 1890 | 1910 |
| Melt Superheat (°K) | 80 | 80 | 100 |
| Jet Diameter (m) | 0.068 | 0.060 | 0.060 |
| Number of Jets | 236 | 1 | 1 |
| Jet Velocity (m/s) | 2.26 | 0.17 | 0.17 |
| Melt Flow rate (kg/s) | 15,100 | 3.8 | 3.8 |
| Water Pool Depth* (m) | 3.89<br>0.46 | 3.89<br>0.46 | 3.89<br>0.46 |
| Nominal Pool Area ($m^2$) | 20 | 2.5 | 5.0 |
| Water Temperature (°K) | 342 | 342 | 385 |
| Nominal Subcooling (°K) | 40 | 40 | 0 |
| System Pressure (MPa)** | 0.17 | 0.17 | 0.17 |

* Deep pool considered for bottom triggering, shallow pool for side triggering
** Full depressurization of RPV to containment pressure is assumed

Table 19.2-3 Peak Impulse and Pressure from Westinghouse's Assessment of AP600 Ex-Vessel Steam Explosions

| Calculation Case | Impulse (kPa-s)* | Pressure (MPa)* |
|---|---|---|
| Base Case (Hinged Failure) | 490<br>(66) | 170<br>(30) |
| Base Case (Localized Failure) | 2.1<br>(negligible) | 0.6<br>(0.16) |
| Sensitivity 1 (Melt Superheat) | 2.2<br>(negligible) | N/A |
| Sensitivity 2 (Nominal Pool Area) | 1.5<br>(negligible) | N/A |
| Sensitivity 3 (Breakup Model) | 2.1<br>(negligible) | N/A |
| Sensitivity 4 (Water Temperature) | 2.6<br>(negligible) | N/A |

* Numbers in parentheses refer to cavity wall loading; numbers without to floor loading

Table 19.2-4 Maximum Pressure from Staff's Assessment of AP600 Ex-Vessel Steam Explosions

| Description of Calculation | Maximum Calculated Pressure (MPa) | | | | | |
|---|---|---|---|---|---|---|
| | ESPROSE.m | | | TEXAS | | |
| | Pool | Floor | RPV | Pool | Floor | RPV |
| Scenario I (Unsubmerged RPV) | | | | | | |
| Base Case, Saturated Water Pool | 163 | 78 (80)* | N/A | N/A | N/A | N/A |
| Subcooled Water Pool | 390 | 225 (165) | N/A | N/A | N/A | N/A |
| Scenario II (Partially Submerged RPV) | | | | | | |
| Base Case, Saturated Water Pool | 375 | 150 (150) | 115 | 60 | 60 (205) | 30 |
| Melt Superheat | 375 | 150 (150) | 125 | 75 | 75 (215) | 30 |
| Subcooled Water Pool | 473 | 350 (294) | 235 | 90 | 90 (335) | 65 |
| Metallic Melt | 102 | N/A | N/A | 40 | 40 (153) | 20 |
| Hole Diameter of 0.2 m | 201 | 90 (68) | 60 | N/A | N/A | N/A |
| Hole Diameter of 0.8 m | 650** | 450 (383) | 300 | 140 | 140 (644) | 130 |
| Impact of RPV Lower Head | 350 | 190 (190) | 120 | N/A | N/A | N/A |
| Fragmentation Constant Increase to 0.0125 | N/A | N/A | N/A | 125 | 125 (457) | 90 |
| Scenario III (Fully Submerged RPV) | | | | | | |
| Base Case, Subcooled Water Pool | 520 | 370 (300) | 300 | N/A | N/A | N/A |
| Saturated Water Pool; RPV Modeled | 350 | 150 (288) | 120 (320) | N/A | N/A | N/A |
| Subcooled Water Pool; RPV Modeled | 800 | 430 (625) | 330 (670) | N/A | N/A | N/A |

* Numbers in parentheses refer to corresponding impulse loading in kPa-s

** Calculation encountered numerical difficulties and was terminated after 3 ms

Table 19.2-5 Meridional and Hoop Stresses at the Knuckle Region

| Pressure | Meridional Stress | Hoop Stress |
|---|---|---|
| 411.6 kPa ( 45 psig) | 75.8 MPa (11.00 ksi) | -75.8 MPa (-11.00 ksi) |
| 1,066.6 kPa (140 psig) | 236.4 MPa (34.29 ksi) | -171.3 MPa (-24.85 ksi) |
| 1,135.6 kPa (150 psig) | 253.6 MPa (36.79 ksi) | -180.5 MPa (-26.18 ksi) |
| 1,294.1 kPa (173 psig) | 291.0 MPa (42.21 ksi) | -182.6 MPa (-26.48 ksi) |

Table 19.4-1 Comparison of Estimated Benefits from Averted Offsite Exposure

| Design Alternative | Estimated Capital Cost, $ | Averted Risk, person-rem per year | Westinghouse Benefits*, $ | Staff Benefits** @ $2000/ person-rem, 1996$ | Staff Benefits** @ $5000/ person-rem, 1996$ |
|---|---|---|---|---|---|
| Upgrade Chemical and Volume Control System for Small LOCA <4" | 1,500,000.00 | 0.00055 | 4 | 17 | 39 |
| Filtered Containment Vent | 5,000,000.00 | 0.001 | 6 | 30 | 70 |
| Self-Actuating Containment Isolation Valves | 33,000.00 | 0.00074 | 5 | 22 | 52 |
| Passive Safety Grade In-Containment Sprays | 3,900,000.00 | 0.0069 | 44 | 207 | 484 |
| Active High Pressure Safety Injection System | 20,000,000.00 | 0.0061 | 39 | 183 | 428 |
| Steam Generator Shell Side Passive Heat Removal | 1,300,000.00 | 0.00053 | 3 | 16 | 37 |
| Direct Steam Generator Safety and Relief Valve Flow to RWST | 620,000.00 | 0.00042 | 3 | 13 | 29 |
| Increased Steam Generator Pressure Capability | 8,200,000.00 | 0.00042 | 3 | 13 | 29 |
| Secondary Containment Ventilation with Filtration | 2,200,000.00 | 0.00074 | 5 | 22 | 52 |
| Diverse IRWST Valves | 570,000.00 | 0.0053 | 34 | 159 | 372 |
| Diverse Containment Recirculation Valves | 150,000.00 | 0.00015 | 1 | 5 | 11 |
| Ex-Vessel Core Catcher | 1,660,000.00 | 0.0061 | 39 | 183 | 428 |
| High Pressure Containment Design | 50,000,000.00 | 0.0061 | 39 | 183 | 428 |
| Increase Reliability of Diverse Actuation System (DAS) | 470,000.00 | 0.00022 | 2 | 7 | 15 |
| 100% Effective Design Alternative: | | 0.00734 | 47 | 221 | 551 |

*Benefits account only for offsite effects, 15.7% effective discount rate, 30 yr plant life,$1,000/person-rem

**Benefits account only for offsite effects, 7% effective discount rate, 60 yr plant life

Table 19.4-2 Key Differences between Westinghouse and NUREG/BR-0058

| Westinghouse Design Alternative Evaluation Approach | NUREG/BR-0058 Recommended Approach |
|---|---|
| $1,000 per person-rem averted for valuing risk reduction | $2,000 per person-rem averted to account for health effects, plus $3,000 per person-rem averted to account for other offsite effects and other related costs |
| 15.7% discount rate | 7% discount rate |
| No accounting for benefits of averted on-site cleanup and decontamination costs | Consideration given for benefits of averted on-site cleanup and decontamination costs |
| No accounting for benefits of averted replacement energy costs | Consideration given for benefits of averted replacement energy costs |

Table 19.4-3 Key Parameters Used in Evaluating Maximum SAMDA Benefits

| Parameter | Value |
|---|---|
| Reference AP600 Core Damage Frequency (CDF) | 1.7E-7/r-yr (error factor: EF=5.7) |
| Average public radiation exposure per accident: | 43,200 person-rem (rounded to 50,000) (assumed error factor: 5) |
| Plant lifetime: | 60 years |
| Discount rate: | 7% |
| Conversion factor*, $/person-rem | $5000/person-rem |
| Replacement energy costs: | $277,000/day of downtime |
| Averted cleanup and decontamination costs** | $1.69E9/major accident |
| Averted replacement energy costs***: | $20.2E9/major accident |

*Based on NUREG/CR-6349, accounts for both offsite health effects and offsite property damage effects
**Based on guidance provided in NUREG/BR-0184 (not adjusted for AP600 specific features)
***Based on average replacement energy costs for PWRs in the 500 - 1000 MWe range

Table 19.4-4 Design Alternative Benefits Accounting for Uncertainties and External Events Effects (Benefits, 1996$)

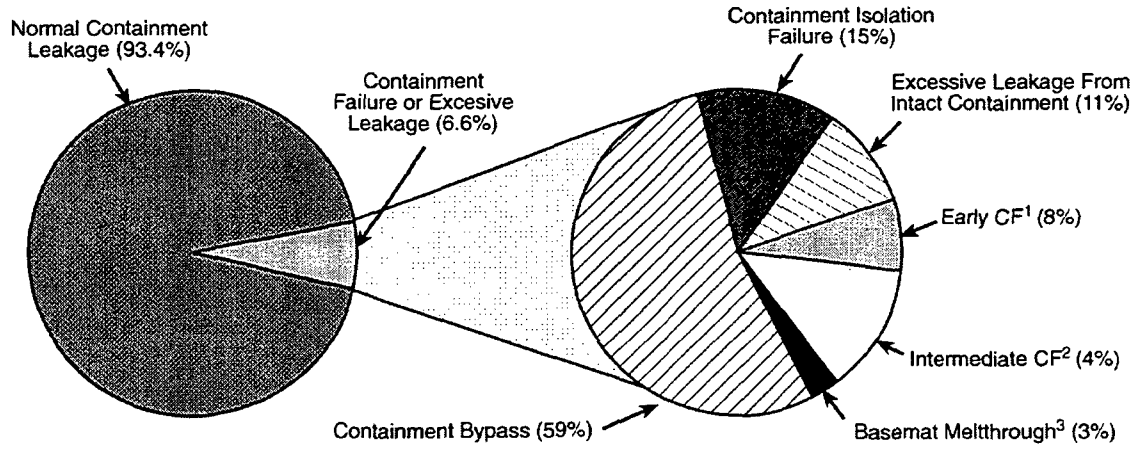
| Case No. | Description | 5% Confidence Level | Mean | 95% Confidence Level |
|---|---|---|---|---|
| 1 | Base CDF (1.7E-07/yr) and reference offsite release (50,000 person-rem); design alternatives which reduce the accident frequency to zero | 1100 | 8000 | 26600 |
| 2 | Base CDF increased by factor of 100 to account for external events and other accident sequences not yet accounted for, other factors same as Case 1; design alternatives which reduce the accident frequency to zero | 90500 | 647000 | 2257000 |
| 3 | Base CDF increased by factor of 100 to account for external events, other factors same as Case 1; design alternatives which reduce the offsite releases to zero but do not change the accident frequency | 1700 | 49000 | 223000 |

## Table 19.4-5 Estimated Maximum Benefit from Individual Design Alternatives

| Design Alternative | Fractional Risk | Capital Cost | Mean Benefit from Reduced Risk[1] | Mean Benefit form Averted Onsite Costs[2] | Adjusted Capital Costs Reduced by Mean Averted Onsite Costs[3] | $/person-rem based on Mean Benefits[4] |
|---|---|---|---|---|---|---|
| Design Alternatives that Reduce Core Damage Frequency | | | | | | |
| Upgrade Chemical and Volume Control System for Small LOCA <4" | 0.075 | $1,500,000 | $3,675 | $44,850 | $1,455,150 | $1,979,796 |
| Active High Pressure Safety Injection System | 0.83 | $20,000,000 | $40,670 | $496,340 | $19,503,660 | $2,397,794 |
| Steam Generator Shell Side Passive Heat Removal | 0.07 | $1,300,000 | $3,430 | $41,860 | $1,258,140 | $1,834,023 |
| Diverse IRWST Valves | 0.72 | $570,000 | $35,280 | $430,560 | $139,440 | $19,762 |
| Increase Reliability of Diverse Actuation System (DAS) | 0.03 | $470,000 | $1,470 | $17,940 | $452,060 | $1,537,619 |
| Diverse Containment Recirculation Valves | 0.02 | $150,000 | $980 | $11,960 | $138,040 | $704,286 |
| Design Alternatives that Reduce Offsite Releases but do not Impact Core Damage Frequency | | | | | | |
| Direct Steam Generator Safety and Relief Valve Flow to IRWST | 0.057 | $620,000 | $2,793 | | $620,000 | $1,109,918 |
| Increased Steam Generator Pressure | 0.057 | $8,200,000 | $2,793 | | $8,200,000 | $14,679,500 |
| Filtered Containment Vent | 0.136 | $5,000,000 | $6,664 | | $5,000,000 | $3,751,501 |
| Passive Safety Grade In-Containment Sprays | 0.94 | $3,900,000 | $46,060 | | $3,900,000 | $ 423,361 |
| Secondary Containment Ventilation with Filtration | 0.1 | $2,200,000 | $4,900 | | $2,200,000 | $2,244,898 |
| Self-Actuating Containment Isolation Valves | 0.1 | $33,000 | $4,900 | | $33,000 | $33,673 |
| Ex-Vessel Core Catcher | 0.83 | $1,660,000 | $40,670 | | $1,660,000 | $204,082 |
| High Pressure Containment Design | 0.83 | $50,000,000 | $40,670 | | $50,000,000 | $6,147,037 |

1- Benefit because of reduced offsite exposures. For design alternatives that reduce CDF, this value also includes any benefits from reduced occupational exposures from averted onsite cleanup and decontamination efforts.
2- Benefits from averted onsite costs, i.e., averted cleanup and decontamination costs and averted replacement energy costs.
3- The benefits from averted onsite costs are used to effectively reduce the capital cost of each design alternative.
4- The cost/benefit ratio for each design alternative evaluated for the AP600 based on "mean" estimates of benefits. Each person-rem of averted public exposure was assigned a value of $5,000.

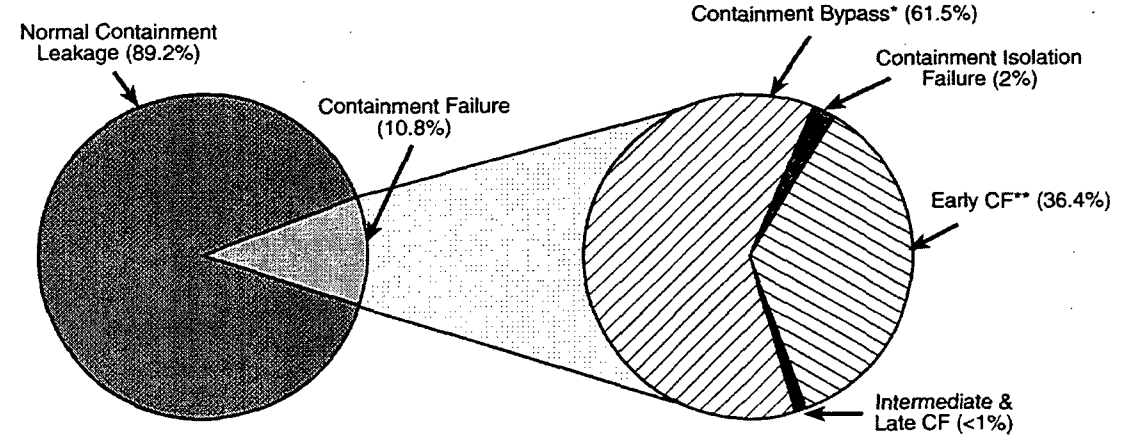
**ORIGINAL PRA RESULTS**




**Total Core Damage Frequency = 3.3 E-7/y** **Total Release Frequency = 2.2 E-8/y**

Footnotes:
1 Containment failure (CF) during core relocation phase
2 Containment failure prior to 24 h after the onset of core damage
3 Basemat meltthrough after 72 h

**UPDATED PRA RESULTS**




**Total Core Damage Frequency = 1.7 E-7/y** **Total Release Frequency = 1.8 E-8/y**

* Includes all events in which core damage occurs at high RCS pressure and late depressurization is unsuccessful.

** Includes all events that result in reactor pressure vessel meltthrough, including events assigned to basemat meltthrough in original PRA.

Figure 19.1-1
Comparison of AP600 Containment Release Frequency based on the Original and Updated Level 2 PRA Results Reported by Westinghouse (Baseline PRA, Internal Events)

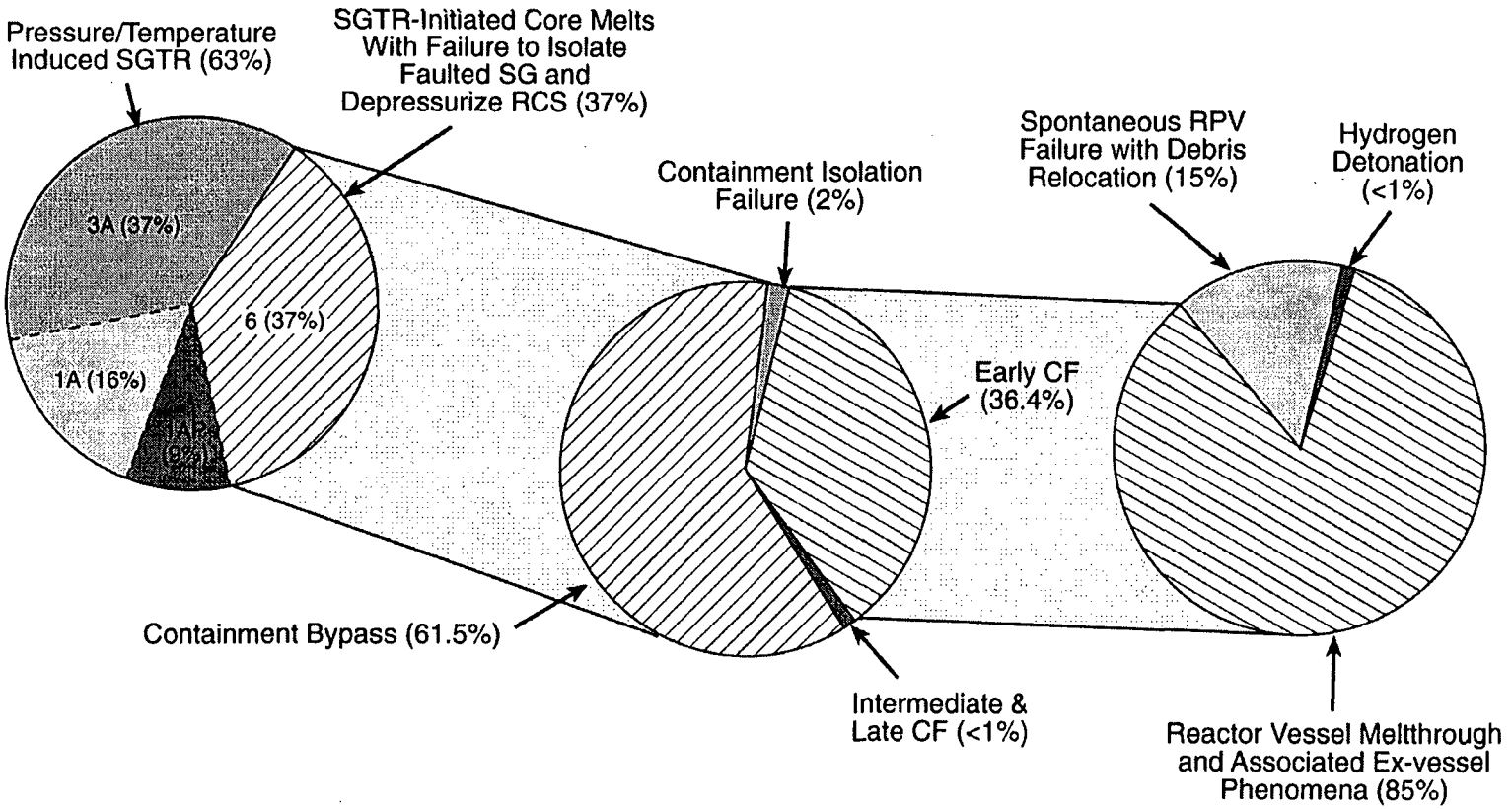



Figure 19.1-2 Breakdown of AP600 Containment Release Modes by Contributor, as Reported by Westinghouse

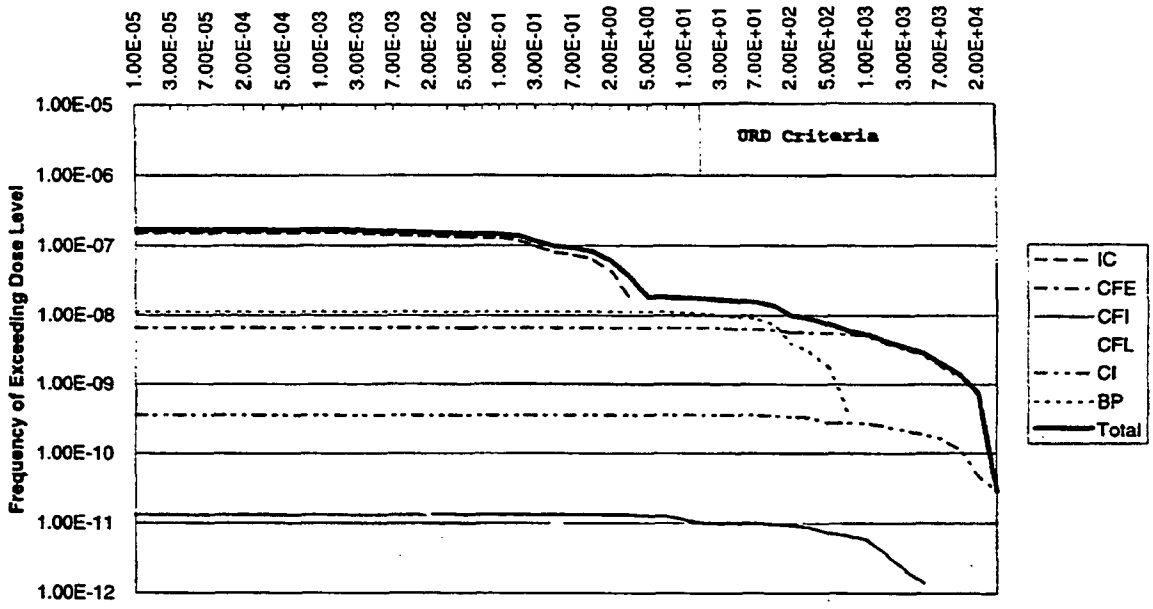



Figure 19.1-3
Overall Dose Risk,
Site Boundary Whole Body EDE, 24 Hour Dose

## Appendix 19A: Seismic Margin Assessment

### 19A.1 Introduction

In Chapter 55 of the AP600 PRA, Revision 10, dated June 10, 1997, Westinghouse discussed the seismic margin analysis (SMA). In this section, the staff evaluates the adequacy of Westinghouse seismic margin using an estimate of high confidence in low probability of a failure (HCLPF) methodology.

In the SRM dated July 21, 1993, the Commission approved the following staff recommendation specified in Section II.N, "Site-Specific Probabilistic Risk Assessments and Analysis of External Events" of SECY-93-087 with modification:

> PRA insights will be used to support a margins-type assessment of seismic events. A PRA-based seismic margins analysis will consider sequence-level High Confidence, Low Probability of Failures (HCLPFs) and fragilities for all sequences leading to core damage or containment failures up to approximately one and two-thirds the ground motion acceleration of the Design Basis SSE.

The staff evaluated the margins-type assessment of seismic events as contained in AP600 design certificate documents, including Revision 10 of the AP600 PRA, Westinghouse's RAI responses and other submittals, which include the materials presented and discussed during NRC/Westinghouse meetings and teleconference calls. The details of the staff's evaluation are provided as follows.

### 19A.2 Evaluation

Westinghouse based the AP600 SMA on established criteria, design specifications, existing qualifications test reports, established designs, and public domain generic data.

A review level earthquake (RLE) equal to 0.5g has been established for the SMA, and used to demonstrate margin over the SSE of 0.3g. This RLE is consistent with the SRM dated July 21, 1993.

The conclusion in Section H.1 of the PRA Appendix H (Revision 1), dated July 22, 1994, regarding reserve margin in the soil for liquefaction potential, was not evident from the information provided. The potential for soil liquefaction should be evaluated at the site specific conditions. Westinghouse was requested to explain how this will be done. Westinghouse responded that since the evaluation is performed for a generic site, both rock and soil foundation conditions are considered. There will be no necessity to perform a new site-specific risk-based seismic analysis by a COL applicant as long as the site-specific parameters are enveloped by those defined in Section 2.5 of the SSAR.

If characteristics are outside the range discussed in the Section 2.5 of the SSAR, then a site-specific risk-based seismic analysis may be necessary. Further, it will be necessary for the COL applicant to evaluate the potential for soil liquefaction using site-specific conditions. With the COL commitment, the soil liquefaction is considered closed.

For the HCLPF values of the equipment and structures, Westinghouse used one of the following:

- Probabilistic fragility analysis
- Conservative deterministic failure margin method
- Test results
- Deterministic approach
- Generic fragility data

19A.2.1 Probabilistic Fragility Analysis (FA)

In many seismic PRAs, the fragility of a component is represented by a double lognormal model using three parameters as follows: (1) $A_m$ for median ground acceleration capacity, (2) logarithmic standard deviation (LSD) $ß_r$ for randomness in the capacity, and (3) LSD $ß_u$ for uncertainty in the median value. Using the double lognormal model, the fragility curves are developed. The design capacity, $ß_r$, and $ß_u$, are estimated using design analysis information, test data, earthquake experience data, and engineering judgment. In estimating the median ground acceleration capacity and the associated variability, an intermediate variable defined as margin factor F is used. The margin factor is related to the median ground acceleration capacity by the equation of $A_m = FA_d$, where $A_d$ is the ground acceleration of the reference design earthquake (i.e., the SSE peak ground acceleration [pga] for the plant) to which the structure or component is designed. The composite LSD for the associated variability ($ß_c$) is defined by $(ß_r^2+ß_u^2)^{½}$.

A key step in the seismic fragility estimate involves the evaluation of the margin factor associated with the design for each important potential failure mode. The design margins inherent in the component capacity and the dynamic response to the specific acceleration are two basic considerations. Each of the capacity and response margins involves several variables, and each variable has a median margin factor and variability associated with it. The overall margin factor F is the product of the margin factor for each variable $F_i$. The overall composite LSD is the square root of sum of squares (SRSS) of the composite LSDs in the individual margin factors.

The HCLPF capacity is calculated using this fragility model as:

$$\text{HCLPF capacity} = A_m \exp(-1.65\,[ß_r + ß_u]) = A_m \exp(-2.326\,ß_c)$$

The following are general parameters that should be considered in the probabilistic FA methodology (from EPRI report TR-103959, "Methodology for Developing Seismic Fragilities," dated June 1994):

| Response | Capacity |
|---|---|
| Ground Motion | Strength |
| Damping | Inelastic Energy Absorption |
| Modeling | |
| Mode Combination | |
| Time History Simulation | |

Response
Soil-Structure Interaction
Earthquake Component Combination

Westinghouse stated that the following seismic Category I structures are subjected to design-basis accident (DBA) loads in response to RAI 230.106:

Containment Vessel
Containment Internal Structure and IRWST Tank Modules
Steam Generator Supports
Pressurizer Supports
Reactor Pressure Vessel Supports

Only the HCLPF values for the primary component supports (steam generator [SG], pressurizer, and reactor pressure vessel [RPV] supports) are affected by the DBA loads. For the containment vessel and critical containment modules, the DBA loads would increase the HCLPF value, if included. That is because the DBA loads would cause tension in the containment vessel which is controlled by the compressive buckling stress, and the DBA pressure acts opposite to the hydro-pressure stress associated with the tank module walls which control the containment structure HCLPF value.

19A.2.1.1 Response

19A.2.1.1.1 Ground Motion

The use of the NUREG/CR-0098 median shape response spectrum for the RLE of 0.5g supported in Revision 1 to Section H.1 of PRA Appendix H on the basis of NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities" was questioned. In NUREG-1407, the NRC guidance is intended for use in IPEEE of currently operating nuclear power plants and is not intended for use in the seismic margins evaluation for advanced standard passive reactor designs such as the AP600. The NRC staff does not believe that it is appropriate to use the median shape spectrum from NUREG/CR-0098 nor the NUREG-1407 for the advanced passive design of AP600. Westinghouse responded that the AP600 latest design response spectra anchored to 0.5g pga specified in the Section 3.7.1 of the SSAR was used in this SMA. The design response spectra anchored to 0.5g pga is based on the design response spectra anchored to 0.3g pga multiplied by 1.67 in accordance with SECY-93-087. The staff found the design response spectra anchored to 0.3g pga acceptable as discussed in Section 3.7.1 of this report, and finds that Westinghouse modified the design response spectra anchored to 0.5g pga correctly. Therefore the design response spectra anchored to 0.5g pga is an acceptable response spectrum shape.

19A.2.1.1.2 Damping

Westinghouse used the SSE damping values in HCLPF calculation. The margin factor and variability associated with damping are determined considering the 7 percent damping value as median-centered, with the design damping values representing the 84 percentile damping values. The margin factor is defined by $Sa_d/Sa_m$ and the composite LSD $\ln(Sa_d/Sa_m)$, where $Sa_d$ is spectral acceleration value associated with the design damping value and $Sa_m$ spectral

acceleration value associated with the median-centered damping value. This method is consistent with EPRI report TR-103959 (page 3-12), thus acceptable.

19A.2.1.1.3 Modeling

Modal Frequency Variability

The composite LSD is defined as the ratio of the spectral acceleration value associated with one-sigma variation in frequency to the spectral acceleration value at the median-centered frequency ($\ln[S_\beta/S_f]$), where $S_\beta$ is spectral acceleration value at 84 percent exceedance probability frequency estimate, $f_\beta$ and $S_f$ is spectral acceleration value at median-centered frequency. The $f_\beta$ is estimated as f exp(±0.3), representing the composite LSD, $\beta_c$, of 0.3 which is consistent with the American Society of Civil Engineers (ASCE) report, ISBN 0-87262-547-8, "Uncertainty and Conservatism in the Seismic Analysis and Design of Nuclear Facilities," dated 1986, (page 145). Therefore, it is acceptable.

Mode Shape

Westinghouse used the composite LSDs of 0.15 and 0.10 for multi-degree of freedom system model and a system that responds predominantly in one mode, respectively. These values are consistent with the ASCE report ISBN 0-87262-547-8, (page 144). EPRI report TR-103959 (page 3-18) recommended 0.15 and 0.05 for complex structure and simple structure whose response is dominated by a fundamental mode with a simple mode shape. Therefore, it is acceptable.

Imperfection

The composite LSD is defined as 0.64 for the critical buckling load. It is consistent with NUREG/CR-3127, "Probabilistic Seismic Resistance of Steel Containment," dated January 1984 (page 9), thus acceptable.

19A.2.1.1.4 Mode Combination

Westinghouse stated that fragility parameters associated with mode combination are not included in the FA methodology because they do not effect the HCLPF values calculated using the probabilistic FA method. Westinghouse provided the following reasons in response to RAI 230.107 in which the staff requested justification for not using the mode combination.

For primary components supports:

- SG supports and RPV supports

  The seismic response for these structures is from time history (TH) analyses and not from response spectra. Therefore, mode combination fragility parameters are not appropriate.

- Pressurizer supports

  The pressurizer response is predominantly resulting from modes around 23 Hz, and modes above 33 Hz which are in the rigid region. Therefore, the response is not multi-mode in character and thus mode combination fragility parameters are not appropriate.

- Containment vessel:

  The seismic response that contributes to the critical "failure mode" which is buckling is predominantly single mode and not multi-mode. Therefore, mode combination fragility parameters are not appropriate. The containment vessel is a cylindrical structure so that the earthquake response from each of the seismic components are uncoupled and any effect from variations because of combination of earthquake components are negligible.

- Containment internal structure and IRWST tank modules:

  The seismic response is not made up of multiple modes as a multi-mass system, and therefore, variation in seismic response because of mode combination is not applicable.

However, EPRI report TR-103595 (page 3-19) states that the combination of response modes is random because of random phasing of the individual modal responses. This is true whether a response spectrum or a TH analysis is performed. A TH analysis, conducted using a different earthquake record but with the same ground motion parameter value (e.g., pga), will result in different phasing between the Fourier components and hence a different peak response. It recommends that a $\beta_r$ of 0.15 for structures with multiple important modes and 0.05 for simple structures, such as a containment building that responds primarily in a single mode. Westinghouse should revise the Chapter 55 of the AP600 PRA to include this mode combination randomness for the probabilistic FA method.

In its response dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis and the corresponding HCLPF values satisfy the requirement of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to Chapter 55 of the AP600 PRA. The staff concludes that it is unnecessary to revise Chapter 55 because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in the AP600 PRA Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA, therefore, this item is considered closed. As previously discussed this is COL Action Item 19.1.5-2.

19A.2.1.1.5 Time History (TH) Simulation

In the SSAR, Westinghouse stated that when seismic TH analysis results were used, the margin factor was adjusted so that the seismic response associated with the TH reflected the responses that would be obtained if the envelope spectra associated with the different soil cases were used. This was accomplished by verifying that the TH seismic response, defined by its response spectrum, at the dominant component frequencies, envelope the broadened design floor response spectrum (FRS) associated with the analyzed soil cases.

Adjusting the seismic margin factor so that the response spectrum of the TH, at the dominant component frequencies, envelops the broadened design FRS for all the soil cases, is an acceptable approach.

Westinghouse stated that the response for SG and RPV supports is from TH analyses. EPRI report TR-103959 (page 3-20) recommends that the associated uncertainty ($\beta_u$) of $\frac{1}{2}\ln(Sa_{med}/Sa_{low})$ be used in the vicinity of the fundamental structure frequency if the TH simulation is used. The staff requested the rationale for not using this uncertainty for the probabilistic fragility analysis. Westinghouse responded that in Fig. 3-5 of EPRI report TR-103959, $Sa_{low}$ is below $Sa_{med}$. As seen in Figures 3.7.1-6 to 3.7.1-8 of the SSAR, $Sa_{low}$ is above $Sa_{med}$ (RAI 230.137, R1). Based on the above, the staff agrees with Westinghouse that there is no need to use this uncertainty, therefore, it is acceptable.

19A.2.1.1.6 Soil-Structure Interaction (SSI)

The staff requested Westinghouse perform any sensitivity analyses to evaluate the effect of changes in certain assumptions used in the SMA (e.g., changes in HCLPF values of key components because of different site soil conditions). Westinghouse responded that the HCLPF calculations are made with a spectra that considers different types of soil properties, and no additional sensitivity analyses are needed to reflect different soil conditions (RAI 230.117).

The staff believes that an additional uncertainty, $\beta_u$, should be included in the HCLPF evaluation to account for the response variability because of different site conditions and requested of Westinghouse that the quantification of this additional uncertainty be described in the AP600 PRA. Westinghouse responded that it is noted that an envelope spectra for the different soil conditions is used in the development of the HCLPF values. No credit is taken for the margin at a specific site. Variability is included to account for SSI effects. The variability, $\beta_c$, is estimated to be 0.1 (RAI 230.119). This is consistent with EPRI report TR-103959 (page 3-26), thus acceptable.

19A.2.1.1.7 Earthquake Component Combination

For primary component supports (SG, RPV, and pressurizer), containment vessel, and containment internal structure and IRWST tank modules, Westinghouse stated that the critical component seismic load is dependent primarily on a single earthquake component, and therefore, fragility parameters associated with the combination of earthquake components are not included. However, EPRI report TR-103959 (page 3-27) recommends that a randomness ($\beta_r$) for response be included in the FA since the actual response will be higher or lower and provides an upper bound value of $\beta_r$ (0.18) and a typical value of $\beta_r$ (0.15) for building response because of the effects of earthquake component combination. The staff requested that Westinghouse provide the rationale for not using this randomness for the probabilistic FA. Westinghouse responded by quoting "that an upper bound value of $\beta_r$ equal to 0.18 can always be used but may be excessively conservative for cases where the response is primarily from a single direction" in EPRI report TR-103959 (page 3-27). Westinghouse claimed that since the critical seismic load is dependent primarily on a single earthquake component or the components are uncoupled, any effect from variations in response because of the combination of earthquake components are negligible (RAI 230.137, R1). However, this statement needs to be justified since for the example given, the containment will see compression loads because of

one horizontal earthquake along with shear loads because of the other horizontal earthquake, as well as compressive loads because of the vertical earthquake. The effects from all three components should be considered. For comparison, ASCE report ISBN 0-87262-547-8 (page 159) also shows the variability of a combination of earthquake components ($\beta_c$) as 0.15 in addition to analysis and modeling error. Westinghouse should revise the AP600 PRA Chapter 55 to include this combination of earthquake components for the probabilistic FA method.

In its letter dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis. The corresponding HCLPF values satisfy the provision of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to the AP600 PRA Chapter 55. The staff believes that it is unnecessary to revise the AP600 PRA Chapter 55 because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in the AP600 PRA Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA, therefore, this item is considered closed. This COL action was discussed in Section 19A.2.1.1.4 and 19.1.5 of this report (COL Action Item 19.1.5-2).

Sliding and overturning were considered for the containment vessel. Overturning of the containment vessel controls over sliding.

19A.2.1.2 Capacity

19A.2.1.2.1 Strength

Variable Strength Factors

Westinghouse used different margin factors for the different failure modes:

- For buckling, the margin factor of 1.5 and composite LSD of 0.11 without material variability are used. The margin factor 1.5 was predicated on the basis of the curve in ASME Code Case N-284, Revision 0 that was derived from lower bound tests. Using test data provided by Westinghouse, the staff performed a regression analysis on the basis of methodology provided in NUREG/CR-4604, and found that the median is higher than 1.5 times the lower bound curve. Therefore, the median factor of 1.5 is acceptable. The composite LSD of 0.11 is acceptable on the basis of Greimann, Lowell and Fanous, Fouad, "Reliability of Containments under Overpressure," Pressure Vessel and Piping Technology, A Decade of Progress, 1985, (page 847).

- For shear strength of high-strength bolts, the mean shear strength of $0.625\sigma_{\text{tensile strength}}$ and the composite LSD of 0.05 are used.

- For shear strength of weld, the mean shear strength of $0.84\sigma_{\text{ultimate strength}}$ and the composite LSD of 0.10 are used.

On the basis of the response to RAI 230.133, Revision 1, the failure mode for SG upper support ring girder flange joint bolts is tension failure. This is not presented in the AP600 PRA. The composite LSD is specified as 0.02 on the basis of the following two documents:

- Westinghouse letter from B. A. McIntyre to Brookhaven National Laboratory, "Information for Review of AP600 Large Support Seismic HCLPF Evaluations," dated August 13, 1997.

- Westinghouse letter from B. A. McIntyre to Brookhaven National Laboratory, "Information for Review of AP600 Shielding Building Seismic Margin HCLPF Evaluation," dated October 17, 1997.

EPRI report TR-103959 (page 3-15) specifies the composite LSDs as 0.13, 0.10 and 0.19 for the tension strength of bolt, the shear strength of bolt, and the shear strength of weld, respectively. These values are used for common materials. Therefore, Westinghouse should revise Chapter 55 of the AP600 PRA to increase the composite LSDs for these common materials.

In its letter dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis, and the corresponding HCLPF values satisfy the provisions of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to Chapter 55 of the AP600 PRA. The staff did not require Chapter 55 to be revised because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA, therefore, this item is considered closed. This COL action was discussed in Section 19A.2.1.1.4 and 19.1.5 of this report (COL Action Item 19.1.5-2).

Material

Westinghouse used the statistical estimates of the mean and standard deviation of the material properties (steel and reinforced concrete) available in the public domain. No increase in material properties because of the application of dynamic load was considered in the SMA, which is conservative. Therefore, this is acceptable.

19A.2.1.2.2 Inelastic Energy Absorption, Ductility

The staff asked Westinghouse how the HCLPF values were calculated for concrete-filled steel type IRWST modules. Westinghouse responded that damping and ductility factors were considered in the calculation of the HCLPF values. These modules, described in Section 3.8.3 of the SSAR, are seismically qualified using 5 percent critical damping. An additional increase in damping was considered up to a level 7 percent damping without double counting occurring (RAI 230.134, R1). EPRI report TR-103959 (page 3-13) shows 7 percent is the median and RG 1.61 recommends 7 percent for reinforced concrete at SSE.

These structures are of shear wall type construction. The associated median ductility margin factor of 2.25 and the composite LSD of 0.25 were used. Local inelastic energy absorption was

not considered (RAI 230.126). These values are consistent with ASCE report ISBN 0-87262-547-8 (page 180), and are therefore, acceptable.

19A.2.1.3 Review of Large Supports

For the RPV and SGs, it seems that the variability of the floor responses are not properly accounted for. The calculated $\beta_c$ values of 0.27 and 0.29 in Table 55-1 of Chapter 55 of the AP600 PRA are considered to be too low in comparison with typical values of 0.5 to 0.6 in the past seismic PRA studies. The staff requested the rationale for the nonconservative evaluation of variabilities. If it is intended to use conservative FRS to compensate for this nonconservative assumption (i.e., low $\beta_c$), the staff requested that Westinghouse explain quantitatively that the net results for the HCLPF calculations are still on the conservative side (RAI 230.133, R1).

Westinghouse responded that a nonconservative evaluation of variabilities was not used. Comparisons to typical values from past generic seismic PRA studies can be misleading since they reflect a large population of different types of components having different types of failure modes, and therefore, potentially have large variability. The values used in the AP600 SMA for total variabilities reflecting both randomness and uncertainty components are appropriate for the critical fragility modes of the primary components.

The governing failure modes associated with the RPV and SG are related to bolts within the primary component supports:

- SG upper support ring girder flange joint bolts - tension failure
- RPV support box hold down bolts - shear failure

Inelastic energy absorption or ductility was not considered since the governing failure modes are local without large energy absorption capability. This reserve margin factor associated with ductility generally has a large variability that significantly contributes to the variability $\beta_c$. A review of ABWR fragility data associated with the RPV primary component supports reported in ABWR SSAR (Seismic Capacity Analysis, Amendment 31) was made. It was found that the variability used was not near the 0.5 to 0.6, but much nearer to the 0.27 and 0.29 values used in the AP600 SMA (cf., the variability $\beta_c$ of ABWR RPV pedestal, support, and shroud without ductility are 0.36, 0.33, and 0.36, respectively). The staff believes that Westinghouse considered neither response variabilities from mode combination and earthquake component combination nor capacity variabilities from tension strength of bolt, shear strength of bolt, and shear strength of weld as discussed above. Therefore, the staff informed Westinghouse that Table 55-1 of the AP600 PRA should provide the latest variabilities used for RPV and SGs supports.

In its letter dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis, and the corresponding HCLPF values satisfy the provisions of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to Chapter 55 of the AP600 PRA. The staff did not require Chapter 55 of the AP600 PRA to be revised because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in the AP600 PRA Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA,

therefore, this item is considered closed. This COL action was discussed in Section 19A.2.1.1.4 and 19.1.5 of this report (COL Action Item 19.1.5-2).

19A.2.2 Conservative Deterministic Failure Margin (CDFM) Method

In the general CDFM method, a set of deterministic guidelines (e.g., ground response spectra, damping, material strength, and ductility) has been recommended. The HCLPF capacity of the component is determined using these guidelines. The procedure is similar to that used in the Systematic Evaluation Program (SEP), although the choice of some of the parameter values (e.g., damping) may be more liberal in the CDFM method. The method is appealing because it is very similar to the design procedures followed in the industry, except that some of the parameter values were liberalized.

The details of the CDFM method are given in Chapter 2 of EPRI report NP-6041-SL, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin," Revision 1 dated August 1991. The basic approach is to select the parameter values of different variables (e.g., strength, damping, ductility, load combination, and response analysis methods), taking into account the margins and uncertainties. The object is to obtain a conservative yet somewhat realistic assessment of the capacity.

The HCLPF for the shield building roof was calculated by the CDFM method. A finite analysis was performed of this structure that considered cracking of the concrete and redistribution of the loads. Deterministic margin factors were defined for three items: strength, inelastic energy absorption, and damping.

19A.2.2.1 Strength

This margin factor is defined from the finite element analysis on the basis of the increase in seismic acceleration to failure on the basis of ultimate stress criteria. American Concrete Institute (ACI) ACI-349 provisions were used to define ultimate strength for axial and flexure loads. For shear loads, the concrete and rebar capacities have been evaluated. If the design shear load is greater than the concrete shear strength, the shear modulus has been increased to account for the shear strength in the reinforcements.

19A.2.2.2 Inelastic Energy Absorption

The increased capacity because of inelastic energy absorption is defined using recognized deterministic methods. It is only applied to the column structural elements that act as shear walls in the shield building roof. The formulation defining ductility margin follows the effective frequency/effective damping approach given in NUREG/CR-3805, "Engineering Characterization of Ground Motion - Task 1, Effects of Characteristics of Free-Field Motion on Structural Response," dated May 1984.

In its letter dated January 18, 1998, Westinghouse stated that the inelastic energy absorbing factor, $F_\mu$, is estimated for the column structural elements in the shield building roof, for which the CDFM approach in EPRI report NP-6041-SL, Revision 1, is used. Westinghouse also stated that an additional margin factor is considered to account for a higher damping value because of inelastic responses. However, the formulation for the $F_\mu$ factor in the PRA should be used to

modify the linear responses for which a linear (lower) damping value (e.g., 7 percent for concrete structures) is used. To account for both the $F_\mu$ factor and a higher damping value is considered to be a double counting of the nonlinear response effects and should be avoided.

In its response to RAI 230.134, Revision 1, Westinghouse agreed that double counting of nonlinear response effects should be avoided and modified the HCLPF calculations. The HCLPF value of the shield building is controlled by the failure of the tension ring, and its capacity is estimated to be 0.648g, according to the calculations in the following to documents:

- Westinghouse letter from B. A. McIntyre to Brookhaven National Laboratory, "Information for Review of AP600 Shielding Building Seismic Margin HCLPF Evaluation," dated October 17, 1997.

- Westinghouse letter from B. A. McIntyre to Brookhaven National Laboratory, "Loading Information from ANSALDO Calculation No. 1277-S3C-006, Revision 2, For the AP600 Shielding Building," dated October 30, 1997.

In the calculation, an inelastic energy absorption factor of 1.19 is assumed for the columns only, and a factor of 1.0 is assumed for other components of the shield building. In evaluating the seismic margin of tension ring, the effects of biaxial bending and the torsional moment (along the ring axis) are not considered properly.

EPRI report NP-6041-SL, Revision 1, (page 6-5) suggested that in lieu of computing $F_\mu$, for all but the most brittle failure modes, $F_\mu$ can be conservatively chosen as being equal to 1.25 which is as low as any of the results presented in NUREG/CR-3805 for shear wall structures. Most components have both ductile and non-ductile failure modes. Non-ductile failure modes must be checked. Unless the capacity of the lowest non-ductile failure mode exceeds the yield capacity of the lowest ductile failure mode by at least 125 percent, the component CDFM capacity should be defined by non-ductile failure mode capacity with $F_\mu = 1.0$. The 1.25 factor accounts for the variability in the yield and brittle capacities.

Because of a very low shear span ratio (about 0.2) the shield building columns are considered to fail in a very brittle diagonal failure under in-plane shear loading. The assumed $F_\mu$ of 1.19 is, therefore, considered inadequate for this type of brittle failure mode.

The tension ring is expected to fail predominantly in tension; the failure mode (even if the torsional effects are considered) is not considered to be a brittle rupture under cyclic earthquake loads. Therefore, it is considered adequate to use a $F_\mu$ of greater than 1.0 (but not greater than 1.25) in the HCLPF evaluation of the tension ring. Although this assumption yielded a conservative HCLPF value, nevertheless the calculation package should be revised, and Table 55-1 of the PRA should be updated to reflect the new HCLPF values.

In its letter dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis and the corresponding HCLPF values satisfy the provisions of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to Chapter 55 of the AP600 PRA. The staff did not require Chapter 55 to be revised because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in the AP600 PRA Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA, therefore, this item is

considered closed. This COL action was discussed in Section 19A.2.1.1.4 and 19.1.5 of this report (COL Action Item 19.1.5-2).

19A.2.2.3 Damping

A margin factor associated with damping is defined, recognizing that damping of reinforced concrete can increase from 7 percent to 10 percent when cracking is present. This margin factor is equal to the ratio of the spectral accelerations at 7 percent and 10 percent damping for the dominant building structure frequency.

However, EPRI report NP-6041-SL, Revision 1, (page 2-48) recommended that the higher damping values (e.g., 10 percent for concrete structures) only be used when fixed base linear elastic analyses are performed since these higher values are likely to incorporate some radiation of energy back into the foundation media (rock or soil) and some hysteretic energy dissipation from nonlinear behavior. In a letter dated October 17, 1997, from B. A. McIntyre to Brookhaven National Laboratory, "Information for Review of AP600 Shielding Building Seismic Margin HCLPF Evaluation," Westinghouse shows a margin factor of 1.1 for damping was used. Westinghouse should revise the AP600 PRA Chapter 55 for the damping margin factor of 1.0 to be used.

In its letter dated January 16, 1998, Westinghouse performed an assessment for the SSC HCLPF values using the staff's recommendation as a sensitivity analysis, and the corresponding HCLPF values satisfy the provisions of SECY-93-087 for the RLE of 0.5g. The sensitivity analysis results are provided in the Attachment C to the AP600 PRA Chapter 55. The staff did not require Chapter 55 to be revised because the COL applicant will compare the as-built SSC HCLPF values to those Westinghouse values specified in the AP600 PRA Chapter 55. This COL commitment is described in Section 59.10.6 of the AP600 PRA, therefore, this item is considered closed. This COL action was discussed in Section 19A.2.1.1.4 and 19.1.5 of this report (COL Action Item 19.1.5-2).

19A.2.3 Test Results

The HCLPF calculations for a motor control center (MCC) were reviewed on the basis of a document, SM96-9 Class 1E Equipment. The HCLPF values were determined on the basis of the estimated lower bound of qualification test results. Information regarding critical failure modes (e.g., relay chatter) was not made available during the meeting dated January 9, 1997. Variability values of $\beta_r \approx 0.05$ and $\beta_u \approx 0.10$ were used to establish the relationship between the median and HCLPF values. These variability values are considered to be too low, and it seems that the calculation procedure does not follow the acceptable SMA methodologies (deterministic or probabilistic). Another concern is the calculation of the ratio of test response spectra (TRS) to required response spectra (RRS). This ratio, which was determined only at 4.6 Hz, should be calculated throughout the frequency range of interest. Westinghouse responded by proposing to eliminate all the median and ß values from the fragility table, and HCLPF values will be calculated deterministically for electric equipment.

For electrical equipment for which documented test results are available, the HCLPF value is defined from the comparison of RRS and TRS. The method employed follows a deterministic approach using existing test data for similar types of equipment.

The existing test data were reviewed to determine a lower-bound seismic capacity. Regarding the use of test data, the TRS should be used at about 99 percent exceedance probability level for the capacity according to Appendix Q to EPRI report NP-6041-SL, Revision 1. This results in a lower HCLPF value. Westinghouse was requested to provide the rationale for not using the 99 percent exceedance probability level for test response spectra. Westinghouse followed a deterministic approach that used the lower bounds equipment test response spectra. This results in lower HCLPF values. If individual equipment TRS should be used with 99 percent probability of exceedance, then higher HCLPF values will be obtained. Westinghouse provided the lowest HCLPF values on the basis of several test programs (RAI 230.135).

When the natural frequency of the equipment was not known, it was assumed that the natural frequency coincided with the RRS peak acceleration so that the lowest HCLPF value was calculated. This is usually the case, however, it is expected that Westinghouse will confirm this during the course of calculating the lowest TRS to RRS ratio. Where equipment frequencies are known, and are used for comparing the RRS and TRS, these frequencies will be included in the design specification for the equipment to assure that the dynamic characteristics are the same as those expected. This methodology is considered conservative and thus acceptable provided that the lowest HCLPF value is obtained by comparing the TRS to RRS ratio. The need to verify any assumption such as specific frequencies used to compare TRS and RRS is addressed in Section 19A.3 of this report.

Solid state switching devices and electro-mechanical relays will be used in the AP600 protection and control systems. Solid state switching devices are inherently immune to mechanical switching discontinuities such as contact chatter. Robust electro-mechanical relays are selected for AP600 applications such that inherent mechanical contact chatter is within the required system performance criteria. Therefore, contact chatter has no effect on system operation and was not included in the SMA.

The loss of offsite power event has a very low HCLPF value (0.09g). The control rod generator sets are powered by ac load centers that are de-energized on loss of offsite power sources. When the control rod motor generator sets are de-energized, current to the magnetic jack mechanisms stops and the gripper coils open allowing the rods to drop into the core. Therefore, relay chatter is deemed to be a non-issue for reactor trip.

The PRHR heat exchanger and core makeup tank (CMT) valves automatically fail open upon loss of air because of loss of seismic loss of offsite power. Thus, relay chatter is deemed to be a non-issue also for PRHR and CMT system functions. However, the assumptions related to relay chatter would need to be verified as a COL Action Item (see Section 19A.3 of this report).

19A.2.4 Deterministic Approach

A lower-bound estimate of the HCLPF is obtained for selected structures or equipment based on margin to design limit for the appropriate load combination defined by the fault tree logic. This approach was used for the primary component to verify that their supports would control the HCLPF value. It was also used for a few cases to define the HCLPF when it was apparent that seismic capacity would not control the plant HCLPF value. This approach was used for the polar crane, baffle plate supports, PRHR heat exchanger, CMT, and valves.

19A.2.5 Generic Fragility Data

Generic fragility data were used when insufficient information was available to define the HCLPF value using one of the methods described above. Those cases where this approach was used were:

- reactor internals and core assembly that includes fuel
- control rod drive mechanism (CRDM) and hydraulic drive units
- reactor coolant pump
- accumulator tank
- piping
- cable trays
- valves
- battery racks
- main control room operation and switch stations
- ceramic insulators

All of the components listed above except ceramic insulators, for which recognized industry low-fragility data were available, used the ALWR Utility Requirements Document (URD), Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Revisions 5 & 6, issued December 1993.

The staff concluded that the suggested generic fragility values are intended for a preliminary analysis only. The staff informed Westinghouse that these generic values should not be used for critical components which are important to plant risks. In addition, for components with new design features, it should be confirmed that the new design features do not potentially contribute to lowering fragility values. Such examples may include the fuel rods, for which some differences in design (e.g., different outside diameter and additional gas space below the fuel pellets) are observed compared with the typical four-loop design.

Westinghouse responded that ALWR URD, Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Revisions 5 & 6, provides a summary of generic fragility data for preliminary analysis only, however, they are representative of the anticipated capacity. Westinghouse identified a COL item that requires verification of as-built conditions conforming to the seismic margin evaluation. In Section 59.10.6 of the AP600 PRA, Westinghouse states, "The combined license applicant referencing the AP600 certified design will confirm that the as-built plants conforms to the design used as the bases for the seismic margin evaluation" (RAI 230.136). The verification of as-built conditions is discussed in Section 19A.3 of this report. This is COL Action Item 19A.2.5-1.

The staff requested information on HCLPF margin for rigid components with non-ductile supports. The SSE design load and the RLE for the AP600 are 0.3g and 0.5g, respectively. Therefore, a HCLPF margin of 1.67 is implied for all the safety-related equipment and components. To achieve this HCLPF margin, a median margin factor of at least 4.2 is needed. This is on the basis of assumptions that a relatively low variability of $\beta_c$ of 0.40 is used for a fragility estimate and the seismic design is performed up to the limits of the code design allowables.

For relatively flexible/ductile components, such as piping, the design criteria in the PRA is considered to give a sufficient margin to achieve the above median factor of 4.2. However, for dynamically rigid components whose support structures are considered to have a non-ductile failure mode, such as elastic buckling and shear failure in fillet welds or anchor bolt joints, the design requirements in the SSAR may not be sufficient to provide this safety margin. According to the staff's estimate, an additional median margin factor of 2.1 to 3.0 is necessary to achieve the aforementioned HCLPF margin of 1.67 for relatively rigid components with non-ductile support structures.

Westinghouse responded that the components in the AP600 design generally have margin factors in excess of the range of 2.1 to 3.0. The calculated margins of several specific examples were included in the response to RAI 230.139, Revision 1.

For the hypothetical case where the component has rigid response characteristics with non-ductile support structures, Westinghouse stated that generic fragility data that is in the public domain, and is also used in ALWR URD, Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Revisions 5 & 6, does not reflect components having low HCLPF values. Therefore, this hypothetical case would be very plant specific. The AP600 component support designs do not deviate from those seen in other plants and reflected in the generic fragility data, and, therefore, have HCLPF values below seismic margin requirements. If this hypothetical case did exist, it would be a plant specific case, and it would probably not provide the seismic margin commitments of AP600, unless the as-built plant is verified to conform to the seismic margin of 0.5g. In Section 59.10.6 of the PRA, Westinghouse states, "The combined license applicant referencing the AP600 certified design will confirm that the as-built plants conform to the design used as the bases for the seismic margin evaluation." Therefore, this case will be identified and addressed by the COL applicant (RAI 230.139, R1). This COL action item was discussed above (COL Action Item 19A.2.5-1).

However, it is not clear how an as-built verification program will identify such deficiencies in median margin factors for other supports which may be designed up to the code allowable values. In its letter dated January 9, 1998, Westinghouse committed to revise the COL action item reported in Section 59.10.6 of the AP600 PRA. The COL applicant referencing the AP600 certified design is required to perform a seismic walkdown to confirm that as-built plant conforms to the design used as the basis for the seismic margin evaluation and to assure that seismic spatial systems interactions do not exist. The COL applicant will develop details of the seismic walkdown. This is COL Action Item 19A.2.5-1.

Also, the COL applicant referencing the AP600 certified design is required to compare the as-built SSC HCLPF values to those assumed in the AP600 seismic margin evaluation. The COL applicant, to determine if unacceptable vulnerabilities have been introduced, shall evaluate deviations from the HCLPF values or assumptions in the seismic margin evaluation. This is the acceptable COL commitment, therefore, this item is considered closed. This is part of COL Action Item 19.1.5-2.

19A.3 Verification of Equipment Fragility Data

Because walkdowns can not be performed at this time, the staff requested that Westinghouse show how the key assumptions for SSCs considered in the SMA can be verified for the as-built and as-operated plant conditions. Examples of this include proper anchorage of equipment and

seismic fragility of electrical/electronic equipment which may be different in the future. Westinghouse responded that a verification that the as-built plant that confirms the basis of the seismic margin evaluation will be performed by the COL applicant (RAI 230.115). This was discussed above (COL Action Item 19.1.5-2).

Westinghouse states in Section 55.2.2.5 of AP600 PRA that the seismic margin evaluation focused on demonstrating that the design of nuclear island structures, safety-related equipment, and equipment supports can carry the loads induced by the RLE. This evaluation incorporates as-specified equipment data. After the plant has been built, it will be necessary to perform a verification of the seismic margin assessment for the installed conditions. The AP600 PRA Section 59.10.6, Revision 9 provides the COL information for the AP600 PRA, including the SMA. The COL action item for seismic margin, as stated in the PRA, is the COL applicant referencing the AP600 certified design will confirm that the as-built plant conforms to the design used as the basis for the seismic margin evaluation. It is the responsibility of the COL applicant to define how this confirmation is performed (RAI 230.112).

The staff agrees that there needs to be a verification program to confirm the data and assumptions made in the SMA for all items. The description of how this will be accomplished is lacking and should be defined. The process of identifying what data and assumptions need to be verified, how and where they will be documented, and how the verification process will be conducted by the COL applicant should be included in the AP600 PRA. For example, where generic fragility data from ALWR URD, Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Revisions 5 & 6 was used, will the COL applicant perform a new SMA to confirm the assumed HCLPF values?

In its letter dated January 9, 1998, Westinghouse committed to revise the COL action item reported in Section 59.10.6 of the AP600 PRA. The COL applicant referencing the AP600 certified design is required to perform a seismic walkdown to confirm that as-built plant conforms to the design used as the basis for the seismic margin evaluation and to assure that seismic spatial systems interactions do not exist. The COL applicant will develop details of the seismic walkdown. This COL action was discussed in Section 19A.2.5 of this report (COL Action Item 19A.2.5-1).

Also, the COL applicant referencing the AP600 certified design is required to compare the as-built SSC HCLPF values to those assumed in the AP600 seismic margin evaluation. The COL applicant, to determine if unacceptable vulnerabilities have been introduced, shall evaluate deviations from the HCLPF values or assumptions in the seismic margin evaluation. This is an acceptable COL commitment, therefore, this item is considered closed. This COL action was discussed in Section 19A.2.5 of this report (COL Action Item 19.1.5-2).

19A.4 Spatial Interaction

The staff requested that Westinghouse include spatial interactions (e.g., seismic impact between adjacent components and Seismic II/I interactions) in the SMA. Westinghouse responded that the interaction between the turbine building and the north end of the auxiliary building is explicitly discussed in PRA Section 55.5.8 (RAI 230.114).

As part of SMA, the seismic interaction between the turbine building and the nuclear island was evaluated. The following items were determined:

- The adjacent auxiliary building structural integrity will not be lost with the failure of the turbine building.

- It is not likely that the size and energy of debris from the turbine building will be large enough to result in penetration through the auxiliary building roof structure.

Even though it is not likely that the turbine building debris could be large enough or have sufficient energy for penetration through the auxiliary building roof structure, this event was evaluated. The consequences of damage to the safety-related equipment in the auxiliary building was investigated. It was determined from this investigation that, should an event occur that causes the failure of equipment in the upper elevations of the auxiliary building, the results of the SMA analysis, the plant HCLPF value, and the insights derived from the SMA would not be affected. Moreover, according to the AP600 focused-PRA results, steamline break events that would result from damage to equipment in upper elevations are not dominant contributors to the core damage frequency. Further, any loss of equipment in the upper elevations would not affect the passive safety systems used to put the plant in a safe-shutdown condition should an event occur.

The information presented in Sections 55.5.8 and 55.2.2.6 of the AP600 PRA addresses the concern of seismic interaction between the turbine building and the auxiliary building. In the AP600 PRA Section 55.3.3, the annex building, diesel generator building, and radwaste building are assumed to have failed for the SMA. No credit is taken for systems in those buildings. The interaction between the other building and the nuclear island is assumed to have no detrimental effect on the nuclear island structures. However, the AP600 PRA does not address how the failure of the annex building and/or the radwaste building affects the safety-related structures and components of the nuclear island. Given this approach by Westinghouse, a COL action would be required to address the concern of interaction effects including potential impact from deflection of adjacent components or collapse of non-seismic Category I structures and components.

Westinghouse responded that the annex building is a seismic Category II structure which assures a similar margin as those associated with seismic Category I structures (i.e., HCLPF values $\geq$ 0.5g). The staff review of the interaction between the annex building and the nuclear island structures is discussed in Section 3.7.2.8 of this report. The staff agrees with Westinghouse that this building need not be considered further with respect to spatial interaction.

Westinghouse evaluated the radwaste building failure on the nuclear island structures. The staff reviewed this evaluation and found it acceptable as discussed in Section 3.7.2.8 of this report. Therefore, there is no further need to consider spatial interaction associated with this building (see RAI 220.116F). As discussed in Section 19A.2.5 of this report, the COL applicant will develop details of the seismic walkdown (see COL Action Item 19A.2.5-1).

## 19A.5 Conclusion

SECY-93-087 provides that each plant designer perform a PRA-based margins analysis to identify the vulnerabilities of their design to seismic events larger than the design basis SSE. In the SRM dated July 21, 1993, the Commission approved the HCLPF values at least one and two-thirds of the ground motion acceleration of the design basis SSE for the important SSCs required for safe shutdown. For the AP600 standard design this ground motion should be at least at a level that causes peak ground acceleration value of 0.5 g.

In order to satisfy this requirement, Westinghouse performed a PRA-based SMA to assess the seismic robustness of the AP600 design and to provide an acceptable estimate of the maximum earthquake ground motion which the AP600 plant is expected to be able to survive without core damage.

On the basis of the review of the methodology discussed in Chapter 55 of the AP600 PRA, audit of sample calculations of SMA and the closure of the open items discussed above, the staff concludes that the AP600 SMA is founded on an acceptable methodology and that the HCLPF values for the important SSCs are equal to or greater than the minimum required peak ground acceleration of 0.5g. The limiting plant HCLPF value is determined by the seismically induced failure of the fuel in the reactor vessel. Thus the AP600 standard design regarding the SMA methodology meets the criteria indicated in SECY-93-087 and the corresponding SRM, therefore it is acceptable.