AP600 DOCUMENT COVER SHEET

TDC: _____ IDS: I _____ S _____

Form 58202G(5/94) [t:\xxxx.wpf:1x] AP600 CENTRAL FILE USE ONLY:

0058.FRM RFS#: RFS ITEM #:

AP600 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
GWGL022	6	Page 1 of 1	

ALTERNATE DOCUMENT NUMBER: WORK BREAKDOWN #: 3.1.2

DESIGN AGENT ORGANIZATION: Westinghouse

TITLE: AP600 Probabilistic Risk Assessment

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION

☐ WESTINGHOUSE PROPRIETARY CLASS 2
This document contains information proprietary to Westinghouse Electric Corporation; it is submitted in confidence and is to be used solely for the purpose for which it is furnished and returned upon request. This document and such information is not to be reproduced, transmitted, disclosed or used otherwise in whole or in part without prior written authorization of Westinghouse Electric Corporation, Energy Systems Business Unit, subject to the legends contained hereof.

☐ WESTINGHOUSE PROPRIETARY CLASS 2C
This document is the property of and contains Proprietary Information owned by Westinghouse Electric Corporation and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

COMPLETE 1 IF WORK PERFORMED UNDER DESIGN CERTIFICATION OR COMPLETE 2 IF WORK PERFORMED UNDER FOAKE.

1 ☒ **DOE DESIGN CERTIFICATION PROGRAM** – GOVERNMENT LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-AC03-90SF18495.

☐ DOE CONTRACT DELIVERABLES (DELIVERED DATA)
Subject to specified exceptions, disclosure of this data is restricted until September 30, 1995 or Design Certification under DOE contract DE-AC03-90SF18495, whichever is later.

EPRI CONFIDENTIAL: NOTICE: 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ CATEGORY: A ☒ B ☐ C ☐ D ☐ E ☐ F ☐

2 ☐ **ARC FOAKE PROGRAM** – ARC LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-FC02-NE34267 and subcontract ARC-93-3-SC-001.

☐ ARC CONTRACT DELIVERABLES (CONTRACT DATA)
Subject to specified exceptions, disclosure of this data is restricted under ARC Subcontract ARC-93-3-SC-001.

ORIGINATOR	SIGNATURE/DATE	
C. L. Haag	C Haag 11-16-95	
AP600 RESPONSIBLE MANAGER	SIGNATURE*	APPROVAL DATE
B. A. McIntyre		11/16/95

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

Form 58202G(5/94)

LIMITED RIGHTS STATEMENTS

DOE GOVERNMENT LIMITED RIGHTS STATEMENT

(A) These data are submitted with limited rights under government contract No. DE-AC03-90SF18495. These data may be reproduced and used by the government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacturer nor disclosed outside the government; except that the government may disclose these data outside the government for the following purposes, if any, provided that the government makes such disclosure subject to prohibition against further use and disclosure:
   (I) This "Proprietary Data" may be disclosed for evaluation purposes under the restrictions above.
   (II) The "Proprietary Data" may be disclosed to the Electric Power Research Institute (EPRI), electric utility representatives and their direct consultants, excluding direct commercial competitors, and the DOE National Laboratories under the prohibitions and restrictions above.

(B) This notice shall be marked on any reproduction of these data, in whole or in part.

ARC LIMITED RIGHTS STATEMENT:

This proprietary data, furnished under Subcontract Number ARC-93-3-SC-001 with ARC may be duplicated and used by the government and ARC, subject to the limitations of Article H-17.F. of that subcontract, with the express limitations that the proprietary data may not be disclosed outside the government or ARC, or ARC's Class 1 & 3 members or EPRI or be used for purposes of manufacture without prior permission of the Subcontractor, except that further disclosure or use may be made solely for the following purposes:

This proprietary data may be disclosed to other than commercial competitors of Subcontractor for evaluation purposes of this subcontract under the restriction that the proprietary data be retained in confidence and not be further disclosed, and subject to the terms of a non-disclosure agreement between the Subcontractor and that organization, excluding DOE and its contractors.

DEFINITIONS

CONTRACT/DELIVERED DATA — Consists of documents (e.g. specifications, drawings, reports) which are generated under the DOE or ARC contracts which contain no background proprietary data.

EPRI CONFIDENTIALITY / OBLIGATION NOTICES

NOTICE 1: The data in this document is subject to no confidentiality obligations.

NOTICE 2: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for limited purposes only. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited except as agreed to in advance by the Electric Power Research Institute (EPRI) and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted.

NOTICE 3: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for use only in evaluation tasks specifically authorized by the Electric Power Research Institute (EPRI). Any use, disclosure to unauthorized persons, or copying this document or parts thereof is prohibited except as agreed to in advance by EPRI and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted. This document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 4: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is being revealed in confidence and trust only to Employees of EPRI and to certain contractors of EPRI for limited evaluation tasks authorized by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. This Document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 5: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. Access to this data is given in Confidence and Trust only at Westinghouse facilities for limited evaluation tasks assigned by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. Neither this document nor any excerpts therefrom are to be removed from Westinghouse facilities.

EPRI CONFIDENTIALITY / OBLIGATION CATEGORIES

CATEGORY "A" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is contained in an issued reported.

CATEGORY "B" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is not contained in an issued report, except for computer programs.

CATEGORY "C" — Consists of CONTRACTOR Background Data except for computer programs.

CATEGORY "D" — Consists of computer programs developed in the course of performing the Work.

CATEGORY "E" — Consists of computer programs developed prior to the Effective Date or after the Effective Date but outside the scope of the Work.

CATEGORY "F" — Consists of administrative plans and administrative reports.

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

Included in Appendix A are Figures A-1 through A-197

Simplified Passive Advanced Light Water Reactor Plant Program

AP600 Probabilistic Risk Assessment

Prepared for

U.S. Department of Energy
San Francisco Operations Office

DE-AC03-90SF18495

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

Included in Appendix A are Figures A-1 through A-197

Simplified Passive Advanced Light Water Reactor Plant Program

AP600 Probabilistic Risk Assessment

Prepared for

U.S. Department of Energy
San Francisco Operations Office

DE-AC03-90SF18495

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

Included in Appendix A are Figures A-1 through A-197

Simplified Passive Advanced Light Water Reactor Plant Program

AP600 Probabilistic Risk Assessment

Prepared for

U.S. Department of Energy
San Francisco Operations Office

DE-AC03-90SF18495

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

Simplified Passive Advanced Light Water Reactor Plant Program

AP600 Probabilistic Risk Assessment

Prepared for

U.S. Department of Energy
San Francisco Operations Office

DE-AC03-90SF18495

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF TABLES (Cont.)

LIST OF FIGURES (Cont.)

LIST OF FIGURES (Cont.)

Included in Appendix A are Figures A-1 through A-197

CHAPTER 59

PRA RESULTS AND INSIGHTS

59.1 Introduction

This chapter summarizes the use of the AP600 PRA in the design process, PRA results and insights, plant features important to reducing risk, and PRA input to the design certification process.

AP600 is expected to achieve a higher standard of severe accident safety performance than currently operating plants, because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PRA insights, PRA success criteria analysis, severe accident research, and severe accident analysis. Since PRA considerations have been integrated into the AP600 design process from the beginning, many of the traditional PRA insights relating to currently operating plants are not at issue for the AP600. Both the Level 1 and Level 2 results show that addressing PRA issues in the design process leads to a low level of risk. The PRA results indicate that the AP600 design meets the higher expectations and goals for new generation passive pressurized water reactors (PWRs).

The total plant core damage frequency (CDF) and large release frequency from internal and external events, except seismic, at power and shutdown for the AP600 plant is calculated to be 3.0E-07 events per reactor-year and 2.4E-08 events per reactor-year, respectively. These frequencies are at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to many plant design features, with the dominant reduction coming from highly reliable and redundant passive safety-related systems that impact both at-power and shutdown risks. These passive systems are much less dependent on operator action and support systems than plant systems in currently operating plants.

A synopsis of the insights gained from the PRA about the AP600 design includes:

- The AP600 design benefits from the high level of redundancy and diversity of the passive safety-related systems. The passive systems have been shown to be highly reliable, their designs are simple so that a limited number of components are required to function.

- AP600 is less dependent on nonsafety-related systems than current plants or advanced light water reactor evolutionary plants. When no credit is taken for nonsafety-related systems following an accident, AP600 still meets the NRC safety goal, whereas current plants may not.

- The nonsafety-related support systems (ac power, component cooling water, service water, air) have a limited role in the plant risk profile because the passive safety-related systems do not require cooling water or ac power.

- AP600 is less dependent on human actions than current plants or advanced light water reactor evolutionary plants. Even when no credit is taken for operator actions, the AP600 meets the NRC safety goal, whereas current plants may not.

- The core damage and large release frequencies are low despite the conservative assumptions made in specifying success criteria for the passive systems. The success criteria have been developed in a more systematic, rigorous manner than typical PRA success criteria. The baseline success criteria are bounding cases for a large number of PRA success sequences. The baseline success sequences, in most cases, have been defined with:

  - worst break size and location for a given initiating event
  - worst automatic depressurization system (ADS) assumption in the success criterion
  - worst number of core makeup tanks (CMT) and accumulators
  - worst containment conditions for in-containment refueling water storage tank (IRWST) gravity injection.

  Many less-limiting sequences are therefore represented by a baseline success criteria.

- Single system or component failures are not overly important due to the redundancy and diversity of safety-related systems in the design. For example, the following lines of defense are available for reactor coolant system (RCS) makeup:

  - chemical and volume control system
  - core makeup tanks
  - partial automatic depressurization system in combination with normal residual heat removal
  - full automatic depressurization system with accumulators and in-containment refueling water storage tank
  - full automatic depressurization system with core makeup tanks and in-containment refueling water storage tank

- Typical current PRA dominant initiating events are significantly less important for the AP600. For example, the reactor coolant pump (RCP) seal loss-of-coolant accident

(LOCA) event has been eliminated as a core damage initiator since AP600 uses canned motor reactor coolant pumps which do not have seals. Another example is the loss of offsite power (LOOP) event. The station blackout and loss of offsite power event is a minor contributor to AP600 since the passive safety-related systems do not require the support of ac power.

- Passive safety-related systems are available in all shutdown modes. Planned maintenance of passive features is only performed during shutdown modes when that feature is not risk important. In addition, planned maintenance of nonsafety-related defense-in-depth features used during shutdown is performed at power.

- The AP600 passive containment cooling design is highly robust. Air cooling alone can prevent containment overpressurization, although the design has several lines of defense for containment cooling.

- The potential for containment isolation and containment bypass is lessened by having fewer penetrations to allow fission product release. In addition, all normally open and risk important penetrations are fail closed, thus eliminating the dependence on instrumentation and control (I&C) and batteries.

- The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential vessel failure mode. Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Therefore, AP600, through the prevention of core debris relocation to the containment, significantly reduces the likelihood of containment failure.

59.2 Use of PRA in the Design Process

The AP600 design has evolved over a period of years. PRA techniques have been used since the beginning in an iterative process to optimize the AP600 with respect to public safety. Each of these iterations has included:

- Development of a PRA model
- Use of the model to identify weaknesses
- Quantification of PRA benefits of alternate designs and operational strategies
- Adoption of selected design and operational improvements.

The scope and detail of the PRA model has increased from the early studies as the plant design has matured. This iterative design process has resulted in a number of design and operational improvements. The use of PRA in the AP600 is presented in this section as five distinct stages including: conceptual design analysis (stages 1 and 2), PRA analysis as part

of the design certification application (stage 3), and revisions of the PRA in support of further refinement of the design and modeling assumptions (stages 4 and 5).

59.2.1 Stage 1 - Use of PRA During the Early Design Stage

The initial AP600 design incorporated features that were intended to address leading causes of core damage and severe release, as identified from existing PRA studies, including the APWR (SP-90) and Sizewell. These features included passive safety-related core damage prevention and mitigation systems, active nonsafety-related systems, and other plant features. Passive safety-related core damage prevention systems are capable of mitigating PRA events, require no support systems other than instrumentation and control, and need fail safe equipment for the most common events. Passive system mitigative features included a reduced number of containment penetrations compared to currently operating plants, the penetrations that are open at power are fail safe, improvement of the interfacing systems loss-of-coolant accident event, and hydrogen igniters are provided in the containment. Other plant features factored into the initial design include a physical separation of electrical and instrumentation and control trains, reduction in the number of flooding sources, and a diverse actuation system (DAS) for anticipated transients without scram (ATWS) events.

Prior to 1989, several probabilistic scoping studies were performed on the AP600 conceptual design, which concentrated on quantifying the core damage frequency and large release frequency for internal initiating events during power operation. The early studies included detailed models of the passive safety-related fluid systems. They did not include detailed models of other systems such as instrumentation and control. The use of scoping studies was an iterative process at this stage of the design's evolution. Several feedback loops were included within the evaluation process: results and insights of a scoping study would identify areas of weakness, then alternative system designs and/or operational strategies were evaluated to optimize plant safety.

The outcome of the scoping study provided insights into the AP600 conceptual design, which led to many design and operational enhancements. Examples of design enhancements include:

- 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 which included a fourth depressurization stage off the hot leg with valve types diverse from the first three stages.

- Diverse automatic actuation for certain safety-related functions was introduced. In addition, separate and diverse manual actuation for certain safety-related functions was provided. Specifically, the diverse actuation system was provided to automatically actuate passive residual heat removal (PRHR), core makeup tank, passive containment cooling system (PCS), reactor protection function, automatic depressurization, and containment isolation. In addition, the system provides alarms and information to the main control room for manual actuation of these systems.

- The normal residual heat removal system (RNS) is a separate system from the spent fuel pool cooling system. The normal residual heat removal system, with piping routed outside of the containment, was designed with three containment isolation valves to reduce the probability of interfacing systems loss-of-coolant accident events that result in containment bypass.

- Protection system logic modifications are adopted to preclude steam generator overfilling during a steam generator tube rupture (SGTR) event. This reduces the need for full reactor depressurization and, therefore, reduces the frequency of core damage for steam generator tube rupture events with the containment bypassed.

- The number of onsite power supplies was increased to two nonsafety-related diesel generators.

In addition to plant design changes, some changes to the success criteria were made. In the early stages of the PRA, the success criteria were primarily based on engineering judgement or preliminary design basis analyses. However, during the iterative process of this stage of the PRA, some success criteria refinement was examined. An example is the success criteria originally did not credit the accumulators for mitigation of a small loss-of-coolant accident event. Further examination of the response of the accumulators to small and medium loss-of-coolant accidents indicated that, if the core makeup tanks fail, the accumulators will inject and the core will be cooled provided the operators manually initiate automatic depressurization system. Thus, the small and medium loss-of-coolant accident success criteria were enhanced.

Operational changes were also evaluated at this stage of the PRA. Initial automatic depressurization system valve positioning is an example of an operational change. Originally, the first three stages each contained two lines with two normally closed motor-operated valves. The valve configuration was changed to one valve open and one valve closed in each line to allow for testing during refueling.

59.2.2 Stage 2 - Preliminary PRA

Beginning in 1989, a preliminary PRA was conducted in support of the Westinghouse AP600 application for design certification. The preliminary PRA was performed on the AP600 design that existed at the time of completion of the scoping studies along with design changes made as a result of the final scoping study. The scope of the PRA was also expanded to evaluate both at-power and shutdown conditions as well as external events. Because the AP600 design was evolving throughout this period, the success criteria were primarily based on engineering judgement derived from preliminary design basis safety analyses. The system and component dependency analysis and the data used in the preliminary PRA were deliberately conservative. The results of the preliminary PRA identified important areas of

the AP600 design where the design effort would focus. Examples of specific system design changes made during this stage of the PRA include:

- The in-containment refueling water storage tank 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 two series check valves. 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. Instead, the system operates solely by pressure differential between the pressure in the in-containment refueling water storage tank and the pressure of the direct vessel injection (DVI) line.

- 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. Thus, the resulting recirculation path consists of one line of two motor-operated valves and one line of two series check valves.

- Alarms are 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.

In the first stage of the PRA, the success criteria were primarily based on engineering judgement. For this stage of the PRA, the success criteria were refined. Examples of more refined success criteria include:

- The more significant success criteria change related to the depressurization system. The original success criterion for a small loss-of-coolant accident was one-half of all the automatic depressurization system stages were required. Taking credit for a design change that increased the size of the fourth-stage valves and performing best-estimate loss-of-coolant accident calculations allowed the use of a success criteria that tolerated multiple failures.

- Analysis shows that the containment cooling system only requires air cooling to prevent containment failure.

Operational changes were also made as part of this stage of 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 start the normal residual heat removal system, it was necessary for the operators to locally open three valves. 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 the scoping PRA stage, the automatic depressurization system stage 1, 2, and 3 valve configuration was 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, during the preliminary PRA stage, the automatic depressurization system valve configuration was changed to two closed valves with quarterly testing.

59.2.3 Stage 3 - AP600 PRA Submittal to NRC (1992)

The third stage culminated with the submittal of the AP600 PRA report, along with the *AP600 Standard Safety Analysis Report* (SSAR), to the NRC on June 26, 1992. This stage included a complete Level 3 PRA. The PRA factored in design changes made as a result of the preliminary PRA findings. The success criteria assumptions were verified. Some of the conservative data and dependency factors were adjusted to be more realistic during this stage. The outcome of the PRA program, which was characterized by frequent interactions between PRA analysts and design engineers, is an AP600 design that exceeds the NRC and ALWR Utility Requirements Document safety goals.

Because of the extensive interactions during previous design/PRA studies, few plant changes resulted from this study. Two design changes that did result include:

- The core makeup tank can now be actuated on a low steam generator level plus high hot leg temperature indication. This was done to indirectly reduce the importance of operator actions to initiate passive feed and bleed.

- The scope of the diverse actuation system was expanded to include control rod insertion. The system was also expanded to include an actuation signal for opening of the in-containment refueling water storage tank motor-operated valves during mid-loop operations. This was done to provide automatic operation to reduce the dependence on operators to open the valves in the event of an accident during mid-loop operation.

59.2.4 Stage 4 - PRA Revision 1 (1994)

Stage 4 was the first revision to the AP600 PRA. The revision, submitted in July 1994, included the following major changes: introduction of phenomonology onto the Level 2

containment event tree and performance of the risk-based seismic margins analysis. In addition to Revision 1 of the PRA, this stage also included the focused PRA sensitivity study and initiating event evaluation as part of the regulatory treatment of nonsafety-related systems (RTNSS) topic.

In September 1993, the focused PRA sensitivity study and initiating event evaluation were submitted to the NRC via the *AP600 Implementation Report for Regulatory Treatment of Nonsafety-Related Systems* (WCAP-13856). The focused PRA sensitivity study evaluated the core damage and large release frequencies for AP600 without taking mitigation credit for nonsafety-related systems. The results of the study show that even with no credit taken for nonsafety-related systems, AP600 meets the regulatory goals.

The Level 2 PRA was revised to introduce the use of decomposition event trees and to incorporate phenomena onto the containment event tree. Six decomposition event trees were created to analyze the following phenomena:

- In-vessel retention of molten core debris
- Thermally induced failures of the reactor coolant system pressure boundary
- In-vessel steam explosion
- Ex-vessel steam explosion
- Ex-vessel debris coolability
- Hydrogen combustion analysis.

A containment event tree displays the characteristics of the severe accident progression that impact the fission-product source term to the environment. The containment event tree from the Stage 3 PRA that was submitted to the NRC in 1992 was enhanced to include the phenomena that was analyzed in the decomposition event trees.

A risk-based seismic margins analysis was also performed as part of Revision 1 of the AP600 PRA.

There were no appreciable changes in the plant design as a result of this stage of the PRA.

59.2.5 Stage 5 - PRA Revisions 2 - 6 (1995)

This stage includes the updates leading to various revisions submitted to the NRC during 1995. The changes made to the PRA resulted from plant changes and NRC questions. Most plant changes incorporated into the PRA were made for other reasons than the PRA. The design changes resulted in small improvements to the core damage and large release frequencies. The primary emphasis of this stage of the PRA was to refine the success criteria calculations and the system and event tree modeling. Some of the PRA-related feedback to the design is summarized below.

- Further refinement of the PRA success criteria calculations resulted in making the automatic depressurization system success criteria more conservative.

- The automatic depressurization system stage 4 valves were changed from air-operated to explosive-operated (squib) valves. This design change was not PRA-motivated; however, a PRA sensitivity study was performed to provide input into the decision to change the fourth-stage valves to squib valves.

- Service water blowdown procedures and sources of makeup water were evaluated as a function of service water heat loads during various plant conditions to ensure that the assumed success criteria will be met. The heat loads were also evaluated to assess the required number of cooling tower fans that must operate to ensure adequate cooling. In addition, the initial fault tree evaluated indicated the potential vulnerability to bypass flow occurring upon loss of a dc power supply causing an air-operated valve to open. Consequently, the power supplies to the equipment were reevaluated.

- Initial PRA modeling of the need to open the main generator breaker in the fault trees for the 4160 vac buses following a plant trip highlighted the importance of certain functions initially assumed to be performed by the plant control system. It was determined that the plant control system would not be fast enough to perform this action and that a reverse power relay would control opening this breaker.

59.3 Core Damage Frequency from Internal Initiating Events at Power

Internal initiating events are transient and accident initiators that are caused by plant system, component, or operator failures. External initiating events, which include internal fire and flooding events, and events at shutdown are discussed in other subsections.

The AP600 mean plant core damage frequency for internal initiating events at power is calculated to be 2.4E-07 events per year. Twenty-six separate initiating event categories were defined to accurately represent the AP600 design. Of these event categories, 11 are loss-of-coolant accidents (LOCAs), 12 are transients, and 3 are anticipated transients without scram precursors (initiating events that result in an anticipated transient without scram sequence as a result of failure to trip the reactor). Initiating event categories unique to the AP600 design have been defined and evaluated, including safety injection line breaks, core makeup tank line breaks, and passive residual heat removal heat exchanger (HX) tube ruptures. The resulting core damage frequency is very small; a value of 2.4E-07 means that only one core damage event is expected in over 4 million plant-years of operation. This core damage frequency value is two orders of magnitude (i.e., 100 times) smaller than corresponding values typically calculated for current pressurized water reactors.

The contribution of initiating events to the total plant core damage frequency is summarized in Table 59-1. Figure 59-1 illustrates the relative contributions to core damage frequency from the various at-power initiating events.

Six initiating events, including five loss-of-coolant accidents and one anticipated transient without scram precursor, comprise approximately 91 percent of the total at-power plant core

damage frequency. The remaining 20 initiating events contribute a total of approximately 9 percent to the core damage frequency from internal events. The dominant initiating events are:

- Safety injection line break
- Anticipated transient without scram precursor with loss of main feedwater
- Intermediate loss-of-coolant accident
- Large loss-of-coolant accident
- Reactor vessel rupture
- Medium loss-of-coolant accident

Within this group of events, the first four each contribute more than 10 percent to the total core damage frequency. These four events account for approximately 85 percent of the total core damage frequency.

The results show a very low core damage frequency dominated by rare events (i.e., intermediate, medium, and large loss-of-coolant accidents, and anticipated transients with failure of reactor trip). This indicates that the AP600 design is robust with respect to its ability to withstand challenges from more frequent events (e.g., transients) and that adequate protection against the more severe events is provided through the defense-in-depth features.

While the anticipated transient without scram contribution appears to be relatively important, this is due in part to PRA modeling simplifications whereby core damage has been assumed to occur if certain combinations of failures occur. For example, core damage is assumed to occur if the protection and safety monitoring system (PMS) and diverse actuation system (DAS) fail (approximately 12 percent of total core damage frequency); if reactor coolant system (RCS) pressure relief fails (approximately 8 percent of total core damage frequency); or if startup feedwater and passive residual heat removal fail. In reality, plant response similar to loss-of-coolant accident response is more likely given these scenarios, with a significant probability of avoiding core damage. The modeling simplifications were made because the anticipated transient without scram core damage frequency is already very low.

Information regarding loss-of-coolant accident categories defined for the AP600 PRA was presented in the discussion of PRA success criteria. For the PRA, the various loss-of-coolant accident categories have been defined based on which plant features are required to mitigate the events. As a result, the PRA and SSAR Chapter 15 loss-of-coolant accident size definitions are not identical. The following listing shows how the PRA and SSAR break sizes are related and identifies the PRA size criteria.

- SSAR Chapter 15 break size definitions are large (break size greater than 1 $ft.^2$) or small (break size less than 1 $ft.^2$).

- PRA break sizes are defined as follows:

  - Large breaks are those with an equivalent inside diameter of approximately 9 in. or larger. Reactor vessel rupture is included in this category. The automatic depressurization system (ADS) is not required for in-containment refueling water storage tank (IRWST) injection for large breaks.

  - Medium breaks are those with an equivalent inside diameter between approximately 5 in. and 9 in. Core makeup tank line breaks and safety injection line breaks are included in this category. Automatic depressurization system is not required for normal residual heat removal system (RNS) operation for medium breaks, but is required for in-containment refueling water storage tank injection.

  - Intermediate breaks are those with an equivalent inside diameter between approximately 2 in. and 5 in. Operation of automatic depressurization system stages 1, 2, or 3 (or, alternatively, passive residual heat removal) is not required to satisfy the automatic depressurization system stage 4 automatic actuation pressure interlock with intermediate breaks, but is required to depressurize the reactor coolant system to the normal residual heat removal system operating pressure.

  - Small breaks are those with an equivalent inside diameter between approximately 3/8 in. and 2 in. Steam generator tube rupture and passive residual heat removal heat exchanger tube rupture break sizes fall within this range, but are evaluated as separate events based on differing initial plant response. Small breaks are larger than those for which the chemical and volume control system (CVS) can maintain reactor coolant system water level, but not large enough to allow automatic actuation of automatic depressurization system stage 4 without operation of either automatic depressurization system stages 1, 2, or 3 or passive residual heat removal.

  - Coolant losses smaller than those resulting from small breaks are defined as reactor coolant system leaks. Operation of one chemical and volume control system makeup pump can maintain reactor coolant system water inventory for reactor coolant system leaks.

59.3.1 Dominant Core Damage Sequences

A total of 566 potential core damage event sequences for internal initiating events at power are modeled in the AP600 PRA. These core damage sequences are the combinations of initiating event occurrences and subsequent successes and failures of plant systems and operator actions that result in core damage. Some of these sequences are composite sequences, i.e., they consist of similar event sequences that are combined and analyzed together (such as consequential steam generator tube rupture resulting from various initiators). Therefore, a larger number of sequences are actually represented by the model. Of these

566 event sequences, 208 result in frequencies ranging from 8E-08 to 2E-15 events per year. The remaining sequences do not produce any cutsets representing them in the top 21,000 cutsets; that is, their core damage frequencies are not significant relative to the core damage frequencies for the other sequences.

The majority of the core damage frequency is represented by the top sequences, specifically:

- The 10 sequences with the highest core damage frequency together contribute approximately 87 percent of the total core damage frequency (2.12E-07 events per year)
- The top 13 sequences contribute approximately 90 percent (2.19E-07 events per year)
- The top 50 sequences contribute approximately 99.2 percent (2.41E-07 events per year)
- The top 100 sequences contribute over approximately 99.9 percent (2.43E-07 events per year)

Each core damage sequence is composed of component-level cutsets, with a total of approximately 21,000 cutsets included in the baseline analysis of internal initiating events at power (100 percent of 2.43E-07 events per year core damage frequency). A cutset is a combination of initiating event occurrence and the component or operator failures that constitute the various system-level failures that lead to core damage.

- The 100 highest frequency cutsets together contribute approximately 90 percent of the total core damage frequency (approximately 2.18E-07 events per year)
- The top 200 cutsets contribute approximately 94 percent (2.28E-07 events per year)
- The top 500 cutsets contribute approximately 97 percent (2.35E-07 events per year)
- The top 1,000 cutsets contribute approximately 98 percent (2.39E-07 events per year)
- The top 2,000 cutsets contribute approximately 99 percent (2.41E-07 events per year)

The top 13 accident sequences that contribute 90 percent of the core damage frequency from internal initiating events at power are discussed in this section. These sequences are listed in Table 59-2 and discussed in detail later in this chapter.

The following information is provided to aid the reader in understanding the information presented for these dominant sequences:

- An identifier is provided along with the sequence name that corresponds to the sequence in the event trees. The sequence identifier indicates the name of the event tree for the initiating event and the sequence number on that event tree. For example, SI-LB-02 stands for the second sequence, or path, on the safety injection line break (SI-LB) event tree.

- Sequence frequency is the core damage frequency contributed by the individual sequence. It is the initiating event frequency multiplied by the probabilities of failure and success of the various systems modeled to mitigate the event and prevent core damage. Any given sequence may have both successes and failures of various systems; for a core damage sequence, the set of failures implies that at least one of the success criteria defined for prevention of core damage was not met.

- Contribution to core damage is the percentage of the total core damage frequency from initiating events that was produced by the sequence in question.

- Initiating event frequency is the number of events per year calculated for the type of core damage initiator in question.

- Conditional core damage probability is defined as the ratio of event sequence frequency divided by the initiating event frequency. It provides a measure of the reliability of plant features for mitigating a core damage initiator.

The conditional core damage probability results for the dominant core damage sequences indicate the following:

- The conditional probability of core damage, given the occurrence of a loss-of-coolant accident, is generally in the range of about 1E-04 to 1E-05 (with the exception of reactor vessel rupture, for which core damage is assumed). This indicates that the various features of the AP600 would act to prevent core damage from all but between 1 in 10,000 and 1 in 100,000 loss-of-coolant accidents. Since loss-of-coolant accidents are relatively rare events, this is a significant level of protection.

- The conditional probability of core damage, given the occurrence of the most limiting anticipated transient without scram precursor, is on the order of 5E-08. Anticipated transient without scram precursors are more frequent than loss-of-coolant accidents (anticipated transient without scram precursor frequency is on the order of one per year). However, AP600 features provide a high level of protection against core damage (only 1 in 20 million such events is expected to lead to core damage), resulting in a low anticipated transient without scram core damage frequency.

Sequence 1: Safety Injection Line Break (SI-LB-02)

Sequence Frequency: 8.4E-08/year
Contribution to Core Damage: 34 percent
Initiating Event Frequency: 1.0E-04/year
Conditional Core Damage Probability: 8.0E-04

Description of Sequence

The initiating event is a break that occurs in one of the two safety injection lines (including the direct vessel injection (DVI) line and the line that connects the core makeup tank, accumulator, or in-containment refueling water storage tank to the direct vessel injection), resulting in a loss of reactor coolant. All capability for reactor coolant system injection from the core makeup tank and in-containment refueling water storage tank through this broken line is postulated to be lost due to excessive spillage through the break, but core makeup tank injection through the intact line is successful. Full reactor coolant system depressurization, (depressurization to the pressure at which in-containment refueling water storage tank gravity injection can occur) is successful through operation of automatically or manually actuated automatic depressurization system operation. However, in-containment refueling water storage tank injection through the intact line fails. All normal residual heat removal system injection is assumed to spill through the break and, as a result, is unavailable.

Core damage is postulated due to reactor coolant loss through the break and the open automatic depressurization system valves, with subsequent lack of capability to maintain reactor coolant inventory due to failure of injection through the intact in-containment refueling water storage tank line. Core damage will be delayed since core makeup tank injection is successful; accumulator injection is expected due to the success of full reactor coolant system depressurization via the automatic depressurization system, but its status is not evaluated in this sequence since core damage would not be prevented without in-containment refueling water storage tank injection.

This sequence is assigned to the 3BE plant damage state. The definition of this plant damage state is full depressurization at the time of core damage, with successful core makeup tank and accumulator injection.

For this event, the redundant injection path for reactor coolant system inventory makeup is disabled by the break. This leaves only one injection path, which results in a relatively high frequency of core damage from this event. In this sequence, only one system fails, in-containment refueling water storage tank injection.

Important Modeling Assumptions

- It is assumed that the break is large enough to cause one injection path to fail due to excessive spillage of the injected water. If a smaller break were to occur, the loss

through the break and the spillage of the injected water through the break would be less, which might provide alternative success criteria.

- The size of the break in the safety injection line can range from small to medium loss-of-coolant accidents. For this analysis, a medium loss-of-coolant accident is postulated.

- It has been conservatively assumed that the break occurs in the line to which the normal residual heat removal system is connected. Thus, no credit is given for operation of the normal residual heat removal system following successful depressurization of the reactor coolant system.

Risk Important Failures

The dominant cutsets for this sequence are provided in Table 59-3. These cutsets show that the risk important failures are:

- Common cause and random failure of both check valves on the intact in-containment refueling water storage tank discharge line (70-percent contribution)

- Plugging of the in-containment refueling water storage tank discharge line strainer in the intact line (30-percent contribution)

This sequence does not depend directly on success of operator actions. Credit is given for manual actuation of the core makeup tank and automatic depressurization system as a backup action if automatic actuations fail. The core damage frequency of this sequence would not change significantly if these actions were not credited.

Sequence 2: Anticipated Transient Without Scram Precursor (Loss of Normal Feedwater with Failure of Reactor Trip) (ATWS-1-07)

Sequence Frequency: 3.0E-08/year
Contribution to Core Damage: 12 percent
Initiating Event Frequency: 6.1E-01/year (anticipated transient without scram precursor without main feedwater)
Conditional Core Damage Probability: 4.9E-08

Description of Sequence

A loss of main feedwater transient occurs. Reactor trip is needed, but both automatic and manual reactor trip fail as a result of the failure of the protection and safety monitoring system to provide a trip signal to the reactor trip breakers. Automatic and manual reactor trip using the diverse actuation system also fail. Core damage is postulated because the failures involved in the protection and safety monitoring system and diverse actuation system are assumed to prevent actuation of any other safety systems, resulting in reactor coolant system overpressure, loss of reactor coolant system integrity and inventory, and core damage. This sequence is assigned to the 3A core damage state (high-pressure core damage) without further analysis.

Important Modeling Assumptions

- Common cause failures of instrumentation and control hardware will affect only similar hardware (only similar groups of control boards, not all boards, are affected by a given hardware common cause failure).

- Core damage occurs through subsequent overpressure, loss of inventory, and loss of core cooling if the protection and safety monitoring system and diverse actuation system reactor trip signals fail.

- In this sequence, no credit is taken for the ability of active or passive safety-related systems to provide reactor coolant system makeup and core cooling following a break in the reactor coolant system as a result of overpressure caused by the loss of feedwater and failure to trip the reactor.

Risk Important Failures

The dominant cutsets for this sequence are provided in Table 59-4. For this sequence, contributing failures involve the failure of both the protection and safety monitoring system and diverse actuation system to actuate a reactor trip and failure of the operators to take action to trip the reactor in a timely manner. The most important failures are:

- Operator fails to perform manual reactor trip either by the protection and safety monitoring system (action to initiate opening of the reactor trip breakers) or by the

diverse actuation system (action to initiate tripping of the control rod motor-generator sets)

- Common cause hardware failure of the protection and safety monitoring system boards
- Hardware failure of the diverse actuation system
- Failure of the diverse actuation system transmitters (turbine impulse chamber pressure transmitters are modeled)

Credit is taken for manual trip of the reactor by the operators using either the protection and safety monitoring system or diverse actuation system cues and equipment. The combined failure probability of the operator actions in the protection and safety monitoring system and diverse actuation system for this sequence is 0.027. This is a relatively high probability of failure (almost 3 failures in 100 attempts) as a result of the modeling of the diverse actuation system-related operator action as strongly dependent on the protection and safety monitoring system-related action. The action for manual trip by the operator appears in most of the cutsets. If no credit is taken for this action, the sequence frequency would increase to about 1.0E-06.

Sequence 3: Anticipated Transient Without Scram Precursor (Loss of Normal Feedwater with Failure of Reactor Trip) (ATWS-28)

Sequence Frequency: 2.0E-08/year
Contribution to Core Damage: 8 percent
Initiating Event Frequency: 6.1E-01/year (anticipated transient without scram precursor without main feedwater)
Conditional Core Damage Probability: 3.3E-08

Description of Sequence

This sequence encompasses all combinations of failures on the anticipated transient without scram loss of main feedwater precursor event tree that do not directly lead to success or to core damage, and for which further evaluation of plant response is modeled in the event tree. There are several scenarios encompassed by this sequence:

- Failure of reactor trip as a result of failure of the protection and safety monitoring system trip signal, success of the diverse actuation system trip signal, but failure of the control rod motor-generator sets to open

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, and failure of the diverse actuation system reactor trip signal

- Successful protection and safety monitoring system trip signal generation, failure of the reactor trip breakers to open, successful diverse actuation system trip signal generation, but failure of the control rod motor-generator sets to trip

In each scenario, both automatic and manual actuations are modeled for the protection and safety monitoring system and diverse actuation system.

Following failure to trip the reactor, heat removal by either startup feedwater or passive residual heat removal is successful. The operators fail to actuate the rod control system (via the plant control system) so that the control rods fail to step into the core. This leads to a heatup and pressurization of the reactor coolant system. Reactor coolant system pressure relief fails as a result of either failure of one or both of the pressurizer safety valves to open, or as a result of the occurrence of the event early in the fuel cycle, during which the core reactivity feedback is not adequate to prevent reactor coolant system heatup in excess of the safety valve relief capacity.

Core damage is postulated due to reactor coolant system pressure in excess of 3200 psig, which is beyond the established stress limits for the reactor coolant system (and beyond design basis and analysis domain). Thus, core damage is postulated due to lack of analysis. In reality, it is likely that a break would occur in the reactor coolant system due to the high pressure; this break would relieve the high reactor coolant system pressure, allowing operation

of the various mitigation systems. This sequence is assigned to the 3A plant damage state, in which the reactor coolant system is at high pressure when core damage occurs.

Important Modeling Assumptions

- There is a period of time at the beginning of each cycle during which core reactivity feedback is not sufficient to prevent overpressurization of the reactor coolant system given a loss of normal feedwater anticipated transient without scram. However, if the operators can initiate the stepping in of the control rods within one minute after the event occurs, sufficient negative reactivity will be inserted to eliminate the concern that the capacity of the safety valves is exceeded due to insufficient reactivity feedback.

- If reactor coolant system pressure goes beyond 3200 psi, core damage is assumed; no credit for loss-of-coolant accident-mitigating systems is credited.

- The time available for operator actions to trip the reactor is very short (approximately 2 minutes) for the loss of normal feedwater anticipated transient without scram.

Risk Important Failures

The dominant cutsets for this sequence are listed in Table 59-5. They indicate that the following failures are risk important in this sequence:

- Failure of reactor coolant system overpressure protection due to either pressurizer safety valves failing to open or adverse reactivity feedback considerations

- Failure of control rod motor generator sets to deenergize

- Common cause failure of protection and safety monitoring system hardware

- Common cause failure of reactor trip breakers to open

Three operator actions are important to success for this sequence. These are:

- Operator actuation of reactor trip via the protection and safety monitoring system

- Operator actuation of reactor trip (motor-generator set trip) by diverse actuation system

- Operator actuation of control rod insertion via the plant control system (PLS)

Sequence 4: Large Loss-of-Coolant Accident (LLOCA-03)

Sequence Frequency: 1.7E-08/year
Contribution to Core Damage: 7 percent
Initiating Event Frequency: 1.1E-04/year
Conditional Core Damage Probability: 1.6E-04

Description of Sequence

This sequence is a large loss-of-coolant accident initiating event (equivalent to a break diameter of greater than 9 in., other than reactor vessel rupture), followed by successful injection by one or more accumulators, but failure of the in-containment refueling water storage tank injection from both lines. Core damage is postulated due to in-containment refueling water storage tank injection failure, after which it is assumed that the loss of reactor coolant system inventory can not be made up in time to prevent core damage. After the accumulators have fully injected, the reactor coolant system water level will keep dropping due to boil-off and coolant losses through the break.

This sequence is assigned to the 3BE plant damage state, which is defined as full depressurization with successful core makeup tank and accumulator injection. The reactor coolant system is at low pressure due to depressurization through the break.

Important Modeling Assumptions

- No credit is taken for core makeup tank injection; core makeup tank injection is expected and would delay, but not prevent, core damage.

Risk Important Failures

Dominant cutsets for this sequence are listed in Table 59-6. The dominant failure for this sequence is the common cause failure of in-containment refueling water storage tank injection line check valves to open. These valves can only be tested and maintained during a refueling outage. Thus, the failure exposure time assigned to them is large, which makes the failure probability high.

There are no operator actions modeled in this sequence.

Sequence 5: Safety Injection Line Break (SI-LB-03)

Sequence Frequency: 1.6E-08/year
Contribution to Core Damage: 6.5 percent
Initiating Event Frequency: 1.0E-04/year
Conditional Core Damage Probability: 1.5E-04

Description of Sequence

The initiating event is a break that occurs in one of the two safety injection lines, resulting in a loss of reactor coolant. All capability for reactor coolant system injection from the core makeup tank and in-containment refueling water storage tank through this broken line is postulated to be lost due to excessive spillage through the break, but core makeup tank injection through the intact line is successful. Full reactor coolant system depressurization via the automatic depressurization system fails, i.e., depressurization to the pressure at which in-containment refueling water storage tank injection can occur.

Core damage is postulated due to the inability to inject in-containment refueling water storage tank water into the core after the core makeup tank inventory is depleted, because, without automatic depressurization system operation, the reactor coolant system pressure remains above the pressure at which in-containment refueling water storage tank injection can occur.

This sequence is assigned plant damage state 3D, which is defined as core damage with partial depressurization of the reactor coolant system (in this case, due to the break).

Important Modeling Assumptions

- Credit is taken for both automatic and manual automatic depressurization system actuation, both of which are unsuccessful in this sequence.

- It is assumed that the break is large enough to cause one injection path to fail due to excessive spillage of the injected water. If a smaller break were to occur, the loss through the break and the spillage of the injected water through the break would be less; this might provide alternative success criteria (e.g., reactor coolant system depressurization using automatic depressurization system stages 1, 2, and 3 rather than stage 4).

- The size of the break in the safety injection line can range from small to medium loss-of-coolant accidents. For this analysis, a medium loss-of-coolant accident is postulated.

- It has been conservatively assumed that the break occurs in the line to which the normal residual heat removal system is connected.

Risk Important Failures

The dominant cutsets for this sequence are provided in Table 59-7. The dominant failure is the common cause failure of the automatic depressurization system fourth-stage squib valves (explosive valves) to open after an actuation signal is received. Failure of automatic and manual automatic depressurization system actuation is a much lower contributor to automatic depressurization system failure.

The following operator actions are modeled for manual actuation of the automatic depressurization system, if automatic actuation fails:

- Operator fails to recognize the need for automatic depressurization system actuation or fails to actuate the system using protection and safety monitoring system-related cues and equipment

- Operator fails to actuate automatic depressurization system using diverse actuation system cues and equipment. This failure is assigned a failure probability corresponding to a high dependence on the preceding action to actuate automatic depressurization system using protection and safety monitoring system

Sequence 6: Intermediate Loss-of-Coolant Accident (NLOCA-04)

Sequence Frequency: 1.2E-08/year
Contribution to Core Damage: 4.8 percent
Initiating Event Frequency: 7.7E-04/year
Conditional Core Damage Probability: 1.5E-05

Description of Sequence

This is an intermediate loss-of-coolant accident initiating event with a break size range equivalent to a 2- to 5-in. diameter. After the break occurs, a core makeup tank injection signal is generated, either one or both core makeup tanks actuate, the reactor coolant pumps trip, and the core makeup tanks inject when required. Full reactor coolant system depressurization (depressurization to the point at which in-containment refueling water storage tank injection can occur) using the automatic depressurization system valves is successful, but both the normal residual heat removal system and the in-containment refueling water storage tank fail to inject.

Core damage is postulated due to the failure to make up reactor coolant system inventory from both long-term sources (normal residual heat removal system and in-containment refueling water storage tank) after the core makeup tank has injected. The sequence is assigned to the 3BE plant damage state. The reactor coolant system is at low pressure due to depressurization through the break. This sequence involves failures of both safety-related (in-containment refueling water storage tank) and nonsafety-related (normal residual heat removal) systems.

Important Modeling Assumptions

- Credit is taken for automatic and manual actuation of automatic depressurization system. Only manual actuation is credited for the normal residual heat removal system.

Risk Important Failures

The dominant cutsets for this sequence are provided in Table 59-8. The following are the risk important failures:

- Common cause failure of the check valves in both in-containment refueling water storage tank injection lines to open
- Normal residual heat removal system isolation motor-operated valves (MOVs) 011, 022, or 023 fail to open due to hardware failure
- In-containment refueling water storage tank motor-operated valves 117B or 118B fail to open, resulting in failure of normal residual heat removal system recirculation
- Common cause plugging of strainers in in-containment refueling water storage tank

The models credit an operator action for actuation of the normal residual heat removal system. There is no modeled operator action for in-containment refueling water storage tank injection.

Sequence 7: Intermediate Loss-of-Coolant Accident (NLOCA-06)

Sequence Frequency: 1.1E-08/year
Contribution to Core Damage: 4.4 percent
Initiating Event Frequency: 7.7E-04/year
Conditional Core Damage Probability: 1.4E-05

Description of Sequence

An intermediate loss-of-coolant accident initiating event occurs (equivalent to a 2- to 5-in. diameter break). After the break occurs, a core makeup tank injection signal is generated, either one or both core makeup tanks actuate, the reactor coolant pumps (RCPs) trip, and the core makeup tanks inject when required. Full reactor coolant system depressurization fails (depressurization via the automatic depressurization system valves to the pressure at which in-containment refueling water storage tank injection can occur), but partial depressurization is successful (depressurization via automatic depressurization system to the pressure at which normal residual heat removal system injection can occur). However, normal residual heat removal system injection fails.

Core damage is postulated due to the inability to provide reactor coolant system makeup after the core makeup tank empties, as a result of normal residual heat removal system failure and the inability to inject from the in-containment refueling water storage tank as a result of the failure to depressurize sufficiently. This sequence is assigned plant damage state 3D, which is defined as core damage with partial depressurization of the reactor coolant system.

Important Modeling Assumptions

- Credit is taken for the ability to depressurize the reactor coolant system partially (to normal residual heat removal system injection pressure) via the automatic depressurization system if full reactor coolant system depressurization via the automatic depressurization system fails. The automatic depressurization system success criteria for partial depressurization are less restrictive than the automatic depressurization system success criteria for full depressurization.

- Credit is taken for manual actuation of the normal residual heat removal system following partial depressurization.

- For this sequence, the full depressurization success criteria for automatic depressurization system require operation of the fourth-stage automatic depressurization system valves, with no credit for the first three stages. The automatic depressurization system success criteria are determined assuming operation of only one core makeup tank; with both core makeup tanks injecting, there could be a higher probability of successful full depressurization.

Risk Important Failures

The dominant cutsets for this sequence are provided in Table 59-9. The following failures are risk important:

- Common cause failure of automatic depressurization system fourth-stage squib (explosive) valves to open
- Normal residual heat removal system isolation motor-operated valves 011, 022, or 023 fail to open due to hardware failures
- In-containment refueling water storage tank motor-operated valves 117B or 118B fail to open, resulting in failure of normal residual heat removal system recirculation

The models credit an operator action for actuation of the normal residual heat removal system. Credit is also given for manual actuation of automatic depressurization system if automatic actuation fails.

Sequence 8: Reactor Vessel Rupture (RV-RP-02)

Sequence Frequency: 1.0E-08/year
Contribution to Core Damage: 4.1 percent
Initiating Event Frequency: 1.0E-08/year
Conditional Core Damage Probability: 1.0

Description of Sequence

A reactor vessel rupture event occurs. This event prevents the core from remaining covered with water due to the size and location of the break. Core damage is postulated as a direct result of the initiating event.

This event is assigned the 3C plant damage state category, which is a special category for the reactor vessel rupture initiating event.

Important Modeling Assumptions

It is assumed that the safety-related systems cannot keep the core covered after the event occurs.

Risk Important Failures

The initiating event frequency is the only risk important failure. There are no operator actions modeled. The only cutset for this event (as shown in Table 59-10) is the occurrence of the initiating event.

Sequence 9: Large Loss of Coolant Accident (LLOCA-04)

Sequence Frequency: 7.3E-09/year
Contribution to Core Damage: 3.0 percent
Initiating Event Frequency: 1.1E-04/year
Conditional Core Damage Probability: 6.7E-05

Description of Sequence

A large loss-of-coolant accident initiating event occurs (break size equivalent to greater than 9-in. in diameter). Both accumulators fail to inject. Core damage is postulated due to core uncovery as a result of accumulator injection failure; core damage occurs before in-containment refueling water storage tank injection can reflood the core. No credit is taken for core makeup tank injection. This sequence is assigned to the 3BR plant damage state, which is defined as full reactor coolant system depressurization with failure of both accumulators and core makeup tanks.

Important Modeling Assumptions

- No credit is taken for core makeup tank injection; core makeup tank injection is expected, but it is assumed to be too slow to prevent core damage for this event. Core damage is assumed to occur solely on the failure of accumulators. This is conservative since it is expected that core makeup tank injection would be effective for breaks at the smaller end of the size range defined for a large loss-of-coolant accident in the PRA.

Risk Important Failures

The dominant cutsets for this sequence are listed in Table 59-11. Common cause failure of the accumulator check valves to open is the dominant failure mode. This is followed by various combinations of random failure of two check valves to open. There are no operator actions modeled in this sequence.

Sequence 10: Intermediate Loss of Coolant Accident (NLOCA-16)

Sequence Frequency: 5.8E-09/year
Contribution to Core Damage: 2.4 percent
Initiating Event Frequency: 7.7E-04/year
Conditional Core Damage Probability: 7.5E-06

Description of Sequence

An intermediate loss-of-coolant accident initiating event occurs (equivalent to a 2- to 5-in. diameter break). After the break occurs, a core makeup tank injection signal is generated, but one or more reactor coolant pumps fail to trip; this failure is assumed to prevent effective core makeup tank injection. Both full reactor coolant system depressurization (depressurization via the automatic depressurization system valves to the pressure at which in-containment refueling water storage tank injection can occur) and partial depressurization (depressurization via automatic depressurization system to the pressure at which normal residual heat removal system injection can occur) fail.

Core damage is postulated due to the inability to provide reactor coolant system injection. Failure of the reactor coolant pump trip prevents core makeup tank injection, and failure of automatic depressurization system prevents injection from both the normal residual heat removal system and the in-containment refueling water storage tank in time to prevent core damage.

This sequence is assigned to the 1AP plant damage state. This state is defined as a small loss of coolant with failure to depressurize but with passive residual heat removal operating. In this sequence, the status of passive residual heat removal is not determined, but the break size is sufficiently large that at least partial depressurization is provided.

Important Modeling Assumptions

- Core makeup tank injection is assumed to fail as a result of failure of reactor coolant pump trip.
- In this sequence, no credit is taken for automatic depressurization system actuation, as a result of the failure of core makeup tank injection. This makes operator actions important in this sequence.
- A relatively high failure probability is assigned to the failure to trip reactor coolant pumps, since the reactor coolant pump breakers can only be tested during a refueling outage. Thus, the failure exposure time assigned to them is large, which makes the failure probability high.

Risk Important Failures

The dominant cutsets for this sequence are shown in Table 59-12. Risk important component failures are related to failure of the reactor coolant pumps to trip:

- Common cause failure to open of 4.16 Kvac circuit breakers to trip the reactor coolant pumps
- Reactor trip breakers fail to open

There are several operator actions that appear in the dominant core damage cutsets. These are:

- Operator fails to recognize the need for or fails to perform manual reactor coolant system depressurization by actuating automatic depressurization system using protection and safety monitoring system cues and equipment
- Operator fails to manually actuate the automatic depressurization system using diverse actuation system cues and equipment

These operator actions are important in this sequence because failure of core makeup tank injection prevents automatic depressurization system actuation on low core makeup tank level. Failure of the protection and safety monitoring system-related operator action results in failure of both full and partial depressurization. Further, a failure probability corresponding to a high dependency is assigned to the diverse actuation system-related operator action because it follows the similar protection and safety monitoring system-related action in the sequence.

Sequence 11: Medium Loss-of-Coolant Accident (MLOCA-04)

Sequence Frequency: 2.4E-09/year
Contribution to Core Damage: 1.0 percent
Initiating Event Frequency: 1.6E-04/year
Conditional Core Damage Probability: 1.5E-04

Description of Sequence

A medium loss-of-coolant initiating event occurs (break size equivalent to between 5 and 9 in. diameter). One or more core makeup tanks inject into the reactor coolant system, but the normal residual heat removal system fails. Reactor coolant system depressurization via automatic depressurization system stage 4 valve operation is successful, but both lines of in-containment refueling water storage tank injection fail. Core damage is postulated due to the inability to provide long-term reactor coolant system inventory makeup and core cooling following the failures of normal residual heat removal system and in-containment refueling water storage tank injection. This sequence is assigned to the 3BE plant damage state. In this state, the reactor coolant system is fully depressurized after a loss-of-coolant accident.

Important Modeling Assumptions

Credit is taken in the models for manual actuation of the normal residual heat removal system in injection mode, followed by gravity recirculation, for successful termination of the event. However, in this sequence, normal residual heat removal system fails.

Although operation of the automatic depressurization system is not required to reach the normal residual heat removal system operating pressure for a medium loss-of-coolant accident, automatic depressurization system operation is required to allow in-containment refueling water storage tank injection following normal residual heat removal system failure.

Risk Important Failures

Table 59-13 lists the dominant cutsets for this sequence. The dominant risk-important failure is the common cause failure to open of in-containment refueling water storage tank injection check valves on both lines.

Other significant failure contributors are:

- Normal residual heat removal system isolation motor-operated valves 011, 022, or 023 fail to open
- In-containment refueling water storage tank recirculation motor-operated valves 117B or 118B fail to open, resulting in failure of normal residual heat removal system recirculation

Credit is taken for the proceduralized operator action to actuate the normal residual heat removal system. Credit is also taken for operator action to actuate the core makeup tanks and automatic depressurization system as a backup to automatic actuation. These actions are not risk important in this sequence.

Sequence 12: Reactor Coolant System Leak (RCSLK-04)

Sequence Frequency: 2.3E-09/year
Contribution to Core Damage: 1.0 percent
Initiating Event Frequency: 1.2E-02/year
Conditional Core Damage Probability: 1.9E-07

Description of Sequence

A reactor coolant system leak initiating event is a coolant leak within the capacity of a chemical and volume control system makeup pump. The chemical and volume control system fails, or the operators fail to take action to shut down the plant, eventually leading to a reactor trip due to excessive reactor coolant system inventory loss. From this point on, the event progresses as a small loss-of-coolant accident. Core makeup tank actuation occurs, the reactor coolant pumps are tripped, and at least one core makeup tank injects. Passive residual heat removal operation and full reactor coolant system depressurization via the automatic depressurization system are successful. However, injection via the normal residual heat removal system and in-containment refueling water storage tank injection both fail. Core damage is postulated due to the inability for long-term reactor coolant system inventory makeup and core cooling following in-containment refueling water storage tank and normal residual heat removal system failures. This sequence is assigned to the 3BE plant damage state. In this state, full reactor coolant system depressurization is achieved after a loss-of-coolant accident.

Important Modeling Assumptions

Following a reactor coolant system leak event, if chemical and volume control system operation and manual shutdown are successful, the event is terminated; otherwise a reactor trip and small loss-of-coolant accident plant response are postulated.

Risk Important Failures

The dominant cutsets for this sequence are listed in Table 59-14. The dominant risk important failure is the common cause failure to open of the in-containment refueling water storage tank check valves; this failure renders in-containment refueling water storage tank injection inoperable.

Other significant contributors fail the nonsafety-related chemical and volume control system and normal residual heat removal system. These are failures of electrical equipment or HVAC chillers. They appear as significant primarily as a result of the PRA modeling, whereby chemical and volume control system unavailability models assume that reactor trip has already occurred. However, for the reactor coolant system leak event sequence, the chemical and volume control system is required to prevent a reactor trip. Thus, in the fault tree model, post-reactor trip electrical bus transfer logic makes failures in supporting systems more significant than they would be had the model been set up specifically for this sequence.

Three operator actions appear in the cutsets; none is dominant:

- Operators fail to perform manual shutdown to avoid reactor trip
- Operators fail to actuate normal residual heat removal system
- Operators fail to align the standby chilled water pump (which affects normal residual heat removal system)

Sequence 13: Medium Loss-of-Coolant Accident (MLOCA-05)

Sequence Frequency: 2.3E-09/year
Contribution to Core Damage: 1.0 percent
Initiating Event Frequency: 1.6E-04/year
Conditional Core Damage Probability: 1.4E-05

Description of Sequence

A medium loss-of-coolant accident initiating event occurs (break size equivalent to between 5- and 9-in. diameter). One or both core makeup tanks inject into the reactor coolant system, but the normal residual heat removal system fails. Reactor coolant system depressurization via the automatic depressurization system also fails. Core damage is postulated due to the inability to provide makeup to the reactor coolant system following normal residual heat removal system failure and the inability to provide in-containment refueling water storage tank injection in time as a result of automatic depressurization system failure.

This sequence is assigned to the 3D plant damage state. In this state, the reactor coolant system is partially depressurized after a loss-of-coolant accident. Although automatic depressurization system failed, the break provides depressurization in this case.

Important Modeling Assumptions

- Credit is taken for manual and automatic actuation of the automatic depressurization system.

Risk Important Failures

The dominant cutsets for this sequence are shown in Table 59-15. The dominant risk important failure is the common cause failure of the fourth-stage squib valves to open.

Other significant contributors include:

- Normal residual heat removal system isolation motor-operated valves 011, 022, or 023 fail to open

- In-containment refueling water storage tank recirculation motor-operated valves 117B or 118B fail to open, resulting in failure of normal residual heat removal system recirculation

Credit is taken for the operator to actuate the normal residual heat removal system. Credit is also taken for operator action to actuate the core makeup tanks and automatic depressurization system as a backup to automatic actuation. These actions are not risk important in this sequence.

59.3.2 Component Importances for At-Power Core Damage Frequency

Chapter 33 presents tables of the relative importances of all basic events appearing in the cutsets for the baseline core damage quantification. These tables indicate risk decrease and risk increase. Risk decrease is the factor by which the core damage frequency would decrease if the failure probability for a given basic event is set to 0.0; it is a useful measure of the benefit that might be obtained as a result of improved component maintenance or testing, better procedures, or operator training. Risk increase is the factor by which the core damage frequency would increase if the failure probability for a given basic event is set to 1.0; it is a useful measure of which components or actions would most adversely affect the core damage frequency if actual operating practices resulted in higher failure probabilities than assumed in the PRA.

The risk decrease results (as discussed in detail in Chapter 50) show that no component contributes more than 20 percent to the total core damage frequency, and that only one single component failure (in-containment refueling water storage tank discharge line strainer plugged) contributes more than 10 percent. In general, there are few single component failures with a risk reduction worth greater than 1 percent. The contribution from unscheduled maintenance is also small; there is no scheduled maintenance for safety-related systems at power. These results indicate that there are no components for which an improvement in design, test, or maintenance (i.e., a change resulting in a significant reduction of the component failure rate) would have a significant impact on core damage frequency.

The risk increase results indicate that there are only three components for which guaranteed failure results in a core damage frequency increase of at least 10 times. Other single-component failures (including unavailability due to unscheduled maintenance) have significantly lower risk increase values, corresponding to a factor of six or lower increase in core damage frequency given an assumption of total unreliability for these components.

These results indicate that the AP600 design includes sufficient redundancy and diversity of protection so that single component-related failures do not have a large impact on the core damage frequency results.

59.3.3 System Importances for At-Power Core Damage

System importances for plant core damage frequency from internal initiating events at power are presented in Chapter 50. They are obtained by setting the failure probabilities for the affected system components to 1.0 in the baseline cutsets and recalculating the core damage frequency.

The results of the sensitivity analyses show that the protection and safety monitoring system, the Class 1E dc power system, and the in-containment refueling water storage tank are important in maintaining a low core damage frequency. The risk-important systems are safety-related systems. Thus, the nonsafety-related systems are significantly less important to plant core damage frequency than are the safety-related systems.

59.3.4 System Failure Probabilities for At-Power Core Damage

Some selected system failure probabilities for typical success criteria used in the at-power PRA are listed in Table 59-16. A system may have different failure probabilities based on the success criteria assigned. For a key safety-related system such as the automatic depressurization system, this is especially pronounced; the automatic depressurization system has many success criteria and corresponding failure probabilities that range over a factor of 100. The values in the table are representative of the various cases.

As can be seen from the system unavailabilities listed in Table 59-16, the highest unavailabilities (i.e., 10^{-2} to 10^{-3}, indicating lower reliability) are associated with nonsafety-related systems or functions. The lower unavailabilities (i.e., 10^{-4} to 10^{-6}, indicating higher reliability) are associated with safety-related systems.

59.3.5 Common Cause Failure Importances for At-Power Core Damage

The basic event risk decrease importance results (as presented in Chapter 50) show that common cause failures of hardware associated with the protection and safety monitoring system, common cause failures of in-containment refueling water storage tank gravity injection components, and common cause automatic depressurization system squib valve failures are of potential significance in maintaining the current level of low plant core damage frequency.

The risk increase importances for common cause failures of the following sets of components show that these are also of potential significance to the current low level of core damage frequency from internal events: software common cause failure of all logic cards in the protection and safety monitoring system, plant control system, and diverse actuation system; logic board failures of the protection and safety monitoring system; failures of transmitters used in the protection and safety monitoring system; failures of reactor trip breakers; plugging of containment sump recirculation screens; failures of in-containment refueling water storage tank gravity injection line check valves; plugging of strainers in the in-containment refueling water storage tank; failures of fourth-stage automatic depressurization system explosive (squib) valves; failures of accumulator check valves; and accumulator tank failures.

59.3.6 Human Error Importances for At-Power Core Damage

In the PRA, credit is taken for various tasks to be performed in the control room by the team of trained professionals. Most of these tasks are rule-based, with only a few skill-based tasks relating to immediate shutdown of the reactor following anticipated transient without scram precursors. Although these tasks are usually termed operator actions, the tasks almost always refer to the completion of a well-defined mission by a team of trained operators following procedures. Further, not every individual or group error during a mission necessarily fails the mission, since procedural recovery is built into the emergency procedures. Moreover, a very strong diversity is introduced through monitoring of the emergency procedure status trees by a shift technical advisor, who is not a regular member of the team. These considerations are factored into the PRA evaluation of human errors.

There are thirty-two such operator actions that appear in the dominant core damage cutsets. The actions appear in the cutsets rather than in the sequences since they are modeled within the functional system fault trees to assess their impact at the appropriate logic level. These actions are grouped by their failure probabilities, without regard to the specific tasks involved (i.e., the action descriptions are intentionally omitted from the table) in Table 59-17 to indicate the general range of credit taken for the various actions included in the PRA models. In reviewing this information, which does not imply an importance ranking, it is useful to note the following.

It can reasonably be expected that a team of trained professionals will have an average mission failure probability on the order of 1.0E-03 or less during the performance of a task (i.e., a failure rate of 1 in 1,000 trials), as long as the following conditions are met:

- There has not been a prior related team failure during the progression of the event, or, if there is one, it has been followed by the successful completion of a task (i.e., the team has not previously mis-diagnosed the actions required to mitigate the event)
- The time window available for the task is equal to or greater than the expected time needed to complete the task
- The task is rule-based rather than knowledge-based (i.e., it requires primarily that the operators follow a set of instructions with which they are familiar, rather than requiring primarily cognitive processes)

It can be seen from Table 59-17 that most of the operator actions modeled have been assigned values that are in the range of average to very high failure probabilities. Most of the human error probabilities that appear in the dominant cutsets are within a close range of an average failure probability. The very high failure probability tasks are primarily conditional or dependent failure probabilities that have been assigned by the human reliability analyst to actions that follow a prior failure to perform a related action in the same event sequence. Such dependent probabilities are assigned when multiple related task failures are not separated by intermediate task successes. The lower probability tasks tend to be those requiring actuation of a device after a separately modeled diagnosis task has succeeded.

The risk decrease results for operator actions (discussed in Chapter 50) show that there are only six human actions with importances greater than 1 percent. There are only three actions for which the internal initiating events at-power core damage frequency contribution would decrease by more than 5 percent if it were assumed that the operators always were successful. This indicates that there would be no significant benefit from additional refinement of the actions modeled nor from special emphasis on operator training in these actions (versus other emergency actions).

The risk increase results show that there are only five operator actions with importance greater than 100 percent; i.e., these are the only modeled operator actions whose guaranteed failure would result in a core damage increase greater than the base case core damage frequency.

The most important action in this ranking (operator fails to actuate automatic depressurization system) results in just under one order of magnitude increase in core damage frequency. These results indicate that the plant design is not overly sensitive to failure of operator actions and the core damage models do not take undue credit for operator response.

A sensitivity was performed in which the failure probabilities for the 32 operator actions are set to 0.0 (perfect operator). The resulting core damage frequency is 1.78E-07 per year, or a decrease of 27 percent. This indicates that perfection in human error probabilities is not risk important at the level of plant risk obtained by the base case; there is no significant benefit to be gained by improving operator response beyond the assumptions made in the PRA.

Another sensitivity was performed in which the failure probabilities for the 32 human error probabilities and also for indication failure (protection and safety monitoring system, plant control system or diverse actuation system originated) are set to 1.0 (failure). The result of the sensitivity analysis shows that the core damage frequency increased to 2.78E-05 events per year. The resulting core damage frequency with no credit for operator actions is still low (about one event in 36,000 reactor-years), on the order of core damage frequency for current plants with credit for operators. This means that, in general, operator actions are important in maintaining a very low plant core damage frequency for internal events at power but are not essential to establishing the acceptability of plant risk. The presence of trained operators will help ensure that the very low core damage frequency prediction is valid. This finding demonstrates a significantly lower dependence on human actions than exists for current plants. The AP600 meets the safety goal without human action, whereas current plants typically do not.

59.3.7 Sensitivity Analyses Summary for At-Power Core Damage

Thirty-six importance and sensitivity analyses were performed on the core damage model for internal initiating events at power. These cases and results are discussed in Chapter 50.

The analyses were chosen to address the following issues:

- Importances of individual basic events and their effect on plant core damage frequency
- Importances of safety-related and nonsafety-related systems in maintaining a low plant core damage frequency
- Importances of containment safeguards systems in maintaining a low large release frequency
- Effect of human reliabilities as a group on plant core damage frequency
- Other specific issues such as passive system check valve reliability and diesel generator mission time

The sensitivity analyses results are listed in Table 59-18. They show that:

- If no credit is taken for operator actions, the plant core damage frequency is 2.8E-05 events per year. This compares well with core damage frequencies for existing plants where credit is taken for operator actions.

- The most important systems for core damage prevention are the protection and safety monitoring system, Class 1E dc power, automatic depressurization system, in-containment refueling water storage tank, and accumulators; none of the nonsafety-related systems have high system importance.

- There are no operator actions that would provide a significant risk decrease if they were made to be more reliable. There are only two sets of operator actions that are risk-important (i.e., whose guaranteed failure would result in a large increase in core damage frequency): manual automatic depressurization system actuation and manual reactor trip following an anticipated transient without scram precursor.

- If the reliability of all check valves is assumed to be a factor of 10 worse, the total plant core damage frequency would only increase into the 1E-06 (i.e., very low) range. This shows that the passive safety-related systems that depend on check valve opening perform well, even if pessimistic check valve reliabilities are assumed.

- The plant core damage frequency is not affected by the diesel generator mission time duration. This is due to the AP600 design's passive features, which do not require ac power for operation.

- The common cause failure basic events, particularly those associated with safety-related systems, are important individually, and also as a group for plant core damage frequency. This is expected for a plant with highly redundant safety-related systems, for which individual component random failure contributions are of reduced significance.

59.3.8 Summary of Important Level 1 At-Power Results

Core Damage Contribution from Various Types of Initiating Events

The results of the PRA show that the following AP600 design features provide the ability for plant systems to respond to various initiating events and contribute to a very low core damage frequency.

- The manual feed and bleed operation in current pressurized water reactors is replaced by the automatic depressurization system and core makeup tank/in-containment refueling water storage tank injection. This increases the success probability for bleed and feed and helps reduce core damage contribution from transients with failure of decay heat removal.

- The switchover-to-recirculation operation in current pressurized water reactors is replaced with automatic recirculation of sump water into the reactor coolant system loops by natural circulation.

- The diverse actuation system provides diverse backup for automatic or manual actuation of safety-related systems, increasing the system reliability for the passive residual heat removal, core makeup tank, and automatic depressurization systems.

Among the plant features that contribute to the small core damage frequency are the following:

- The plant design is based on a defense-in-depth concept whereby there are several means (both active and passive) of providing reactor coolant system makeup following a loss-of-coolant accident, at both high and low pressures (i.e., chemical and volume control system pumps, core makeup tanks, accumulators, in-containment refueling water storage tank gravity injection, and normal residual heat removal system). Similarly, there are diverse means of core cooling, including the passive residual heat removal and normal residual heat removal systems.

- The ability to depressurize and establish feed and bleed heat removal via the automatic depressurization system and core makeup tanks without operator action provides an additional reliable means of core cooling and inventory control.

- The diversity and redundancy in the design of the automatic depressurization system provides a highly reliable system for depressurizing to allow injection and core cooling by the various sources of water.

- The design of the reactor coolant pumps eliminates the dependence on component cooling water and accompanying reactor coolant pump seal loss-of-coolant accident core damage contribution, which is typically significant for current plants.

- The design of the safety-related heat removal systems eliminates the dependence on service water and ac power during accidents; such dependencies can be significant contributors to core damage for current plants.

Loss-of-Coolant Events. The at-power core damage results are dominated (roughly 75 percent) by various loss-of-coolant events. More than half of the loss-of-coolant accident contribution is due to the safety injection line break, which is a special initiator, in that its occurrence partially defeats features incorporated into the plant to respond to losses of primary coolant. Even though the safety injection line break core damage frequency dominates the results, its value is very small (one event in 10 million reactor years), with little credit for nonsafety-related systems.

Anticipated Transients Without Scram. Anticipated transients without scram sequences contribute about 21 percent of the at-power core damage frequency, in part due to modeling

simplifications whereby, in the absence of specific modeling and success criteria, it has been assumed that core damage will occur given certain combinations of failures. With additional analysis and modeling detail, it is expected that the anticipated transient without scram core damage frequency could be shown to be lower. However, since the total anticipated transient without scram core damage frequency is on the order of 1 event in 20 million reactor years, additional modeling was not undertaken.

Transients. The contribution of transients to core damage frequency is only about 3 percent of the at-power core damage frequency (total contribution from all transient initiators with reactor trip is less than 1 event in 100 million reactor years). This is the result of the defense-in-depth features of the AP600 design, whereby core cooling following transients is available from main feedwater, startup feedwater, and passive residual heat removal, as well as from feed and bleed, using diverse and redundant sources of makeup (core makeup tanks, accumulators, in-containment refueling water storage tank, normal residual heat removal system) and of depressurization (four stages of automatic depressurization system).

Loss of Offsite Power. The loss of offsite power core damage frequency contribution at power is insignificant. AP600 passive systems provide cooling without any offsite or onsite ac or dc power. In addition, the passive residual heat removal heat exchanger is backed up by bleed and feed cooling using the automatic depressurization system and core makeup tanks or in-containment refueling water storage tank gravity injection, which require only dc power provided by long-term batteries. With onsite power available, startup feedwater provides an additional means of decay heat removal.

Steam Generator Tube Rupture. The steam generator tube rupture event contributes only about 1.5 percent of the at-power core damage frequency. Compared to operating pressurized water reactors this is a very low contribution. Among the reasons for the small steam generator tube rupture core damage contribution are the following:

- The first line of defense is the startup feedwater system and chemical and volume control system
- A reliable safety-related passive residual heat removal system coupled with the core makeup tank subsystem, which provide automatic protection
- A third line of defense using automatic depressurization system and in-containment refueling water storage tank for accident mitigation should the above-mentioned systems fail.

Further, the automatic depressurization system provides a more reliable alternate decay heat removal path through feed and bleed than the high-pressure manual feed and bleed cooling of current operating plants.

Finally, the large capacity of the in-containment refueling water storage tank increases the long-term recovery probability for unisolable steam generator leaks that bypass containment, by preventing depletion of borated water and core damage.

Dependence on Operator Action

The results of the PRA show that the AP600 is significantly less dependent on operator action to reduce plant risk to acceptable levels than are current plants. This was shown through the sensitivity analyses and the operator action contributions from both the risk decrease and risk increase measures. Almost all operator actions credited in this PRA are performed in the control room; there is very little credit for local actions outside the control room. Further, the human actions modeled in the AP600 PRA are generally simpler than those for current plants (e.g., no manual switchover to ECCS recirculation). Thus, the tanks for AP600 operators are easier and less likely to fail. If it were assumed that the operators never perform any actions credited in the PRA, the internal events core damage frequency would still be lower than the result obtained for many current pressurized water reactors including operator actions.

Dominant System/Component Failure Contributors

Contribution to Core Damage Frequency. Component-related contributors to core damage frequency from internal events at power are dominated by common cause failures. There are no single components for which an improvement in design, test, or maintenance (resulting in perfect component performance) would have a large impact on the core damage frequency results.

Dependence on Component Reliability. Most of the component failures with relatively high risk increase worth are common cause failures. This is an indication of the high degree of built-in redundancy and diversity of AP600 safety-related systems, particularly in view of the low baseline core damage frequency. The results demonstrate a well-balanced design, for which diversity eliminates any strong dependence on active valves or on any specific type of valve.

Sensitivity to Numerical Values and Modeling Assumptions. The core damage results are not sensitive to increases in the failure probabilities of basic events: even for the basic event with the highest contribution to core damage, an increase of a factor of 10 in the failure probability increases the core damage frequency by at most a factor of 2.8. With respect to groups of components, it is observed that check valves are important; if the passive system check valve failure probability is increased by a factor of 10, the core damage frequency increases by a factor of 18. This increase is not insignificant, but it does not change the conclusion that the core damage goal of 1E-05 is comfortably met. Finally, the modeling assumptions in system and accident sequence success criteria are bounding (e.g., conservative) whenever a range of conditions are represented by a single selected condition or success criterion. Since the modeling assumptions already represent an upper bound type estimate, there are no significant contributions to core damage due to conditions outside the assumed ranges that are unaccounted for. As an example, the automatic depressurization system success criteria for

loss-of-coolant accident events are selected to cover the worst conditions (e.g., break size, break location) of the range, rather than typical conditions as is done in most PRAs.

Test and Maintenance Unavailability Safety-related systems do not have scheduled test or maintenance during power operation. This eliminates the unavailability due to test or scheduled maintenance of safety-related system components at power.

System Reliability and Defense-in-Depth. The results show that the safety-related systems have demonstrated high reliabilities (e.g., failure probability in the range of 1E-06 to 1E-04), due to the nature of the system designs (namely passive systems, with no test or maintenance requirements during power operation). Moreover, multiple means of success exist for transients and credible loss-of-coolant accident events. This means that a failure of a safety-related system will not lead to core damage, because other diverse systems back up the first one. This defense-in-depth philosophy leads to the low core damage frequency.

59.4 Severe Release Frequency for Internal Initiating Events at Power

59.4.1 Containment Response and Plant Risk Results

The results of the Level 2 (containment response) and Level 3 (plant risk) analyses for the internal initiating events at power demonstrate that the AP600 containment design is robust in its ability to prevent releases following a severe accident and that the risk to the public due to severe accidents for AP600 is very low. The large release frequency (containment failure frequency) of the AP600 can be divided into three types of failures: 1) initially failed containment, in which the integrity of the containment is either failed due to the initiating event or never achieved from the beginning of the accident; 2) containment-failure-induced by high energy severe accident phenomena; or 3) basemat penetration due to unmitigated core-concrete interaction. The total of these failures is the overall large release frequency. The following summarizes important results of the containment event tree quantification with respect to large release frequency and contributions of the different failure types.

- The overall release frequency for AP600 is 1.0E-08 events per year. This is approximately 4.1 percent of the core damage frequency for internal initiating events at power and well below the design goal of 10 percent.

- The impaired containment frequency, which includes containment bypass, containment isolation failure, and excessive containment leakage, is 9.9E-09 events per year. This accounts for about 99 percent of the overall release frequency. This is significant because, for such sequences, containment integrity is compromised either by the nature of the initiating event (e.g., bypass) or by conditions occurring at the outset of the event (e.g., leakage or failure of isolation), rather than as a result of conditions inside containment following core damage. It indicates the robustness of the AP600 containment design.

- The containment failure frequency as a result of severe accident phenomena is 1.6E-10 events per year; this is about 1.6 percent of the overall release frequency or about 0.06 percent of the core damage frequency. Approximately 64 percent of the early containment failure frequency is due to early containment failures in accident class 3C, in which rupture of the reactor vessel is the initiating event and for which no core damage mitigation is modeled. The contribution of early containment failures in accident class 3C is the result of conservative containment modeling assumptions.

- The frequency of containment isolation failure is dominated (71 percent) by accident class 1AC, in which operator failure to isolate the containment following automatic isolation failures is a significant contributor. This indicates the importance of this operator action.

- The frequency of containment basemat failure is 1.3E-10 events per reactor-year. Basemat failure occurs more than 72 hours after the onset of core damage. The frequency accounts for 1.3 percent of the overall large release frequency. The basemat failure frequency is 0.05 percent of the core damage frequency.

The timing of induced containment failure resulting from severe accident phenomena is defined with respect to the time of fission product release from the damaged core. Early containment failure occurs when the containment fails during the core melt and relocation or as a result of phenomena that occur at the time of reactor vessel failure. Intermediate containment failure occurs within 24 hours of core damage and is typically induced by a hydrogen combustion event. Late containment failure occurs more than 24 hours after core damage and is also often induced by hydrogen combustion. The passive nature of the AP600 containment cooling system removes decay heat from the containment regardless of the operation of any systems; therefore, there are no long-term overpressure failures from decay heat steaming.

- The high-pressure melt ejection frequency is 4.4E-11 events per year. This is approximately 0.5 percent of the overall release frequency, approximately 0.02 percent of core damage frequency, and approximately 0.4 percent of the early containment failure frequency. It is conservatively assumed that all high-pressure melt ejection events lead to containment failure, since the frequency of these events is very small. However, AP600 design features and emerging consensus among industry experts on direct containment heating for existing pressurized water reactors affords considerable promise that containment integrity would be maintained.

- The release frequency is not sensitive to high-pressure core damage sequences. If all high-pressure sequences are assumed to result in a release, the release frequency would increase to 1.31E-08 per year, or about 5.4 percent of the core damage frequency. This conditional containment failure probability is less than the 10 percent goal for AP600.

- Intermediate and late containment failures have very little contribution to the large release frequency.

The reactor cavity becomes flooded for all accident sequences in which the in-containment refueling water storage tank drains into the reactor coolant system. In addition, the design includes a special provision to allow manual flooding of the cavity for those sequences in which in-containment refueling water storage tank draining is unsuccessful. This capability to flood the reactor cavity prevents vessel failure and relocation of core debris to the containment. This involves an operator action that is included in the containment event tree. As a result, only about 6 percent of AP600 sequences result in vessel failure. Approximately two-thirds of this is due to accident class 3C, in which vessel failure is the initiating event. Further, the release frequency is not sensitive to vessel failures into a cavity that is not flooded. If all sequences in which cavity flooding fails are assumed to result in a release, the release frequency would increase to 1.48E-08 per year, or about 6 percent of the core damage frequency. This conditional containment failure probability is less than the 10 percent goal for AP600.

Risk to the public from severe accidents for AP600 is significantly lower than that for typical current generation plants.

Importance of Operator Actions to Containment Response and Plant Risk

The containment response modeling includes credit for operator actions to help mitigate a core damage event. These include depressurizing the reactor coolant system if this did not occur prior to core damage, flooding the reactor cavity if this did not occur automatically, and actuating the containment hydrogen control system.

Of these actions, initiating reactor coolant system depressurization is of particular significance to the risk results, since it transforms potentially high-pressure melt ejection scenarios into low-pressure scenarios, in which there is less chance of containment failure. The combined effect of the credit for operator action and automatic depressurization system response is to reduce the frequency of high-pressure melt ejection by about one order of magnitude. The Level 2 decomposition event tree analysis results show that there is typically greater than an hour between the time of core uncovery and the time at which there is a threat to the integrity of the reactor coolant system (i.e., a potential high-pressure melt ejection concern), so this credit is reasonable. This does indicate, however, the importance of this action to plant severe accident management guidelines.

59.4.2 Sensitivity Analyses for Containment Response

Six sensitivity analyses were performed with the plant damage state event tree systems (containment safeguards systems) individually assumed to be unavailable to determine their effect on the severe release frequency.

A summary of the results is given in Table 59-19.

The results show that guaranteed failure of containment isolation would cause an increase in large release frequency to 2.43E-07 per year, because all core damage sequences would go

to release in this case. This indicates the benefit provided by the robust AP600 containment design. The remaining containment systems have relatively small increases. No other single containment safeguards failure results in a significant increase in the total fission product release frequency.

59.5 Core Damage and Severe Release Frequency from Events at Shutdown

59.5.1 Summary of Shutdown Level 1 Results

The low-power and shutdown assessment calculated a core damage frequency of 5.5E-08 events per year. The top six accident sequences contribute 92 percent of the Level 1 shutdown core damage frequency. These dominant sequences result from:

- Failure of normal residual heat removal system due to a loss of component cooling or service water system initiating event during drained condition, which contributes 54.1 percent of the shutdown core damage frequency
- Loss of offsite power (LOOP) initiating event during drained condition, with failure of grid recovery within 1 hour, which contributes 13.6 percent of the shutdown core damage frequency
- Loss of normal residual heat removal system initiating event during drained condition, which contributes 10.4 percent of the shutdown core damage frequency
- Loss of offsite power initiating event during drained condition, with success of grid recovery within 1 hour, which contributes 5.4 percent of the shutdown core damage frequency
- Loss-of-coolant accident initiating event due to inadvertent opening of RNS-V024 during hot/cold shutdown conditions, which contributes 5.0 percent of the shutdown core damage frequency
- Reactor coolant system overdraining event during drainage to mid-loop, which contributes 3.4 percent of the shutdown core damage frequency

The descriptions of the dominant sequences are provided in the following paragraphs.

Loss of Component Cooling or Service Water System Initiating Event during Drained Condition

This sequence is a loss of decay heat removal initiated by failure of the normal residual heat removal system as a result of failure of the component cooling water or service water system during mid-loop/vessel flange operation, which has an estimated duration of 120 hours. Core damage occurs if automatic and manual actuation of the in-containment refueling water

storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to loss of component cooling water system/service water system during drained condition are:

- Hardware failures of both service water pumps or common cause failure of the output logic I/Os from the plant control system
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Offsite Power Initiating Event during Drained Condition (with failure of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel-flange operation, which has an estimated duration of 120 hours. In this sequence, the normal residual heat removal system fails to restart automatically following the initiating event, and the grid is not recovered within 1 hour. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency given loss of offsite power (without grid recovery) during drained condition are:

- Software common cause failure of protection and safety monitoring system/plant control system instrumentation and control logic cards
- Failure of a normal residual heat removal system pump to restart or run
- Failure of a diesel generator to start and run
- Failure of main circuit breaker 100 (or 200) to open
- Failure to recover ac power within 1 hour
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Normal Residual Heat Removal System Initiating Event during Drained Condition

This sequence is a loss of decay heat removal initiated by failure of the normal residual heat removal system during drained conditions. The loss of decay heat removal occurs following failure of the normal residual heat removal system due to normal residual heat removal system hardware faults during mid-loop/vessel-flange operation. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors t core damage frequency due to loss of the normal residual heat removal system during dra condition are:

- Common cause failure of the normal residual heat removal system pumps to run
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valves
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss of Offsite Power Initiating Event during Drained Condition (with success of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel-flange operation. In this sequence, the normal residual heat removal system does not restart automatically following the initiating event, but the grid is recovered within 1 hour; however, manual normal residual heat removal system restart (after grid recovery) fails. Core damage occurs if automatic and manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency given loss of offsite power (with grid recovery) during drained condition are:

- Software common cause failure of protection and safety monitoring system/plant control system instrumentation and control logic cards
- Failure of normal residual heat removal system pumps to run or to restart
- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve
- Common cause failure of the strainers in the in-containment refueling water storage tank

Loss-of-Coolant Accident Initiating Event due to Inadvertent Opening of RNS-V024 during Hot/cold Shutdown Conditions

This sequence is a loss-of-coolant accident initiated by inadvertent opening of RNS-V024 during hot/cold shutdown conditions when the reactor coolant system is filled and pressurized (which has an estimated duration of 220 hours). Following the initiating event, the core makeup tanks are actuated, and the automatic depressurization system actuates. Core damage occurs if the in-containment refueling water storage tank injection check valves do not open automatically.

The major contributors to core damage frequency due to a loss-of-coolant accident through RNS-V024 during hot/cold shutdown conditions are:

- Inadvertent opening of RNS-V024 due to operator error (an initiating event frequency contributor)
- Common cause failure of the in-containment refueling water storage tank injection check valves
- Common cause failure of the strainers in the in-containment refueling water storage tank

Reactor Coolant System Overdraining Event during Drainage to Mid-Loop

This sequence is initiated by reactor coolant system overdraining during drainage to mid-loop conditions. Draining to mid-loop has an estimated duration of 39 hours. Following the initiating event, manual isolation of the normal residual heat removal system fails. Core damage occurs if manual actuation of the in-containment refueling water storage tank injection motor-operated valves and manual actuation of the normal residual heat removal system pump suction motor-operated valve fail.

The major contributors to core damage frequency due to reactor coolant system overdraining initiated during drainage to mid-loop are:

- Common cause failure of the chemical and volume control system air-operated valves to close automatically upon receipt of low hot leg level signals and failure of the operator to stop draining (initiating event frequency contributors)
- Operator fails to isolate the normal residual heat removal system
- Operator fails to open the in-containment refueling water storage tank injection motor-operated valves
- Operator fails to open the normal residual heat removal system pump suction valve

- Common cause failure of the in-containment refueling water storage tank injection motor-operated valves and normal residual heat removal system pump suction valve

- Common cause failure of the strainers in the in-containment refueling water storage tank

The conclusions drawn from the shutdown Level 1 study are as follows:

- The overall shutdown core damage frequency is very small.

- Initiating events during reactor coolant system drained conditions contribute approximately 85 percent of the total shutdown core damage frequency; loss of decay heat removal capability (during drained condition) due to failure of the component cooling water system or service water system has the greatest contribution (54 percent of the shutdown core damage frequency).

- Common cause failures of in-containment refueling water storage tank components contribute approximately 83 percent of the total shutdown core damage frequency; common cause failure of the in-containment refueling water storage tank motor-operated valves contributes approximately 63 percent of the total shutdown core damage frequency. This indicates that maintaining the reliability of the in-containment refueling water storage tank motor-operated valves and strainers is important in maintaining the current level of low core damage frequency at shutdown.

- Human errors are not overly important to shutdown core damage frequency. There is no particular dominant contributor. Sensitivity results show that the shutdown core damage frequency would remain very low even with little credit for operator actions.

  One action, operator failure to recognize the need for reactor coolant system depressurization during hot/cold shutdown conditions, is identified as having a significant risk increase value. This indicates it is important that the operators understand and are appropriately trained for this operator action.

- Individual component failures are not significant contributors to shutdown core damage frequency, and there is no particular dominant contributor. This confirms the at-power conclusion that single independent component failures do not have a large impact on core damage frequency for AP600 and reflects the redundancy and diversity of protection at shutdown as well.

- The in-containment refueling water storage tank provides a significant benefit during shutdown because it serves as a backup to the normal residual heat removal system.

59.5.2 Large Release Frequency for Shutdown and Low-Power Events

The following items summarize the results of the release frequency assessment for shutdown and low-power operation for the AP600:

- The overall shutdown large release frequency for AP600 is 1.4E-08 events per reactor-year. This frequency includes the containment bypass, containment isolation failure, excessive containment leakage, and containment failures/release modes.

- The frequency of compromised containment integrity resulting from the accident initiator is 3.2E-09 events per reactor-year. This impaired containment frequency includes containment bypass, containment isolation failure, and excessive containment leakage. It accounts for 22.5 percent of the overall shutdown large release frequency.

- The frequency of containment failure within 24 hours of core damage is 2.1E-11 events per reactor-year. This insignificantly small frequency includes early and intermediate containment failures. It accounts for 0.15 percent of the overall large release frequency.

- Early containment failure contributes 0.1 percent to the large release frequency.

- Approximately 88 percent of the early containment failure frequency is due to high-pressure melt ejection cases. The frequency of high-pressure melt ejection cases (1.3E-11 events per reactor-year) is less than 0.02 percent of the core damage frequency and contributes less than 0.1 percent of the large release frequency. Given the insignificant fraction of the core damage frequency involved, no further analyses of the associated phenomena have been performed and no decomposition event trees were developed to demonstrate containment integrity for melt ejection phenomena, despite the fact that both AP600 design features and the emerging consensus on direct containment heating for existing pressurized water reactors afford considerable promise that integrity would be maintained. High-pressure melt ejection cases are included with the early containment failure release category CFE-C.

- The frequency of containment failure after 24 hours of core damage due to basemat failure is 1.1E-08 events per reactor-year. Basemat failure occurs more than 72 hours after the onset of core damage. The frequency accounts for 77.4 percent of the overall large release frequency. Late containment failure due to hydrogen combustion is negligible with respect to basemat failure.

- Because many of the water sources to the containment are valved off during shutdown conditions, a significant percentage of the severe accidents at shutdown result in a dry reactor cavity condition in which the debris cannot be cooled. (No credit is taken in the models for actions by the operators outside the control room to re-open valves to these water sources.)

59.5.3 Shutdown Results Summary

The results of the low-power and shutdown assessment show that the AP600 design includes redundancy and diversity at shutdown not found in current plants; in particular, the in-containment refueling water storage tank provides a unique safety backup to the normal residual heat removal system. Maintenance at shutdown has less impact on the defense-in-depth features for AP600 than for current plants; in accordance with plant technical specifications, safety-related system planned maintenance is performed only during those shutdown modes when the protection provided by the safety-related system is not required. Further, maintenance of nonsafety systems, such as the normal residual heat removal system, component cooling water system, and service water system, is performed at power to avoid adversely affecting shutdown risk. These contribute to the extremely low shutdown core damage and large release frequency.

59.6 Core Damage and Severe Release Frequency from External and Other Events

This section will be completed later, after the corresponding analysis is completed.

59.6.1 Results of Internal Flooding Assessment

A scoping internal flooding analysis was performed based on available AP600 detailed design information, with conservative assumptions or engineering judgement used for areas lacking detailed information.

The AP600 design philosophy of minimizing the number of potential flooding sources in safety-related areas, along with the physical separation of redundant safety-related components and systems from each other and from nonsafety-related components, minimizes the consequences of internal flooding. The core damage frequencies from flooding events at power and during shutdown operations are not appreciable contributors to the overall AP600 core damage frequency. The internal flooding-induced core damage frequencies are estimated to be:

- 2.20E-10 events per year for power operations
- 1.54E-09 events per year for shutdown operations

The internal flooding analysis conservatively assumes that flooding of nonsafety-related equipment results in system failure of the affected system. This results in a higher flooding-induced core damage frequency at shutdown than at power, because of the use of the nonsafety-related normal residual heat removal system as the primary means of decay heat removal at shutdown.

The top three at-power flooding scenarios comprise 95 percent of the at-power flooding-induced core damage frequency. The dominant at-power flooding core damage initiators are as follows:

- Loss of feedwater to both steam generators due to rupture of condensate, fire protection or main and startup feedwater piping in the turbine building 135'-3" general area; this initiator contributes 37 percent of the at-power flooding core damage frequency.

- Loss of feedwater to both steam generators due to rupture of condensate, fire protection or main and startup feedwater piping in the turbine building 117'-6" general area; this contributes 33 percent of the at-power flooding core damage frequency.

- Loss of feedwater to both steam generators due to rupture of an expansion joint on the circulating water system in the turbine building 100'-0" general area; this contributes 24 percent of the at-power flooding core damage frequency.

The top two shutdown flooding scenarios comprise 95 percent of the shutdown flooding-induced core damage frequency. The dominant shutdown flooding core damage initiators are as follows:

- Loss of decay heat removal from failure of the component cooling water system or service water system during reactor coolant system drained condition due to a rupture of component cooling water, fire protection, or service water piping in the turbine building general area; this contributes 48 percent of the shutdown flooding core damage frequency.

- Loss of decay heat removal from failure within the normal residual heat removal system during reactor coolant system drained condition due to a rupture of chemical and volume control or fire protection piping in the auxiliary building RCA; this contributes 47 percent of the shutdown flooding core damage frequency.

59.7 Overall Plant Risk Results

The total plant risk expressed in terms of plant core damage frequency and severe release frequency (releases of 25 rem or more at 24 hours at the site boundary) for all events studied in this PRA are summarized in Table 59-20.

The contribution of various events to total plant core damage frequency is shown in Figure 59-2.

The total plant core damage and large release frequency analysis results show the following:

- The total mean core damage frequency is two orders of magnitude smaller than those for existing pressurized water reactors. The cumulative core damage probability for a population of 50 AP600 units operating for 60 years each would be less than 0.001, which is a low probability of occurrence.

- The total plant severe release frequency is another order of magnitude smaller than that of the core damage frequency; that places such a release frequency in the range of incredible events.

- The plant core damage frequency is dominated by at-power events, with shutdown events as the second contributor; internal flooding events are a negligible contributor to core damage frequency.

- The severe release frequency is almost equally shared by at-power and shutdown events. The severe release frequency as a percentage of core damage frequency is 4 percent for at-power events and 25 percent for shutdown events.

- The results show that the design goals of low core damage frequency and low severe release frequency have been met; the AP600 frequencies are lower than the NRC and ALWR goals set for new plant designs, as shown in Table 59-21. These results show the effectiveness of passive systems in mitigating severe accidents and reflect the reduced dependence of AP600 on nonsafety systems and human actions.

The plant risk results for internal events at power and shutdown are summarized in Tables 59-22 through 59-25.

The plant risk results indicate the following:

- 99 percent of the risk is from containment bypass and containment isolation failure initiated sequences. This demonstrates the robustness of the containment since there is little risk from severe accident sequences that fail the containment structure.

- Approximately 75 percent of the risk is from at-power conditions, and 25 percent is from shutdown and low-power conditions.

- There is little increase (<10 percent) in risk following the first 24 hours after core damage. This demonstrates that the containment continues to provide protection beyond the first 24 hours after the accident.

59.8 Plant Features Important to Reducing Risk

Westinghouse used PRA results extensively in the AP600 design process to identify areas for design improvement and areas for further risk reduction. These results were also compared with existing commercial nuclear power plants to identify additional area of risk reduction. Examples of the more significant AP600 plant features and operator actions that reduce risk are discussed in this section. Examples are provided in the area of reactor design, system design, plant structures and layout, and containment design.

AP600 has more lines of defense as compared to current operating plants, which provide more success paths following an initiating event and provide redundancy and diversity to fight common-cause-related concerns. Examples of extensive AP600 lines of defense follow:

- For criticality control:
  - control rod insertion via reactor trip breaker opening
  - control rod insertion via motor-generator set de-energization
  - ride out via turbine trip
- For core heat removal:
  - main feedwater
  - startup feedwater
  - passive residual heat removal
  - automatic depressurization system and feed-and-bleed via normal residual heat removal injection
  - automatic depressurization system and passive feed-and-bleed via in-containment refueling water storage tank injection
- For reactor coolant system makeup:
  - chemical and volume control system
  - core makeup tanks
  - automatic depressurization system and normal residual heat removal
  - automatic depressurization system, accumulators, and in-containment refueling water storage tank injection
  - automatic depressurization system, core makeup tanks, and in-containment refueling water storage tank injection
- For containment cooling:
  - fan coolers
  - normal residual heat removal
  - passive containment cooling system with passive water drain
  - passive containment cooling system with alternate water supply
  - passive containment cooling system without water (air only)
  - fire water

59.8.1 Reactor Design

The AP600 reactor coolant system has many features that reduce the plant risk profile. The pressurizer is larger than those used in comparable current operating plants, resulting in a longer drainage time during small loss-of-coolant accident events. The larger pressurizer increases transient operation margins, resulting in a more reliable plant with fewer reactor trips

and avoiding challenges to the plant and operator during transients. The larger pressurizer also eliminates the need for fast-acting PORVs, which are a possible source of reactor coolant system leaks.

The AP600 core is larger than comparable operating plants, resulting in a lower power density. If, during a potential severe accident, the core were partially uncovered for a short period of time, the likelihood of fuel damage is reduced.

The AP600 steam generators have large secondary-side water inventories, allowing significant time (greater than 1 hour) to recover steam generator feedwater or other means of core heat removal. The AP600 steam generators also employ improved materials and design features that significantly reduce the probability of forced outages or tube rupture.

The AP600 has canned reactor coolant pumps, thus avoiding seal loss-of-coolant accident issues and simplifying the chemical and volume control system. The reactor coolant system has fewer welds, which reduces the potential for loss-of-coolant accident events. The probability of a loss-of-coolant accident is also reduced by the application of "leak-before-break" to reactor coolant system piping larger than 3 in.

59.8.2 Systems Design

System design aspects that are intended to reduce plant risk are discussed in terms of safety-related and nonsafety-related systems.

59.8.2.1 Safety-Related Systems

AP600 uses passive safety-related systems to mitigate design basis accidents and reduce public risk. The passive safety-related systems rely on natural forces such as density differences, gravity, and stored energy to provide water for core and containment cooling. These passive systems do not include active equipment such as pumps. One-time valve alignment of safety-related valves actuates the passive safety-related systems using valve operators such as:

- DC motor-operators with power provided by Class 1E batteries
- Air-operators that reposition to the safeguards position on a loss of the nonsafety-related compressed air that keeps the safety-related equipment in standby
- Squib valves
- Check valves

The passive systems are designed to function with no operator actions for 72 hours following a design basis accident.

Diversity among the passive systems further reduces the overall plant risk. An example of operational diversity is the option to use passive residual heat removal versus feed-and-bleed functions, and an example of equipment diversity is the use of different valve operators (motor, air, squib) to combat common cause failures.

The passive residual heat removal heat exchanger protects the plant against transients that upset the normal steam generator feedwater and steam systems. The passive residual heat removal subsystem of the passive core cooling system contains no pumps and significantly fewer valves than conventional plant auxiliary feedwater systems, thus increasing the reliability of the system by fewer potential equipment failures (pumps and valves) and less maintenance activities.

For reactor coolant system water inventory makeup during loss-of-coolant accident events, the passive core cooling system uses three passive sources of water to maintain core cooling through safety injection: the core makeup tanks, accumulators, and in-containment refueling water storage tank. These sources are directly connected to two nozzles on the reactor vessel so that no injection flow can be spilled for larger break events.

The automatic depressurization system is incorporated into the design for severe accident depressurization of the reactor coolant system. The automatic depressurization system has 10 paths with diverse valves to combat common cause failures and is designed for automatic or manual actuation by the protection and safety monitoring system or manual actuation by the diverse actuation system. The automatic depressurization system can be used in a partial depressurization mode to provide long-term reactor coolant system cooling with normal residual heat removal system injection, or it can be used in full depressurization mode for passive in-containment refueling water storage tank injection for long-term reactor coolant system cooling. In either case, switchover from injection to recirculation is automatic without manual actions.

The safety-related Class 1E dc and UPS system has a large battery capacity to support all frontline passive safety-related systems for 72 hours. This system has four 24-hour batteries, two 72-hour batteries, and a spare battery. The presence of the spare battery improves testability and helps with the detection of common cause failures.

The passive containment cooling system provides the safety-related ultimate heat sink for the plant. Heat is removed from the containment vessel following an accident by a continuous natural circulation flow of air, without any system actuations. By using the passive containment cooling system following a severe accident, the containment stays well below the predicted failure pressure. The steaming and condensing action of the passive containment cooling system enhances activity removal so that a containment spray system (with pumps and valves) is not required.

AP600 containment isolation is significantly improved over that of conventional PWRs due to a large reduction in the number of penetrations; the number of normally open penetrations is reduced, and there are no penetrations required to support post-accident mitigation features.

Containment isolation is improved due to the chemical and volume control system being a closed system, the safety-related passive safety injection components are located inside the containment, and the number of HVAC penetrations are reduced (no maxi purge connection).

Vessel failure potential upon core damage is reduced (in-vessel retention of the damaged core) by providing in-containment refueling water storage tank dump into the reactor cavity.

For events at shutdown, AP600 has passive safety-related systems for all shutdown conditions as a backup to the normal residual heat removal system. This reduces the risk at shutdown through redundancy and diversity.

Post-72-hour connections are incorporated into the passive system design to allow for long-term accident management.

59.8.2.2 Nonsafety-Related Systems

AP600 has nonsafety-related systems capable of mitigating accidents. These systems use redundant pumps, which are powered by offsite and onsite power supplies. AP600 has certain design features in the nonsafety-related systems to reduce plant risk compared to current operating plants. The main feedwater system can automatically adjust flow from 0 to 100 percent power to reduce the number of transients and provide a continuous decay heat removal function even after the reactor trips in most transients. During transient events, the startup feedwater system can act as a backup to the main feedwater system if the latter is unavailable due to the nature of the initiating event or fails during the transient. During loss of ac power events, startup feedwater pumps are powered by the diesel generators and can be used to remove decay heat since main feedwater is not available. The main feedwater and startup feedwater pumps are motor-driven, rather than steam-driven, for better reliability. Main feedwater controls are digital for better reliability; thus, the main feedwater and startup feedwater system design allows less transients and provides additional nonsafety-related means for decay heat removal for transients. This makes the plant response to transients very robust due to the existence of two nonsafety-related systems in addition to the passive safety-related means of removing decay heat.

The nonsafety-related normal residual heat removal system plays a role in decay heat removal in response to power and shutdown events. The normal residual heat removal system has additional isolation valves and is designed to withstand the reactor coolant system pressure to eliminate interfacing systems loss-of-coolant accident concerns that lead to containment bypass. The normal residual heat removal system provides reliable shutdown cooling, incorporating lessons learned from shutdown events. During mid-loop operations, operation procedures require both normal residual heat removal system pumps to be operable for risk reduction.

Component cooling water and service water systems have a very limited role in the plant risk profile because the passive safety-related systems do not require cooling, and the canned-motor reactor coolant pumps do not require seal cooling from the component cooling water.

The nonsafety-related ac power system (onsite and offsite) also has a very limited role in the plant risk profile since the plant safety-related systems do not depend on ac power. This causes the loss of offsite power event to be less important for the AP600 than in current operating plants. The plant has full load rejection capability to minimize the number of reactor trips. The onsite ac power has two nonsafety-related diesel generators. The diesel generator life is improved and the run failure rate is reduced by avoiding fast starts.

The compressed and instrument air system has low risk importance since the safety-related air-operated valves are fail safe if the air system fails and, except for main feedwater, none of the nonsafety-related systems require air to function. This causes the loss of air event to be less important than in current plant PRAs.

59.8.3 Instrumentation and Control Design

Three instrumentation and control systems are modeled in the AP600 PRA: protection and safety monitoring system, plant control system, and diverse actuation system. Both the protection and safety monitoring system and plant control system are microprocessor-based; they can perform more functions with less components and provide better control capability. Four trains of redundancy are provided for the protection and safety monitoring system; 2-out-of-4 bypass testing in the protection and safety monitoring system reduces the potential for spurious trips due to testing and allows for better testing. Auto testing for the protection and safety monitoring system, and diagnostic self-testing for the protection and safety monitoring system and the plant control system, provide higher reliability in these systems. Both the protection and safety monitoring system and the plant control system use fiber optic cables (with fire separation) and multiplexers. Unlike current plants, there is no cable spreading room, thus eliminating a potential fire area with common cause failure of multiple functions. Additional fault tolerance is built into the plant control system so that one failure does not prevent the operation of important functions.

Improvements in the plant control system and the protection and safety monitoring system are coupled with an improved control room and man-machine interfaces; these include improvements in the form and contents of the information provided to control room operators for decision making to limit commission errors (for example, an overview panel for conveying crucial information to the operators, alarm priority, computerized procedures, longer operator action times, integration of NSSS/BOP presentation). In addition, the remote shutdown control is designed to have more functions, similar to the control room, to be performed at the remote shutdown control location, as opposed to operators sending out personnel to local valves.

The diverse actuation system provides a diverse automatic and manual backup function to the protection and safety monitoring system and reduces risk from anticipated transients without scram events. The diverse actuation system also compensates for rare, but consequential potential common cause failures in the protection and safety monitoring system.

59.8.4 Plant Layout

Plant layout is designed to minimize the consequences of fire and flooding by maximizing the separation of electrical and mechanical equipment areas in the non-radiologically controlled area of the auxiliary building. This separation is designed to minimize the potential for propagation of leaks from the piping areas and the mechanical equipment areas to the Class 1E electrical and Class IE instrumentation and control equipment rooms. The potential flooding sources and volumes in areas of the plant that contain safety-related equipment are limited to minimize the consequences of internal flooding.

AP600 is designed to provide better separation between divisions of safety-related equipment. Unlike current plants, there is no safety-related cable spreading room. Safety-related cables, divisions B and D are routed separately from divisions A and C.

59.8.5 Plant Structures

AP600 has design features in the plant structures that reduce risk, especially for area events, such as internal fires and internal flooding, and seismic events. The turbine building is separated from the safety-related areas of other buildings so that a fire or flood event in the turbine building will not affect safety-related systems.

The number of buildings and the building volume housing safety-related equipment is reduced compared to a current plant. The safety-related buildings are on a common basemat to compensate against the effects of a seismic event. The common basemat for the containment and the safety-related auxiliary building includes all safety-related equipment. Such a building is less susceptible to severe seismic events than the typical multiple building/basemats, which also involve an ultimate heat sink interface (ocean, river, lake, cooling tower).

59.8.6 Containment Design

The containment pressure boundary is the final barrier to the release of fission products to the environment. The AP600 containment has designed-in provisions which help to maintain containment integrity in the event of a severe accident. Much research has been performed to investigate severe accident phenomena since the Three Mile Island Unit 2 (TMI-2) accident in 1979, and the lessons learned from TMI-2 and in the research experiments have been incorporated into the URD and the AP600 design.

The overall AP600 design provides significant protection to the public and the environment against the release of radiation by reducing the likelihood of the occurrence of severe accidents. The at-power core damage frequency of 2.4E-7 per reactor-year is less than the URD large release frequency goal of 1.0E-6 per reactor-year. However, the containment systems provide additional protection against the release of fission products in the event of a severe accident such that the conditional probability of a large release for AP600 is less than 0.1.

The at-power large release frequency of the AP600 is 1.0E-8 per reactor year. This low frequency is dominated by containment bypass and containment isolation failure initiated events. The probability of severe accident induced containment failures are approximately 0.01 of the core damage frequency. This distribution of the containment failure frequency demonstrates the robustness of the containment structure with regard to severe accident phenomena.

59.8.6.1 Containment Isolation and Leakage

Failure of the containment isolation system prior to a severe accident will lead to a direct release pathway from the containment volume to the environment. AP600 has approximately 55 percent fewer piping penetrations and a lower percentage of normally open penetrations compared to current generation plants. Normally open penetrations are closed by automatic valves, and diverse actuation is provided for valves on penetrations with significant leakage potential. All isolation valves have control room indication to inform the operator of the current valve position.

Similarly to containment isolation failure, leakage of closed containment isolation valves in excess of technical specifications may result in larger releases to the environment. Valves which historically have the greatest leakage problems have been eliminated, or their number significantly reduced in the design. Large purge valves have been replaced by smaller more reliable valves, and check valves have only been used in mild service where wear and service conditions would not be a challenge to successful operation. Solenoid valves are only used on 3/8 inch lines which would be expected to plug with particulate in severe accident events and are too small to challenge the 25 rem release goal if plugging does not occur.

Equipment and personnel hatches have the capability of being tested individually to ensure a leak-tight seal. Hatch seals can easily be verified on a frequent basis.

Therefore, AP600 provides significant protection against the failure to isolate the containment and against failure of isolation valves to fully close.

59.8.6.2 Containment Bypass

Historically, containment bypass, an accident in which the fission products are released directly to the environment from the reactor coolant system, is the leading contributor to risk in a nuclear power plant. Typically the containment bypass accident class consists of two types of accident sequences: interfacing systems loss-of-coolant-accidents and unisolated steam generator tube ruptures.

An interfacing systems loss-of-coolant-accident is the failure of valves which separate the high pressure reactor coolant system with a lower pressure interfacing system which extends outside the containment pressure boundary. The failure of the valve causes the reactor coolant system to pressurize the interfacing system beyond its ultimate capacity and can result in a loss-of-coolant accident outside the containment. Coolant and emergency cooling water are

lost outside the containment, failing recirculation of cooling water and providing a pathway for the direct release of fission products to the environment. In AP600, systems connected to the reactor coolant system are designed with higher design pressures which reduces the likelihood of a pipe rupture in the event of the failure of the interfacing valves. This results in a very low interfacing systems loss-of-coolant-accident contribution to core damage.

Steam generator tube ruptures release coolant from the reactor coolant system to the secondary system and from there, possibly directly to the environment through the steam generator safety valves. The safety valve may fail to reseat, thereby providing a pathway for the loss of coolant and for the release of fission products to the environment, particularly if the steam generator overfills with water during the accident. The unisolated steam generator tube rupture can be mitigated by reducing the reactor coolant system pressure below the opening pressure of the safety valve, thereby preventing it from opening.

AP600 has multiple and diverse automatically actuated systems to reduce the reactor coolant system pressure and mitigate the steam generator tube rupture. The passive residual heat removal subsystem is actuated on the S-signal and, together with the secondary relief valve, effectively reduces the reactor coolant system pressure to prevent the safety valve from opening. If the passive residual heat removal does not stop the loss of coolant, the automatic depressurization system will actuate and depressurize the system. The secondary relief valve is required to open to prevent the safety valve from opening. However, no operator actions are required to mitigate the accident. Therefore, the likelihood of large release consequential to steam generator tube rupture has been reduced in AP600.

59.8.6.3 Passive Containment Cooling

The passive containment cooling system provides protection to the containment pressure boundary by removing the decay and chemical heat that slowly pressurize the containment. The heat is transferred to the environment through the steel pressure boundary. The heat transfer on the outside of the steel shell is enhanced by an annular flow path which creates a convective air flow across the shell and by the evaporation of water that is directed onto the top of the containment in the event of an accident. The evaporative heat transfer prevents the containment from pressurizing above the design conditions during most severe accidents.

In some postulated multiple-failure accident scenarios, the water flow may be failed, but the heat transfer on the outside of the steel shell is only reduced, not terminated. The heat removal is limited to convection heat transfer to the air flow and radiation to the annulus baffle. With no water film on the containment shell to provide evaporative cooling, the containment pressurizes above the design pressure to remove decay heat, but reaches a long-term equilibrium well below the ultimate pressure of the containment.

Therefore, the passive containment cooling system provides decay heat removal from the containment in both wet and dry heat transfer conditions without reaching pressures which threaten the containment integrity. Long-term overpressure is not considered to be a credible containment failure mode for AP600.

59.8.6.4 High Pressure Core Melt Scenarios

The automatic depressurization system and the passive residual heat removal heat exchanger provide reliable and diverse reactor coolant system depressurization which significantly reduces the likelihood of high pressure core damage. High pressure core damage sequences have the potential to fail steam generator tubes and create a containment bypass release, or to cause severe accident phenomena at the time of vessel failure which may threaten the containment pressure boundary. Reducing the reactor coolant system pressure during a severe accident significantly lowers the likelihood of phenomena which may induce large fission product releases early in the accident sequence.

59.8.6.5 In-Vessel Retention of Molten Core Debris

The AP600 reactor coolant system, reactor vessel and containment configuration have features which enhance the design's ability to maintain molten core debris in the reactor vessel. As it melts, debris relocates to the lower head of the reactor vessel where it heats and stresses the reactor vessel wall causing it to creep to failure. The AP600 automatic depressurization system provides reliable pressure reduction in the reactor coolant system to reduce the stresses on the vessel wall. The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential vessel failure mode. The containment configuration directs water to the reactor cavity and allows the in-containment refueling water storage tank water to be drained into the cavity to submerge the vessel to cool the external surface of the lower head and create buoyancy forces which reduce the stresses on the vessel wall. Cooling the vessel and reducing the stresses prevents the creep rupture failure of the vessel wall. The reactor vessel reflective insulation has been designed with provisions to allow water inside the insulation panel to cool the vessel surface, and with vents to allow steam to exit the insulation without failing the insulation support structures. The insulation does not interfere with the cooling of the external surface of the vessel.

Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Therefore, through the prevention of core debris relocation to the containment, the AP600 design significantly reduces the likelihood of containment failure.

59.8.6.6 Early Containment Failure

The low probability of high pressure core damage sequences and the high likelihood of in-vessel retention of core debris significantly reduces the likelihood of early containment failure for AP600. Severe accident phenomena such as direct containment heating and ex-vessel steam explosions are prevented and cannot threaten the integrity of the containment pressure boundary.

59.8.6.7 Combustible Gases Generation and Burning

In severe accident sequences, high temperature metal oxidation, particularly zirconium, results in the rapid generation of hydrogen and possibly carbon monoxide. The first combustible gas release occurs in the accident sequence during core uncovery when the oxidation of the zircaloy cladding by passing steam generates hydrogen. A second release may occur if the vessel fails and ex-vessel debris degrades the concrete basemat. Steam and carbon dioxide are liberated from the concrete and are reduced to hydrogen and carbon monoxide as they pass through the molten metal in the debris. These gases are highly combustible and in high concentrations in the containment may lead to detonable mixtures. The release rates are much higher than the rates associated with the design basis hydrogen release via radiolysis of water, so the hydrogen recombiners alone are not effective in maintaining the concentration below combustible levels.

AP600 employs a nonsafety-related hydrogen igniter system for severe releases of combustible gases. The igniters are powered from ac busses or from either of the nonsafety-related diesel generators. Multiple glow plugs are located in each compartment. The igniters burn the gases at the lower flammability limit. At this low concentration, the containment pressure increase from the burning is small and the likelihood of detonation is negligible. The igniters are spaced such that the distance between them will not allow the burn to transition from deflagration to detonation. The combustible gases are removed with no threat to the containment integrity.

Although the hydrogen igniter system is powered from ac sources, there is little threat of the failure of the system power in the event that it is required to operate. The igniters are only needed in core damage accidents, and the AP600 is designed to mitigate loss of power events without the sequence evolving into a severe accident. Loss of ac power contributes less than 0.2 percent to the core damage frequency.

The reliability of reactor coolant system depressurization and the small core damage frequency contribution of high pressure accident sequences reduces the threat to the containment from sudden releases of hydrogen from the reactor coolant system. Low pressure release of in-vessel hydrogen enhances the ability of the igniter to maintain the containment atmosphere at the lower flammability limit.

Hydrogen that during a severe accident could be injected from the reactor coolant system into the containment through the spargers in the in-containment refueling water storage tank has the potential to produce a diffusion flame at the in-containment refueling water storage tank vent exit along the steel containment wall. A diffusion flame is produced when a combustible gas plume which is too rich to burn enters an oxygen rich atmosphere and is ignited by a glow plug or a random ignition source. The plume is ignited into a standing flame which lasts as long as there is a fuel source. Via convection and radiation, the flame can heat the wall to high temperatures, increasing the likelihood of creep rupture failure of the containment pressure boundary. However, the time required to creep the containment wall to failure is estimated to be tens of hours, which is approximately one order of magnitude longer than the

duration of the hydrogen release. Therefore, the potential for containment failure from the formation of a diffusion flame at the in-containment refueling water storage tank vents is considered to be very low.

There is little threat to the containment integrity from severe accident hydrogen releases and a low probability of carbon monoxide generation. The igniter system is highly reliable in the event of a severe accident and maintains the hydrogen concentration to the lower flammability limit.

59.8.6.8 Intermediate and Long-Term Containment Failure

Since the passive containment cooling system prevents decay heat pressurization of the containment, intermediate and long-term containment failure can only occur as a result of combustion. Due to the high likelihood of in-vessel retention of core debris, the potential for ex-vessel combustible gas generation from core-concrete interaction is very low. The frequency of intermediate and long-term containment failures is very low given the high reliability of the hydrogen igniters.

The AP600 containment design promotes water draining to the reactor cavity. In the event of a severe accident the cavity can be flooded with in-containment refueling water storage tank water through an operator actuated cavity flooding valve. In the event that the flooding action fails, the coolant and injection water from the core makeup tanks and accumulators will fill the cavity to approximately the top of the lower head hemisphere. The reactor cavity floor is sized to allow sufficient debris spreading to create a coolable debris geometry. If the vessel fails and debris is relocated to the reactor cavity, there is sufficient water available in the containment to quench the sensible heat from the debris and to allow the water to recirculate to maintain debris cooling over the long-term. Additional system failures must be postulated to limit the mass of water in the containment enough to cause debris dry-out and produce core-concrete interaction. Therefore, the likelihood of basemat penetration during a severe accident in AP600 is very low.

59.8.6.9 Fission Product Removal

AP600 relies on the passive, natural removal of aerosol fission products from the containment atmosphere, primarily from gravitational settling, diffusiophoresis and thermophoresis. Since natural deposition is slower than active deposition, the AP600 containment has a low design leak rate to increase the time available for deposition. Natural removal is enhanced by the passive containment cooling system which provides a large, cold surface area for condensation of steam which increases the diffusiophoretic and thermophoretic removal processes. Severe accident offsite doses are below the 25 rem site-boundary limit. Minimal credit for deposition of fission products in the auxiliary building limits the site boundary dose to less than 1 rem to support emergency planning zone elimination.

59.9 PRA Input to the Design Certification Process

The AP600 PRA was used in the design certification process to identify important safety insights and assumptions to support certification requirements such as ITAACs, reliability assurance program (RAP), technical specifications, as well as COL and interface requirements. Design certification areas that are further discussed in this section include:

- Reliability assurance program
- ITAACs
- Technical specifications
- MMI / human factors / emergency response guidelines (ERGs)
- COL action items
- In-service test program.

59.9.1 PRA Input to Reliability Assurance Program

The AP600 reliability assurance program (RAP) identifies those systems, structures, and components (SSC) that should be given priority in maintaining their reliability through surveillance, maintenance, and quality control actions during plant operation. To identify these SSCs, the PRA importance analysis results are used as one of the inputs. The PRA importance and sensitivity analyses identify those systems and components that are important in plant risk in terms of either risk increase (e.g., what happens to plant risk if a system or component, or a train is unavailable), or in terms of risk decrease (e.g., what happens to plant risk if a component or a train is perfectly reliable/available). This ranking of components and systems in such a way provides an input for the reliability assurance program. For more information on the AP600 reliability assurance program, refer to SSAR Section 16.2.

59.9.2 PRA Input to ITAACs

To be provided later.

59.9.3 PRA Input to Tech Specs

To be provided later. For more information on the AP600 technical specifications, refer to SSAR Section 16.1.

59.9.4 PRA Input to MMI / Human Factors / Emergency Response Guidelines

The PRA models include modeling of operator actions in response to severe accident sequences, following ERGs. These actions are all procedurized and most of them are performed in the main control room. The most risk important of these actions refer to manual actuation of systems in the highly unlikely event of automatic actuation failure of systems. The risk important operator actions are discussed in Section 59.3. These operator actions and the main human reliability analysis (HRA) model assumptions behind them are reviewed by human factors engineers for consistency with the as-designed plant, and also for insights that

they may provide to the man-machine interface (MMI) and human factors areas. For more information on the AP600 MMI, refer to SSAR Chapter 18.

In addition, the human reliability analysis models and operator actions modeled in the PRA were reviewed by the engineers writing the ERGs for consistency between the PRA models and the actual ERGs.

To identify AP600-specific critical and risk important operator actions for further evaluation by the human factors engineers, the risk importance of the operator actions is provided from the PRA results. From the PRA results and sensitivity studies, it can be concluded that the AP600 design has no critical operator actions and very few risk important actions. A critical operator action is defined as that action, when assumed to fail, would result in a plant core damage frequency of greater than 1.0E-04 per year; there are no such operator actions in AP600 PRA. The risk important operator actions are defined in terms of risk increase and risk decrease measures, whenever possible.

59.9.5 PRA Input to COL Action Items

To be provided later.

Table 59-1

INTERNAL INITIATING EVENT CORE DAMAGE FREQUENCY CONTRIBUTION BY INITIATING EVENT

	Core Damage Frequency Contribution	Initiating Event Category	Percent Contribution	Initiating Event Frequency
1	1.0E-07	Safety Injection Line Break	41.2	1.0E-04
2	5.0E-08	ATWS Precursor with no MFW	20.7	[6.1E-01](*)
3	3.0E-08	Intermediate LOCA	12.5	7.7E-04
4	2.6E-08	Large LOCA	10.6	1.1E-04
5	1.0E-08	Reactor Vessel Rupture	4.1	1.0E-08
6	5.0E-09	Medium LOCA	2.0	1.6E-04
7	3.6E-09	Steam Generator Tube Rupture	1.5	5.2E-03
8	2.9E-09	RCS Leak	1.2	1.2E-02
9	2.1E-09	Small LOCA	0.9	1.0E-04
10	2.0E-09	ATWS Precursor with SI Signal	0.8	[2.1E-02](*)
11	1.9E-09	PRHR Tube Rupture	0.8	5.0E-04
12	1.8E-09	Core Power Excursion	0.7	4.5E-03
13	1.7E-09	Loss of Main Feedwater	0.7	3.4E-01
14	1.7E-09	Transient with MFW	0.7	1.4E+00
15	1.5E-09	CMT Line Break	0.6	8.9E-05
16	6.1E-10	Loss of Offsite Power	0.2	1.2E-01
17	3.2E-10	Loss of Condenser	0.1	1.1E-01
18	2.8E-10	Loss of MFW to One Steam Generator	0.1	1.9E-01
19	2.2E-10	Main Steam Line Stuck Open Safety Valve	0.1	1.2E-03
20	1.9E-10	Loss of Component Cooling Water/Service Water	0.1	1.6E-01
21	1.2E-10	Interfacing Systems LOCA	0.1	1.2E-10
22	8.0E-11	ATWS Precursor with MFW Available	0.0	[1.2E+00](*)
23	7.8E-11	Loss of Compressed Air	0.0	3.6E-02
24	5.2E-11	Steam Line Break Upstream of MSIV	0.0	3.7E-04
25	1.8E-11	Loss of RCS Flow	0.0	1.8E-02
26	4.2E-12	Steam Line Break Downstream of MSIV	0.0	6.0E-04
	2.4E-07	TOTALS	100.0	2.4(*)

(*)= Note that the ATWS precursor frequencies are not included in the total initiating event frequency, since they are already accounted for in other categories.

Table 59-2 (Sheet 1 of 2)

INTERNAL INITIATING EVENTS AT POWER DOMINANT CORE DAMAGE SEQUENCES

No.	Sequence Frequency	Percent Contrib.	Sequence Description
1	8.36E-08	34.36	Safety injection line break initiating event occurs Success of one of one CMT Success of full ADS depressurization Failure of one of one IRWST injection line
2	2.97E-08	12.18	ATWS precursor with no MFW initiating event occurs Failure of reactor trip due to PMS faults Failure of DAS Reactor fails to trip
3	1.99E-08	8.17	ATWS precursor with no MFW event sequence continues Success of startup feedwater or PRHR system Failure of manual rod insertion Failure of primary depress. due to PRZR SV or UET
4	1.72E-08	7.07	Large LOCA initiating event occurs Success of one or two accumulators Failure of two IRWST injection lines
5	1.59E-08	6.53	Safety injection line break initiating event occurs Success of one of one CMT Failure of full ADS depressurization
6	1.17E-08	4.79	Intermediate LOCA initiating event occurs Success of reactor coolant pumps to trip Success of one or two CMTs Success of full ADS depressurization Failure of RNS in injection mode Failure of two IRWST injection lines
7	1.08E-08	4.43	Intermediate LOCA initiating event occurs Success of reactor coolant pumps to trip Success of one or two CMTs Failure of full ADS depressurization Success of partial ADS depressurization Failure of RNS in injection mode
8	1.00E-08	4.11	Reactor vessel rupture initiating event occurs
9	7.32E-09	3.01	Large LOCA initiating event occurs Failure of two accumulators
10	5.77E-09	2.37	Intermediate LOCA initiating event occurs Failure of reactor coolant pumps to trip Failure of full ADS depressurization Failure of partial ADS depressurization

Table 59-2 (Sheet 2 of 2)

INTERNAL INITIATING EVENTS AT POWER
DOMINANT CORE DAMAGE SEQUENCES

No.	Sequence Frequency	Percent Contrib.	Sequence Description
11	2.44E-09	1.00	Medium LOCA initiating event occurs Success of one or two CMTs Failure of RNS in injection mode Success of full ADS depressurization Failure of two IRWST injection lines
12	2.32E-09	.95	RCS leakage event sequence leads to small LOCA event Success of one or two CMTs Success of reactor coolant pumps to trip Success of PRHR Success of full ADS depressurization Failure of RNS in injection mode Failure of two IRWST injection lines
13	2.32E-09	.95	Medium LOCA initiating event occurs Success of one or two CMTs Failure of RNS in injection mode Failure of full ADS depressurization

Table 59-3

SEQUENCE 1 - SAFETY INJECTION LINE BREAK DOMINANT CUTSETS (SI-LB-02)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	2.62E-08	31.31	SAFETY INJECTION LINE BREAK CCF OF GRAVITY INJECTION CVs IN 1/1 LINE TO OPEN
2	2.52E-08	30.11	SAFETY INJECTION LINE BREAK IRWST DISCHARGE LINE 'A' STRAINER PLUGGED
3	8.06E-09	9.63	SAFETY INJECTION LINE BREAK CHECK VALVE 123A FAILS TO OPEN CHECK VALVE 125A FAILS TO OPEN
4	8.06E-09	9.63	SAFETY INJECTION LINE BREAK CHECK VALVE 123A FAILS TO OPEN CHECK VALVE 124A FAILS TO OPEN
5	8.06E-09	9.63	SAFETY INJECTION LINE BREAK CHECK VALVE 122A FAILS TO OPEN CHECK VALVE 125A FAILS TO OPEN
6	8.06E-09	9.63	SAFETY INJECTION LINE BREAK CHECK VALVE 122A FAILS TO OPEN CHECK VALVE 124A FAILS TO OPEN

Table 59-4

SEQUENCE 2 - ATWS DOMINANT CUTSETS (ATWS-1-07)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.33E-08	44.86	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS UNAVAILABILITY GOAL FOR DAS COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
2	6.91E-09	23.31	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 002 FAILURE COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
3	6.91E-09	23.31	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 001 FAILURE COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
4	7.66E-10	2.58	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS EDS3 EA 1 DISTR. PNL FAILURE OR T&M
5	2.65E-10	.89	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS CCF OF SAFETY PT LT CONTINUOUSLY INTERFACING HIGH PRESUR COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
6	2.65E-10	.89	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS CCF NON-SAFETY TRANSMITTERS INTERFACING SYSTEM PRSS COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
7	2.51E-10	.85	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS UNAVAILABILITY GOAL FOR DAS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE
8	-10	.68	ATWS PRECURSOR WITH NO MFW SOFTWARE CCF OF ALL CARDS OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS UNAVAILABILITY GOAL FOR DAS COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
9	1.31E-10	.44	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 002 FAILURE FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE
10	1.31E-10	.44	ATWS PRECURSOR WITH NO MFW PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 001 FAILURE FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE
11	1.05E-10	.35	ATWS PRECURSOR WITH NO MFW SOFTWARE CCF OF ALL CARDS OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 002 FAILURE COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)
12	1.05E-10	.35	ATWS PRECURSOR WITH NO MFW SOFTWARE CCF OF ALL CARDS OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 001 FAILURE COND. PROB. OF ATW-MAN04 (OPER. FAILS TO TRIP REACTOR)

Table 59-5 (Sheet 1 of 2)

SEQUENCE 3 - ATWS DOMINANT CUTSETS (ATWS-28)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.69E-08	85.05	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW FAILURE OF MGSETS TO OPEN PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)
2	2.13E-09	10.72	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK FAILURE OF MGSETS TO OPEN OPERATOR FAILS TO STEP IN THE CONTROL RODS
3	3.52E-10	1.77	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK UNAVAILABILITY GOAL FOR DAS OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA DAS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)
4	1.85E-10	.93	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 002 FAILURE OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA DAS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)
5	1.85E-10	.93	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 001 FAILURE OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA DAS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)
6	4.26E-11	.21	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK FAILURE OF MGSETS TO OPEN ROD-CTRL-SYS
7	2.16E-11	.11	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW FAILURE OF MGSETS TO OPEN PMS BOARDS HARDWARE CCF OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS ROD-CTRL-SYS

Table 59-5 (Sheet 2 of 2)

SEQUENCE 3 - ATWS DOMINANT CUTSETS (ATWS-28)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
8	1.32E-11	.07	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK EDS3 EA 1 DISTR. PNL FAILURE OR T&M OPERATOR FAILS TO STEP IN THE CONTROL RODS
9	8.65E-12	.04	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW FAILURE OF MGSETS TO OPEN TRANSMITTERS C:F OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA PMS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)
10	4.34E-12	.02	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK UNAVAILABILITY GOAL FOR DAS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE OPERATOR FAILS TO STEP IN THE CONTROL RODS
11	2.27E-12	.01	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 002 FAILURE FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE OPERATOR FAILS TO STEP IN THE CONTROL RODS
12	2.27E-12	.01	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK TURBINE IMPULSE CHAMBER PRESSURE TRANSMITTER 001 FAILURE FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE OPERATOR FAILS TO STEP IN THE CONTROL RODS
13	1.85E-12	.01	FAILURE OF PRIMARY DEPRESS. DUE TO PRZR SV OR UET ATWS PRECURSOR WITH NO MFW OTH-RTBREAK INSTRUMENT LINE PLUGGED (SG A) INSTRUMENT LINE PLUGGED (SG B) OPERATOR FAILS TO MANUALLY TRIP REACTOR VIA DAS COND. PROB. OF ATW-MAN01 (OPER. FAILS TO STEP-IN CONTROL RODS)

Table 59-6

SEQUENCE 4 - LARGE LOCA DOMINANT CUTSETS (LLOCA-03)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.59E-08	92.44	LARGE LOCA CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
2	1.27E-09	7.38	LARGE LOCA CCF OF STRAINERS IN IRWST TANK
3	6.11E-12	.04	LARGE LOCA IRWST DISCHARGE LINE 'A' STRAINER PLUGGED IRWST DISCHARGE LINE 'B' STRAINER PLUGGED
4	1.95E-12	.01	LARGE LOCA IRWST DISCHARGE LINE 'A' STRAINER PLUGGED CHECK VALVE 123B FAILS TO OPEN CHECK VALVE 125B FAILS TO OPEN
5	1.95E-12	.01	LARGE LOCA IRWST DISCHARGE LINE 'A' STRAINER PLUGGED CHECK VALVE 123B FAILS TO OPEN CHECK VALVE 124B FAILS TO OPEN
6	1.95E-12	.01	LARGE LOCA IRWST DISCHARGE LINE 'A' STRAINER PLUGGED CHECK VALVE 122B FAILS TO OPEN CHECK VALVE 125B FAILS TO OPEN
7	1.95E-12	.01	LARGE LOCA IRWST DISCHARGE LINE 'A' STRAINER PLUGGED CHECK VALVE 122B FAILS TO OPEN CHECK VALVE 124B FAILS TO OPEN
8	1.95E-12	.01	LARGE LOCA CHECK VALVE 123A FAILS TO OPEN CHECK VALVE 125A FAILS TO OPEN IRWST DISCHARGE LINE 'B' STRAINER PLUGGED
9	1.95E-12	.01	LARGE LOCA CHECK VALVE 123A FAILS TO OPEN CHECK VALVE 124A FAILS TO OPEN IRWST DISCHARGE LINE 'B' STRAINER PLUGGED
10	1.95E-12	.01	LARGE LOCA CHECK VALVE 122A FAILS TO OPEN CHECK VALVE 125A FAILS TO OPEN IRWST DISCHARGE LINE 'B' STRAINER PLUGGED
11	1.95E-12	.01	LARGE LOCA CHECK VALVE 122A FAILS TO OPEN CHECK VALVE 124A FAILS TO OPEN IRWST DISCHARGE LINE 'B' STRAINER PLUGGED

Table 59-7 (Sheet 1 of 2)

SEQUENCE 5 - SAFETY INJECTION LINE BREAK DOMINANT CUTSETS (SI-LB-03)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.58E-08	99.68	SAFETY INJECTION LINE BREAK DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
2	3.56E-11	.22	SAFETY INJECTION LINE BREAK COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CCX-INPUT-LOGIC OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
3	1.33E-11	.08	SAFETY INJECTION LINE BREAK COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CMX-VS-FA OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
4	1.05E-11	.07	SAFETY INJECTION LINE BREAK FAILURE OF MANUAL DAS ACTUATION CCF OF EPO BOARDS IN PMS
5	9.05E-12	.06	SAFETY INJECTION LINE BREAK FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE CCF OF EPO BOARDS IN PMS
6	3.80E-12	.02	SAFETY INJECTION LINE BREAK COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CCX-IN-LOGIC-SW OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
7	2.84E-12	.02	SAFETY INJECTION LINE BREAK HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 3 HARDWARE FAILURE OF ST. #4 LINE 4
8	2.84E-12	.02	SAFETY INJECTION LINE BREAK HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 4

Table 59-7 (Sheet 2 of 2)

SEQUENCE 5 - SAFETY INJECTION LINE BREAK DOMINANT CUTSETS (SI-LB-03)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
9	2.84E-12	.02	SAFETY INJECTION LINE BREAK HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 3 HARDWARE FAILURE OF ST. #4 LINE 4
10	2.84E-12	.02	SAFETY INJECTION LINE BREAK HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 3
11	2.70E-12	.02	SAFETY INJECTION LINE BREAK COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CCX-INPUT-LOGIC OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS
12	1.46E-12	.01	SAFETY INJECTION LINE BREAK SOFTWARE CCF OF ALL CARDS FAILURE OF MANUAL DAS ACTUATION
13	1.26E-12	.01	SAFETY INJECTION LINE BREAK SOFTWARE CCF OF ALL CARDS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE
14	1.01E-12	.01	SAFETY INJECTION LINE BREAK COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CMX-VS-FA OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS
15	8.10E-13	.01	SAFETY INJECTION LINE BREAK CMX-VS-FA CCF OF SAFETY PT LT CONTINUOUSLY INTERFACING HIGH PRESSURE
16	7.03E-13	.00	SAFETY INJECTION LINE BREAK FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE CCX-INPUT-LOGIC OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA

Table 59-8

SEQUENCE 6 - INTERMEDIATE LOCA DOMINANT CUTSETS (NLOCA-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.63E-09	14.00	INTERMEDIATE LOCA HARDWARE FAILURE OF ISOLATION MOV 011 CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
2	1.63E-09	14.00	INTERMEDIATE LOCA HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
3	1.63E-09	14.00	INTERMEDIATE LOCA HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
4	1.38E-09	11.86	INTERMEDIATE LOCA HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
5	1.38E-09	11.86	INTERMEDIATE LOCA HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
6	6.03E-10	5.18	INTERMEDIATE LOCA FAILURE OF AIR COMPRESSOR TRANSMITTER CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
7	3.35E-10	2.88	INTERMEDIATE LOCA OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
8	3.11E-10	2.67	INTERMEDIATE LOCA UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
9	3.11E-10	2.67	INTERMEDIATE LOCA BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
10	2.02E-10	1.74	INTERMEDIATE LOCA CHECK VALVE V013 FAILURE TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
11	1.33E-10	1.14	INTERMEDIATE LOCA PUMP 01A FAILS & ST CK V007A & CB FTC & RE FTC & CB ECS122 SPO PUMP 01B FAILS & ST CK V007B & CB FTC & RE FTC & CB ECS221 SPO CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
12	1.30E-10	1.12	INTERMEDIATE LOCA HARDWARE FAILURE OF ISOLATION MOV 011 CCF OF STRAINERS IN IRWST
13	1.30E-10	1.12	INTERMEDIATE LOCA HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC CCF OF STRAINERS IN IRWST
14	1.30E-10	1.12	INTERMEDIATE LOCA HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC CCF OF STRAINERS IN IRWST
15	1.11E-10	.95	INTERMEDIATE LOCA HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN CCF OF STRAINERS IN IRWST
16	1.11E-10	.95	INTERMEDIATE LOCA HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN CCF OF STRAINERS IN IRWST
17	8.88E-11	.76	INTERMEDIATE LOCA CCF TO START OF THE PUMPS CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN

Table 59-9

SEQUENCE 7 - INTERMEDIATE LOCA DOMINANT CUTSETS (NLOCA-06)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.63E-09	15.12	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILURE OF ISOLATION MOV 011
2	1.63E-09	15.12	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC
3	1.63E-09	15.12	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC
4	1.38E-09	12.80	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN
5	1.38E-09	12.80	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN
6	6.03E-10	5.59	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE FAILURE OF AIR COMPRESSOR TRANSMITTER
7	3.35E-10	3.11	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS
8	3.11E-10	2.88	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE
9	3.11E-10	2.88	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE
10	2.02E-10	1.87	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CHECK VALVE V013 FAILURE TO OPEN
11	1.33E-10	1.23	INTERMEDIATE LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE PUMP 01A FAILS & ST CK V007A & CB FTC & RE FTC & CB ECS122 SPO PUMP 01B FAILS & ST CK V007B & CB FTC & RE FTC & CB ECS221 SPO
12	8.88E-11	.82	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CCF TO START OF THE PUMPS
13	7.04E-11	.65	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CCF TO OPEN OF THE STOP CHECK VALVES
14	6.95E-11	.64	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE MAIN GEN. BKR ES 01 FAILS TO OPEN (# 12)
15	3.66E-11	.34	INTERMEDIATE LOCA DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE 125 VDC PANEL EDS2 DS 11 COMPONENT FAILURES

Table 59-10

SEQUENCE 8 - REACTOR VESSEL RUPTURE CUTSET

This event is modeled to go to core damage following the initiating event. No other cutsets exist.

Table 59-11 (Sheet 1 of 2)

SEQUENCE 9 - LARGE LOCA DOMINANT CUTSETS (LLOCA-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	5.41E-09	73.95	LARGE LOCA COMMON CAUSE FAILURE OF 2 ACCUMULATOR CHECK VALVES
2	3.25E-10	4.44	LARGE LOCA CHECK VALVE 029B FAILS TO OPEN CHECK VALVE 029A FAILS TO OPEN
3	3.25E-10	4.44	LARGE LOCA CHECK VALVE 029B FAILS TO OPEN CHECK VALVE 028A FAILS TO OPEN
4	3.25E-10	4.44	LARGE LOCA CHECK VALVE 028B FAILS TO OPEN CHECK VALVE 029A FAILS TO OPEN
5	3.25E-10	4.44	LARGE LOCA CHECK VALVE 028B FAILS TO OPEN CHECK VALVE 028A FAILS TO OPEN
6	1.35E-10	1.85	LARGE LOCA FLOW TUNING ORIFICE PLUGS CHECK VALVE 029A FAILS TO OPEN
7	1.35E-10	1.85	LARGE LOCA FLOW TUNING ORIFICE PLUGS CHECK VALVE 028A FAILS TO OPEN
8	1.35E-10	1.85	LARGE LOCA CHECK VALVE 029B FAILS TO OPEN FLOW TUNING ORIFICE PLUGS
9	1.35E-10	1.85	LARGE LOCA CHECK VALVE 028B FAILS TO OPEN FLOW TUNING ORIFICE PLUGS
10	5.60E-11	.77	LARGE LOCA FLOW TUNING ORIFICE PLUGS FLOW TUNING ORIFICE PLUGS
11	1.27E-11	17	LARGE LOCA COMMON CAUSE FAILURE OF ACCUMULATOR TANKS
12	4.45E-13	.01	LARGE LOCA ACCUMULATOR TANK B (T001B) RUPTURES CHECK VALVE 029A FAILS TO OPEN

Table 59-11 (Sheet 2 of 2)

SEQUENCE 9 - LARGE LOCA DOMINANT CUTSETS (LLOCA-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
13	4.45E-1.	.01	LARGE LOCA ACCUMULATOR TANK B (T001B) RUPTURES CHECK VALVE 028A FAILS TO OPEN
14	4.45E-13	.01	LARGE LOCA CHECK VALVE 029B FAILS TO OPEN ACCUMULATOR TANK A (T001A) RUPTURES
15	4.45E-13	.01	LARGE LOCA CHECK VALVE 028B FAILS TO OPEN ACCUMULATOR TANK A (T001A) RUPTURES
16	1.85E-13	.00	LARGE LOCA ACCUMULATOR TANK B (T001B) RUPTURES FLOW TUNING ORIFICE PLUGS
17	1.85E-13	.00	LARGE LOCA FLOW TUNING ORIFICE PLUGS ACCUMULATOR TANK A (T001A) RUPTURES
18	1.34E-13	.00	LARGE LOCA FLOW TUNING ORIFICE RUPTURE CHECK VALVE 029A FAILS TO OPEN
19	1.34E-13	.00	LARGE LOCA FLOW TUNING ORIFICE RUPTURE CHECK VALVE 028A FAILS TO OPEN
20	1.34E-13	.00	LARGE LOCA CHECK VALVE 029B FAILS TO OPEN FLOW TUNING ORIFICE RUPTURE
21	1.34E-13	.00	LARGE LOCA CHECK VALVE 028B FAILS TO OPEN FLOW TUNING ORIFICE RUPTURE
22	5.55E-14	.00	LARGE LOCA FLOW TUNING ORIFICE RUPTURE FLOW TUNING ORIFICE PLUGS
23	5.55E-14	.00	LARGE LOCA FLOW TUNING ORIFICE PLUGS FLOW TUNING ORIFICE RUPTURE

Table 59-12 (Sheet 1 of 2)

SEQUENCE 10 - INTERMEDIATE LOCA DOMINANT CUTSETS (NLOCA-16)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	3.04E-09	52.58	INTERMEDIATE LOCA COMMON CAUSE FAILURE TO OPEN OF 4.16 KVAC CIRCUIT BREAKERS COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
2	3.83E-10	6.62	INTERMEDIATE LOCA PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
3	3.83E-10	6.62	INTERMEDIATE LOCA PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
4	3.83E-10	6.62	INTERMEDIATE LOCA PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
5	3.83E-10	6.62	INTERMEDIATE LOCA PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
6	2.96E-10	5.12	INTERMEDIATE LOCA CCX-TT-UF COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
7	2.30E-10	3.98	INTERMEDIATE LOCA COMMON CAUSE FAILURE TO OPEN OF 4.16 KVAC CIRCUIT BREAKERS COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPERATOR FAILS TO PULFIL MANUAL ACTUATION OF ADS
8	6.00E-11	1.04	INTERMEDIATE LOCA COMMON CAUSE FAILURE TO OPEN OF 4.16 KVAC CIRCUIT BREAKERS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA
9	2.90E-11	.50	INTERMEDIATE LOCA PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPERATOR FAILS TO PULFIL MANUAL ACTUATION OF ADS

Table 59-12 (Sheet 2 of 2)

SEQUENCE 10 - INTERMEDIATE LOCA DOMINANT CUTSETS (NLOCA-16)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
10	2.90E-11	.50	INTERMEDIATE LOCA PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS
11	2.90E-11	.50	INTERMEDIATE LOCA PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS
12	2.90E-11	.50	INTERMEDIATE LOCA PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN PUMP A FAILS TO TRIP - BREAKER FAILS TO OPEN COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPERATOR FAILS TO FULFIL MANUAL ACTUATION OF ADS
13	2.73E-11	.47	INTERMEDIATE LOCA PUMP B FAILS TO TRIP - BREAKER FAILS TO OPEN COMPONENTS FAILURE COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA

Table 59-13 (Sheet 1 of 2)

SEQUENCE 11 - MEDIUM LOCA DOMINANT CUTSETS (MLOCA-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	3.41E-10	13.99	MEDIUM LOCA HARDWARE FAILURE OF ISOLATION MOV 011 CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
2	3.41E-10	13.99	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
3	3.41E-10	13.99	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
4	2.90E-10	11.90	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
5	2.90E-10	11.90	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
6	1.26E-10	5.17	MEDIUM LOCA FAILURE OF AIR COMPRESSOR TRANSMITTER CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
7	7.00E-11	2.87	MEDIUM LOCA OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
8	6.52E-11	2.68	MEDIUM LOCA UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
9	6.52E-11	2.68	MEDIUM LOCA BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
10	4.23E-11	1.74	MEDIUM LOCA CHECK VALVE V013 FAILURE TO OPEN CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
11	2.79E-11	1.14	MEDIUM LOCA PUMP 01A FAILS & ST CK V007A & CB FTC & RE FTC & CB ECS122 SPO PUMP 01B FAILS & ST CK V007B & CB FTC & RE FTC & CB ECS221 SPO CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
12	2.72E-11	1.12	MEDIUM LOCA HARDWARE FAILURE OF ISOLATION MOV 011 CCF OF STRAINERS IN IRWST TANK
13	2.72E-11	1.12	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC CCF OF STRAINERS IN IRWST
14	2.72E-11	1.12	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC CCF OF STRAINERS IN IRWST
15	2.32E-11	.95	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN CCF OF STRAINERS IN IRWST
16	2.32E-11	.95	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN CCF OF STRAINERS IN IRWST
17	1.86E-11	.76	MEDIUM LOCA CCF TO START OF THE PUMPS CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN

Table 59-13 (Sheet 2 of 2)

SEQUENCE 11 - MEDIUM LOCA DOMINANT CUTSETS (MLOCA-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
18	1.47E-11	.60	MEDIUM LOCA CCF TO OPEN OF THE STOP CHECK VALVES CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
19	1.46E-11	.60	MEDIUM LOCA STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE MAIN GEN. BKR ES 01 FAILS TO OPEN (#12) CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
20	1.01E-11	.41	MEDIUM LOCA FAILURE OF AIR COMPRESSOR TRANSMITTER CCF OF STRAINERS IN IRWST

Table 59-14 (Sheet 1 of 2)

SEQUENCE 12 - RCS LEAK DOMINANT CUTSETS (RCSLK-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	1.06E-10	4.56	RCS LEAK UNAVAILABILITY OF TRAIN "B" DUE TO MAINTENANCE [2] UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
2	1.06E-10	4.56	RCS LEAK CHILLER MS 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
3	1.06E-10	4.56	RCS LEAK CHILLER MS 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
4	8.89E-11	3.83	RCS LEAK CHILLER PUMP MP 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
5	8.89E-11	3.83	RCS LEAK CHILLER PUMP MP 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
6	6.37E-11	2.74	RCS LEAK MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] BATTERY DB1 UNAVAILABLE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
7	5.44E-11	2.34	RCS LEAK TRAIN "B" HARDWARE FAILURES UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
8	4.99E-11	2.15	RCS LEAK STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
9	4.72E-11	2.03	RCS LEAK CCF TO START OF ENGINE-DRIVEN FUEL PUMPS MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
10	2.83E-11	1.22	RCS LEAK COMMON CAUSE FAILURE 4KV BREAKERS TO OPEN MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
11	2.52E-11	1.08	RCS LEAK DUE TO CCF TO RUN OF THE MOTOR PUMPS CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
12	2.52E-11	1.08	RCS LEAK UNIT COOLER MS07B SEGMENT HARDWARE FAILURE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
13	2.52E-11	1.08	RCS LEAK UNIT COOLER MS07B SEGMENT HARDWARE FAILURE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN

Table 59-14 (Sheet 2 of 2)

SEQUENCE 12 - RCS LEAK DOMINANT CUTSETS (RCSLK-04)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
14	2.51E-11	1.08	RCS LEAK UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE OPER. FAILS TO RECOG. THE NEED & ALIGN STANDBY VWS PUMP CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
15	2.51E-11	1.08	RCS LEAK BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE OPER. FAILS TO RECOG. THE NEED & ALIGN STANDBY VWS PUMP CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN
16	2.38E-11	1.02	RCS LEAK CHILLER MS 03 SEGMENT HARDWARE FAILURE OR MAINTENANCE STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] CCF OF GRAVITY INJECTION CVs IN BOTH LINES TO OPEN

Table 59-15 (Sheet 1 of 2)

SEQUENCE 13 - MEDIUM LOCA DOMINANT CUTSETS (MLOCA-05)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
1	3.41E-10	14.72	MEDIUM LOCA HARDWARE FAILURE OF ISOLATION MOV 011 DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
2	3.41E-10	14.72	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V022 / CB FTC / RELAY FTC DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
3	3.41E-10	14.72	MEDIUM LOCA HARDWARE FAILS TO OPEN MOV V023 / CB FTC / RELAY FTC DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
4	2.90E-10	12.52	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 118B FAILS TO OPEN DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
5	2.90E-10	12.52	MEDIUM LOCA HARDWARE FAILURE CAUSES RECIRC MOV 117B FAILS TO OPEN DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
6	1.26E-10	5.44	MEDIUM LOCA FAILURE OF AIR COMPRESSOR TRANSMITTER DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
7	7.00E-11	3.02	MEDIUM LOCA OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
8	6.52E-11	2.82	MEDIUM LOCA UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
9	6.52E-11	2.82	MEDIUM LOCA BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
10	4.23E-11	1.83	MEDIUM LOCA CHECK VALVE V013 FAILURE TO OPEN DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
11	2.79E-11	1.20	MEDIUM LOCA PUMP 01A FAILS & ST CK V007A & CB FTC & RE FTC & CB ECS122 SPO PUMP 01B FAILS & ST CK V007B & CB FTC & RE FTC & CB ECS221 SPO DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
12	1.86E-11	.80	MEDIUM LOCA CCF TO START OF THE PUMPS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
13	1.61E-11	.70	MEDIUM LOCA CCF OF EPO BOARDS IN PMS FAILURE OF MANUAL DAS ACTUATION
14	1.47E-11	.63	MEDIUM LOCA CCF TO OPEN OF THE STOP CHECK VALVES DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
15	1.46E-11	.63	MEDIUM LOCA STANDBY DG UNAVAILABLE DUE TO TEST AND MAINTENANCE MAIN GEN. BKR ES 01 FAILS TO OPEN [# 12] DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
16	1.39E-11	.60	MEDIUM LOCA CCF OF EPO BOARDS IN PMS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE

Table 59-15 (Sheet 2 of 2)

SEQUENCE 13 - MEDIUM LOCA DOMINANT CUTSETS (MLOCA-05)

NUMBER	CUTSET PROB	PERCENT	BASIC EVENT NAME
17	1.22E-11	.53	MEDIUM LOCA OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS ACT.) CCX-INPUT-LOGIC LPM-MAN04C
18	7.66E-12	.33	MEDIUM LOCA 125 VDC PANEL EDS2 DS 11 COMPONENT FAILURES DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE
19	7.25E-12	.31	MEDIUM LOCA BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE

Table 59-16

TYPICAL SYSTEM FAILURE PROBABILITIES, SHOWING HIGHER RELIABILITIES FOR SAFETY SYSTEMS

	System/Function	Failure Probability	Fault Tree Name	
	CMT Valve Signal	4.2e-07	CMT-IC11	(one train; auto and manual actuation)
	PRHR Valve Signal	9.3e-07	RHR-IC01	(one train; auto and manual actuation)
	ADS	3.3e-06	ADS	(including operator actions)
*	Reactor Trip by PMS	1.2e-05	RTPMS	(including operator actions)
	Accumulators	6.9e-05	AC2AB	
*	Reactor Trip by PMS	8.8e-05	RTPMS	(no credit for operator actions)
	Passive Cont. Cool.	1.0e-04	PCT	
	PRHR	1.0e-04	PRT	
	Core Makeup Tanks	1.1e-04	CM2SL	
	IRWST	1.6e-04	IW2AB	
	125 vdc 1E Bus	3.1e-04	IDADS1	(one bus only)
	DC Bus (Non-1E)	3.6e-04	ED1DS1	(one bus only)
	Containment Isol.	1.4e-03	CIC	
	Hydrogen Control	1.5e-03	VLH	
	Reactor Trip by DAS	1.6e-03	DAS	(including operator action; excluding MGSET failure)
	Chilled Water	1.6e-03	VWH	
	RCP Trip	2.1e-03	RCT	
	4160 vac Bus	4.0e-03	ECES1	(one bus only)
	480 vac Bus	6.7e-03	ECEK11	(one bus only)
	Diesel Generators	1.2e-02	DGEN	
	Startup Feedwater	1.2e-02	SFWT	
	Comp. Cooling Water	1.4e-02	CCT	
	Service Water	1.4e-02	SWT	
	Compressed Air	1.5e-02	CAIR	
	Condenser	3.2e-02	CDS	
	Main Feedwater	3.8e-02	FWT	(including condenser)
	CVS	4.4e-02	CVS	
	RNS	9.0e-02	RNR	

* = For RTPMS, failure probability with and without credit for manual actuation is provided.

Table 59-17

RELATIVE DISTRIBUTION OF HUMAN ERROR PROBABILITIES ILLUSTRATING THE USE OF GENERALLY HIGH FAILURE PROBABILITIES[a]

Identifier	Failure Probability	
ATW-MAN01C	5.2E-01	
ATW-MAN04C	5.3E-01	
LPM-MAN02C	5.0E-01	Very High Failure Probability
LPM-MAN04C	5.0E-01	
REC-MANDASC	5.1E-01	
REG-MAN00	2.0E-01	
ATW-MAN01	3.3E-02	
ATW-MAN03	5.2E-02	
ATW-MAN04	5.2E-02	High Failure Probability
CVN-MAN04	4.0E-02	
REC-MANDAS	1.2E-02	
ATW-MAN05	5.2E-03	
ATW-MAN06	5.2E-03	
ATW-MAN11	1.1E-03	
CIB-MAN00	1.8E-03	
CIB-MAN01	1.3E-03	
CVN-MAN02	1.6E-03	
CVN-MAN03	1.1E-03	
DUMP-MAN01	1.3E-03	
LPM-MAN01	2.2E-03	Average Failure Probabilities
LPM-MAN02	6.5E-03	
LPM-MAN03	2.2E-03	
LPM-MAN04	6.5E-03	
LPM-MAN08	6.5E-03	
REN-MAN02	2.0E-03	
RHN-MAN01	2.9E-03	
VWN-MAN01	5.2E-03	
ZON-MAN01	2.7E-03	
ADN-MAN01	4.9E-04	
HPM-MAN01	5.0E-04	Low Failure Probabilities
PRI-MAN01	5.0E-04	
PRN-MAN03	8.8E-04	
(None)		Very Low Failure Probabilities

[a] The purpose of this table is to show the general range of operator action failure probabilities, rather than to discuss individual action probabilities. There are no very low probabilities and few low probabilities.

Table 59-18 (Sheet 1 of 3)

SUMMARY OF LEVEL 1 AT-POWER IMPORTANCE AND SENSITIVITY ANALYSIS RESULTS

Case Number	Case Description	Results
1	Initiating event importances	Safety injection line break (41%) and ATWS (21%) are major contributors to core damage frequency.
2	Common cause failure importances	Software CCF of all cards, PMS board hardware CCF, PMS transmitters CCF, and reactor trip breakers CCF are significant contributors to risk increase.
3	Human error importances	ADS actuation and manual reactor trip operator actions are significant contributors to risk increase.
4	Component importances	IRWST strainer plugging, EDS3 EA 1 distributor panel failure, IRWST failure, and IRWST check valves are significant contributors to risk increase.
5	No credit taken for ADS in core damage sequences	Core damage frequency increases to 1.26E-03.
6	No credit taken for CMT in core damage sequences	Core damage frequency increases to 9.77E-06.
7	No credit taken for ACC in core damage sequences	Core damage frequency increases to 1.11E-04.
8	No credit taken for IRWST injection in core damage sequences	Core damage frequency increases to 3.54E-04.
9	No credit taken for IRWST recirculation in core damage sequences	Core damage frequency increases to 1.49E-03.
10	No credit taken for PRHR in core damage sequences	Core damage frequency increases to 6.17E-06.
11	No credit taken for PMS in core damage sequences	Core damage frequency increases to 1.23E-02.

Table 59-18 (Sheet 2 of 3)

SUMMARY OF LEVEL 1 AT-POWER IMPORTANCE AND SENSITIVITY ANALYSIS RESULTS

Case Number	Case Description	Results
12	No credit taken for PLS in core damage sequences	Core damage frequency increases to 8.92E-07.
13	No credit taken for DAS in core damage sequences	Core damage frequency increases to 6.81E-06.
14	No credit taken for RNS in core damage sequences	Core damage frequency increases to 6.27E-07.
15	No credit taken for SG overfill protection in core damage sequences	No noticeable impact on core damage frequency.
16	No credit taken for main feedwater in core damage sequences	Core damage frequency increases to 2.53E-07.
17	No credit taken for startup feedwater in core damage sequences	Core damage frequency increases to 2.61E-07.
18	No credit taken for ac power in core damage sequences	Core damage frequency increases to 3.78E-06.
19	No credit taken for diesel generators in core damage sequences	Core damage frequency increases to 3.04E-07.
20	No credit taken for 1E dc power in core damage sequences	Core damage frequency increases to 6.96E-03.
21	No credit taken for non-1E dc power in core damage sequences	Core damage frequency increases to 9.14 E-06.
22	No credit taken for service water system in core damage sequences	Core damage frequency increases to 7.15E-07.
23	No credit taken for component cooling water system in core damage sequences	Core damage frequency increases to 6.88E-07.
24	No credit taken for compressed air system in core damage sequences	Core damage frequency increases to 7.35E-07.

Table 59-18 (Sheet 3 of 3)

SUMMARY OF LEVEL 1 AT-POWER IMPORTANCE AND SENSITIVITY ANALYSIS RESULTS

Case Number	Case Description	Results
25	Set human error probabilities to 1.0 in core damage cutsets (no credit for operators)	Core damage frequency increases to 2.78E-05. Impact is most noticeable for ATW-T, SLB-V, SGTR, and PRSTR initiating events.
26	Set human error probabilities to 0.0 (perfect operator)	Core damage frequency decreases to 1.78E-07.
27	Assess importance of HEPs not showing up in baseline core damage output (sets all HEPs = 0.1)	Core damage frequency increases to 5.36E-07.
28	Increase diesel generator mission time from 2.5 Hours to 24 Hours.	Core damage frequency increases to 2.44E-07.
29	Passive system check valve failure to open probability increased by factor of 10.	Core damage frequency increases to 4.32E-06.
30	Lower cutoff probability for I&C model quantification (changes from 1.0E-10 to 1.0E-11)	No increase in core damage frequency.

Table 59-19

SUMMARY OF SENSITIVITY ANALYSIS RESULTS FOR CONTAINMENT RESPONSE

Case Name	Case Description	Severe Release Frequency at 24 Hours
BASE CASE	Base case severe release frequency	1.01E-08 /year
DP	No credit is taken for "operator depressurizes RCS after core damage"	1.19E-08 /year
IS	No credit is taken for containment isolation	2.43E-07 /year
PC	No credit is taken for passive core cooling system	1.01E-08 /year
IG	No credit is taken for hydrogen control	1.27E-08 /year
IR	No credit is taken for flooding reactor cavity after core damage	1.12E-08 /year
RW	No credit is taken for recirculating water into reactor cavity after core damage	1.02 E-08 /year

Table 59-20

SUMMARY OF AP600 PRA RESULTS

	Core Damage Frequency		Release Frequency	
Internal Events	2.4E-07	5.5E-08	1.0E-08	1.4E-08
Internal Flood	2.2E-10	1.5E-09	N/A	N/A
Internal Fire	(1)	(1)	N/A	N/A
TOTALS	3.0E-07		2.4E-08	
GOALS	1.0E-05		1.0E-06	

Notes:
(1) Fire contribution will be provided later.

N/A = not applicable

Table 59-21

COMPARISON OF AP600 PRA RESULTS TO RISK GOALS

Plant/Goal	Core Damage Frequency	Large Release Frequency	Containment Success Probability
Current PWR [1]	6.7E-05	5.3E-06	92%
ALWR URD Goal [2]	1E-05	1E-06	90%
NRC Safety Goal	1E-04	1E-06	90%
AP600	3.0E-07	2.4E-08	92%

Notes:

(1) Selected IPE result (two-loop Westinghouse PWR - internal at-power events and at-power flooding only). Note that there is no shutdown PRA requirement for currently operating plants.

(2) URD for ALWR passive plant, Revisions 5&6 (all events except seismic and sabotage).

Table 59-22

SITE BOUNDARY DOSE 24-HOUR RISK FROM INTERNAL EVENTS

24-Hour Mean Whole-Body Site Boundary Dose (Effective Dose Equivalent at 0.5-mile Radius)							
Release Category	**At-Power Frequency (per reactor-year)**	**Shutdown Frequency (per reactor-year)**	**Mean Site Boundary Dose (rem)**	**At-Power Risk (rem/reactor-year)**	**Shutdown Risk (rem/reactor-year)**	**Total Plant Risk (rem/reactor-year)**	**% Contrib to Total Risk**
IC	2.4E-07	4.1E-08	8.3E-01	2.0E-07	3.4E-08	2.3E-07	0.12
ICP	1.9E-11	3.8E-12	1.2E+00	2.3E-11	4.6E-12	2.8E-11	<0.01
XL	1.9E-09	4.2E-10	2.5E+01	4.8E-08	1.1E-08	5.9E-08	0.03
BP	5.9E-09	2.1E-09	1.9E+04	1.1E-04	4.0E-05	1.5E-04	79.1
CI	2.1E-09	7.2E-10	1.4E+04	2.9E-05	1.0E-05	3.9E-05	20.6
CI-C	1.4E-11	3.1E-12	3.3E+03	4.6E-08	1.0E-08	5.6E-08	0.03
CFE	9.5E-11	1.8E-12	2.4E+03	2.3E-07	4.3E-09	2.3E-07	0.12
CFE-C	6.0E-11	1.3E-11	9.5E+02	5.7E-08	1.2E-08	6.9E-08	0.04
CFI	3.6E-12	6.0E-12	2.9E+02	1.0E-09	1.7E-09	2.7E-09	<0.01
CFL	6.3E-13	2.4E-13	1.6E+00	1.0E-12	3.8E-13	1.4E-12	<0.01
CFV	1.3E-10	1.1E-08	2.3E+00	3.0E-10	2.5E-08	5.5E-08	<0.01
			Total Risk	1.4E-04	5.0E-05	1.9E-04	100.0

Table 59-23

SITE BOUNDARY DOSE 72-HOUR RISK FROM INTERNAL EVENTS

72-Hour Mean Whole-Body Site Boundary Dose (Effective Dose Equivalent at 0.5-mile Radius)

Release Category	At-Power Frequency (per reactor-year)	Shutdown Frequency (per reactor-year)	Mean Site Boundary Dose (rem)	At-Power Risk (rem/reactor-year)	Shutdown Risk (rem/reactor-year)	Total Plant Risk (rem/reactor-year)	% Contrib to Total Risk
IC	2.4-E07	4.1E-08	9.6E-01	2.3E-07	3.9E-08	2.7E-07	0.13
ICP	1.9E-11	3.8E-12	1.4E+00	2.7E-11	5.3E-12	3.2E-11	<0.01
XL	1.9E-09	4.2E-10	2.9E+01	5.5E-08	1.2E-08	6.7E-08	0.03
BP	5.9E-09	2.1E-09	2.1E+04	1.2E-04	4.4E-05	1.6E-04	78.4
CI	2.1E-09	7.2E-10	1.5E+04	3.2E-05	1.1E-05	4.3E-05	21.1
CI-C	1.4E-11	3.1E-12	4.6E+03	6.4E-08	1.4E-08	7.8E-08	0.04
CFE	9.5E-11	1.8E-12	2.5E+03	2.4E-07	4.5E-09	2.4E-07	0.12
CFE-C	6.0E-11	1.3E-11	1.4E+03	8.4E-08	1.8E-08	1.0E-07	0.05
CFI	3.6E-12	6.0E-12	1.6E+03	5.8E-09	9.6E-09	1.5E-08	<0.01
CFL	6.3E-13	2.4E-13	6.8E+01	4.3E-11	1.6E-11	5.9E-11	<0.01
CFV	1.3E-10	1.1E-08	2.7E+00	5.3E-10	3.0E-08	3.1E-08	0.01
			Total Risk	1.5E-04	5.5E-05	2.0E-04	100.0

Table 59-24

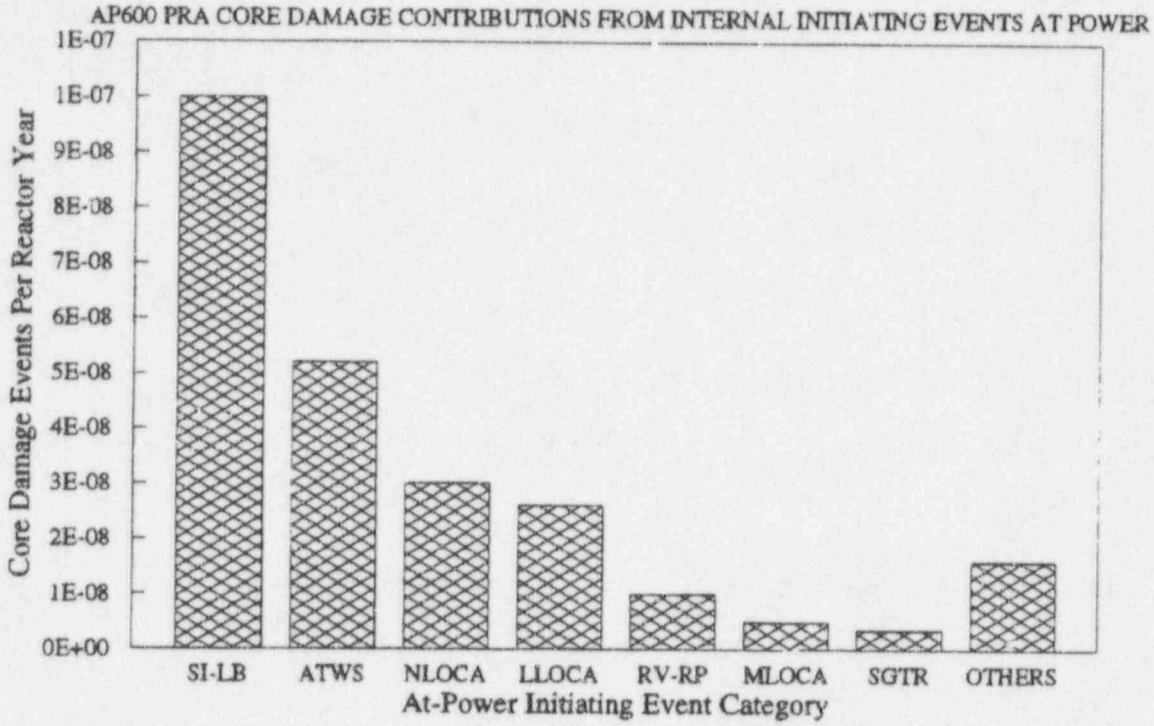
POPULATION DOSE 24-HOUR RISK FROM INTERNAL EVENTS

24-Hour Mean Whole-Body Population Dose (Effective Dose Equivalent to 50-mile Radius)							
Release Category	**At-Power Frequency (per reactor-year)**	**Shutdown Frequency (per reactor-year)**	**Mean Population Dose (person-rem)**	**At-Power Risk (person-rem per reactor-year)**	**Shutdown Risk (person-rem per reactor-year)**	**Total Plant Risk (person-rem per reactor-year)**	**% Contrib to Total Risk**
IC	2.4E-07	4.1E-08	1.6E+02	3.8E-05	6.6E-06	4.5E-05	0.12
ICP	1.9E-11	3.8E-12	2.1E+02	4.0E-09	8.0E-10	4.8E-09	<0.01
XL	1.9E-09	4.2E-10	4.7E+03	8.9E-06	2.0E-06	1.1E-05	0.03
BP	5.9E-09	2.1E-09	3.7E+06	2.2E-02	7.8E-03	3.0E-02	77.7
CI	2.1E-09	7.2E-10	3.0E+06	6.3E-03	2.2E-03	8.5E-03	22.0
CI-C	1.4E-11	3.1E-12	6.3E+05	8.8E-06	2.0E-06	1.1E-05	0.03
CFE	9.5E-11	1.8E-12	5.1E+05	4.8E-05	9.2E-07	4.9E-05	0.13
CFE-C	6.0E-11	1.3E-11	1.5E+05	9.0E-06	2.0E-06	1.1E-05	0.03
CFI	3.6E-12	6.0E-12	5.9E+04	2.1E-07	3.5E-07	5.6E-07	<0.01
CFL	6.3E-13	2.4E-13	1.1E+03	6.9E-10	2.6E-10	9.5E-10	<0.01
CFV	1.3E-10	1.1E-08	4.5E+02	5.9E-08	5.0E-06	5.1E-06	<0.01
			Total Risk	2.8E-02	1.0E-02	3.9E-02	100.0

Table 59-25

POPULATION DOSE 72-HOUR RISK FROM INTERNAL EVENTS

72-Hour Mean Whole-Body Population Dose (Effective Dose Equivalent to 50-mile Radius)							
Release Category	**At-Power Frequency (per reactor-year)**	**Shutdown Frequency (per reactor-year)**	**Mean Population Dose (person-rem)**	**At-Power Risk (person-rem/reactor-year)**	**Shutdown Risk (person-rem/reactor-year)**	**Total Plant Risk (person-rem/reactor-year)**	**% Contrib to Total Risk**
IC	2.4E-07	4.1E-08	1.8E+02	4.3E-05	7.4E-06	5.0E-05	0.12
ICP	1.9E-11	3.8E-12	2.6E+02	4.9E-09	9.9E-10	5.9E-09	<0.01
XL	1.9E-09	4.2E-10	5.4E+03	1.0E-05	2.3E-06	1.2E-05	0.03
BP	5.9E-09	2.1E-09	4.0E+06	2.4E-02	8.4E-03	3.2E-02	76.6
CI	2.1E-09	7.2E-10	3.4E+06	7.1E-03	2.5E-03	9.6E-03	23.0
CI-C	1.4E-11	3.1E-12	9.2E+05	1.3E-05	2.9E-06	1.6E-05	0.04
CFE	9.5E-11	1.8E-12	5.5E+05	5.2E-05	9.9E-07	5.3E-05	0.13
CFE-C	6.0E-11	1.3E-11	2.3E+05	1.4E-05	3.0E-06	1.7E-05	0.04
CFI	3.6E-12	6.0E-12	3.7E+05	1.3E-06	2.2E-06	3.5E-06	<0.01
CFL	6.3E-13	2.4E-13	1.6E+04	1.0E-08	3.8E-09	1.4E-08	<0.01
CFV	1.3E-10	1.1E-08	5.3E+02	6.9E-08	5.9E-06	6.0E-06	0.01
			Total Risk	3.1E-02	1.1E-02	4.2E-02	100.0



Legend:

SI-LB	Safety injection line break
ATWS	Anticipated transients without scram
NLOCA	Intermediate loss of coolant accident
LLOCA	Large loss of coolant accident
RV-RP	Reactor vessel rupture
MLOCA	Medium loss of coolant accident
SGTR	Steam generator tube rupture
OTHERS	All other initiating events at power

Figure 59-1

AP600 PRA Core Damage for Internal Initiating Events at Power

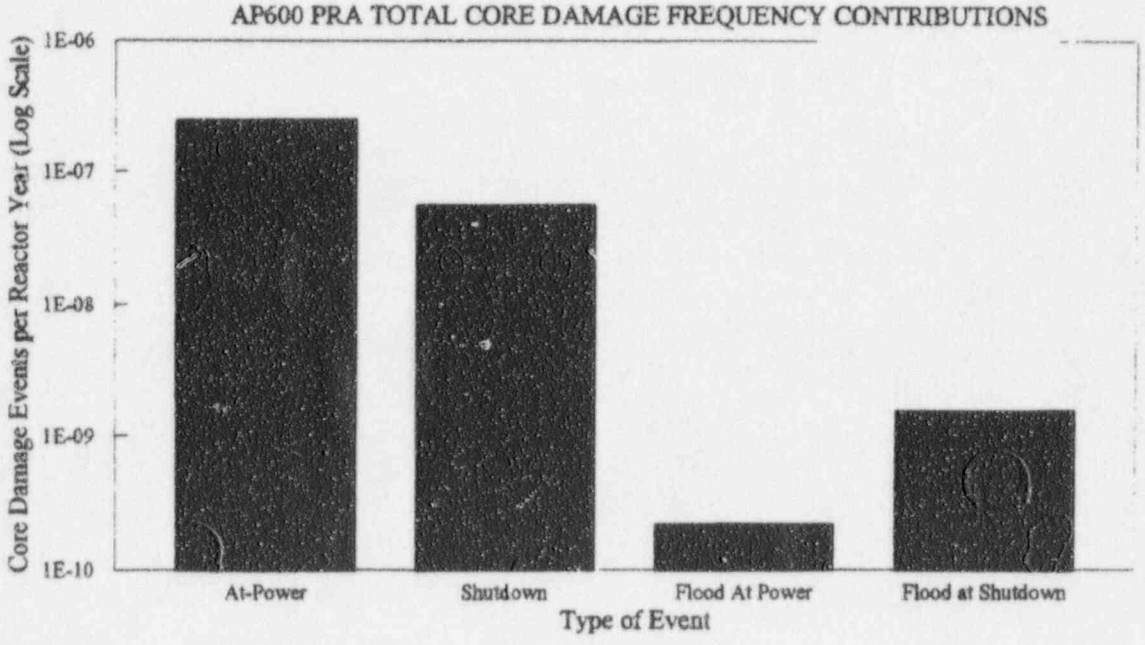


Figure 59-2

AP600 Core Damage Frequency Contributions