Westinghouse Non-Proprietary Class 2

WCAP-14837
Revision 1

AP600 Shutdown Evaluation Report

Westinghouse Energy Systems

Westinghouse Non-Proprietary Class 3

WCAP-14837
Revision 1

AP600 Shutdown Evaluation Report

Westinghouse Energy Systems

AP600 DOCUMENT COVER SHEET

Form 58202G(5/94) [t:\xxxx.wpf:1x]
0058.FRM

AP600 CENTRAL FILE USE ONLY: TDC: ____________ IDS: I ________ S ________

RFS#: RFS ITEM #:

AP600 DOCUMENT NO. GW-GLR-004	REVISION NO. 1	Page 1 of ___	ASSIGNED TO R.K. Nydes

ALTERNATE DOCUMENT NUMBER: WCAP-14837, Rev1 WORK BREAKDOWN #: 3.3.2.19

DESIGN AGENT ORGANIZATION:

TITLE: AP600 Shutdown Evaluation Report

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

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
o:\3497w\3497w.r1 :1b-060697	WordPerfect	

□ 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 R.K. Nydes	SIGNATURE/DATE R.K. Nydes 6/6/97	
AP600 RESPONSIBLE MANAGER J.W. Winters	SIGNATURE*	APPROVAL DATE 6/6/97

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

OK RKN 6/6

AP600 DOCUMENT COVER SHEET

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.

WESTINGHOUSE NON-PROPRIETARY CLASS 3

WCAP-14837, Revision 1

AP600 Shutdown Evaluation Report

AP600 Document Number: GW-GLR-004, Revision 1

E. L. Carlin
M. M. Corletti
K. L. Deutsch
J. L. Grover
G. A. Israelson
R. M. Kemper
R. N. Lewis
R. K. Nydes
S. R. Prokopovich
B. D. Sloane
I. T. Wallace

June 1997

Westinghouse Electric Corporation
Energy Systems Business Unit
P.O. Box 355
Pittsburgh, PA 15230-0355

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (cont.)

LIST OF ACRONYMS

ADS	Automatic Depressurization System
ASME	American Society of Mechanical Engineers
CCS	Component Cooling Water System
CDF	Core Damage Frequency
CLP	Cask Loading Pit
CMT	Core Makeup Tank
CNS	Containment System
COL	Combined Operating License
CVS	Chemical and Volume Control System
CWP	Cask Washdown Pit
DAS	Diverse Actuation System
DBA	Design Basis Accident
DECLG	Double-ended Cold Leg Guillotine
DEDVI	Double-ended Direct Vessel Injection
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DVI	Direct Vessel Injection
ECCS	Emergency Core Cooling System
ERG	Emergency Response Guidelines
ESF	Engineered Safety Feature
FSER	Final Safety Evaluation Report
FTC	Fuel Transfer Canal
FWS	Main and Startup Feedwater System
HFE	Human Factors Engineering
HZP	Hot Zero Power
I&C	Instrumentation and Control
IHST	Integrated Head Storage Stand
IRWST	In-containment Refueling Water Storage Tank
LCO	Limiting Conditions for Operation
LOCA	Loss-of-coolant Accident
LTOP	Low Temperature Overpressure Protection
MFCV	Main Feedwater Control Valve
MFIV	Main Feedwater Isolation Valve
MOV	Motor-operated Valve
MSIV	Main Steam Isolation Valve
MSR	Maximum Steaming Rate
MSS	Main Steam System
MSSV	Main Steam Safety Valve
MTS	Main Turbine System
NFPA	National Fire Prevention Association
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NUREG	Report Designator for NRC Reports
NUMARC	Nuclear Management and Resources Council
OITS	Open Item Tracking System
ORE	Occupational Radiation Exposure

LIST OF ACRONYMS (cont.)

PAMS	Post-accident Monitoring System
PCS	Passive Containment Cooling System
PCT	Peak Cladding Temperature
PIRT	Phenomena Identification Ranking Table
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PORV	Power-operated Relief Valve
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PRHR HX	Passive Residual Heat Removal Heat Exchanger
PSS	Primary Sampling System
PXS	Passive Core Cooling System
PWR	Pressurized Water Reactor
RAI	Request for Additional Information
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System
RTNSS	Regulatory Treatment of Nonsafety Systems
SDER	Shutdown Evaluation Report
SFCV	Startup Feedwater Control Valve
SFIV	Startup Feedwater Isolation Valve
SFS	Spent Fuel Pool Cooling System
SGS	Steam Generator System
SGTR	Steam Generator Tube Rupture
SSAR	Standard Safety Analysis Report
SSC	Systems, Structures, and Components
SSE	Safe Shutdown Earthquake

ABSTRACT

Westinghouse has considered shutdown operations in the engineering of the AP600 nuclear power plant. The AP600 defense-in-depth design philosophy to provide normally operating front-line active systems backed up by passive safety-related systems gives the AP600 a greater degree of safety during normal power operation and improved safety during shutdown operations. This report presents and evaluates the AP600 design features in the context of the specific shutdown issues identified by the Nuclear Regulatory Commission.

1.0 INTRODUCTION

1.1 PURPOSE

The *AP600 Shutdown Evaluation Report* (SDER) presents AP600 design features that address the issues of shutdown risk and shutdown safety. This report further evaluates these design features with respect to their ability to reduce and or mitigate the consequences of events that can occur during shutdown. The SDER provides both design basis evaluations and a probabilistic risk assessment (PRA) for the planr at shutdown.

The SDER provides the Nuclear Regulatory Commission (NRC) with a single-source reference to AP600 design certification issues that address shutdown capabilities. This report includes a roadmap to information previously provided to the NRC and documents any additional information required to resolve shutdown issues related to the AP600 design. The SDER summarizes closure of related *Draft Safety Evaluation Report* (Reference 1-1) open items and responds to request for additional information (RAI) 440.53 (Reference 1-2) by documenting compliance with NUREG-1449 (Reference 1-3).

1.2 SCOPE

The scope of the SDER, as agreed to by the NRC staff, was provided to the NRC in the AP600 SDER Outline (Reference 1-4). Generally, the scope of this report includes discussions of the following:

- Systems designed to operate during shutdown
- Shutdown operations -- including maintenance insights, risk management, and Emergency Response Guidelines (ERGs) (Reference 1-5)
- Safety analyses and evaluations for shutdown operations
- *AP600 Standard Safety Analysis Report* (SSAR), Chapter 16, "Technical Specifications" (Reference 1-6)
- Shutdown risk evaluations – including shutdown PRA results and insights and fire/flood risk
- Compliance with the guidance in NUREG-1449
- *Draft Safety Evaluation Report* open item tracking system (OITS) open item resolutions, including RAI responses

While this report does not address draft Rule 50.57 for shutdown, it does address shutdown-related issues.

The scope of the AP600 SDER provides the NRC staff with the necessary information to support the *AP600 Design Certification Final Safety Evaluation Report* (FSER) with respect to the AP600 shutdown capabilities.

1.3 BACKGROUND

The Diablo Canyon event of April 10, 1987, and the loss of ac power at the Vogtle plant on March 20, 1990, led the NRC staff to issue NUREG-1449, which provides an evaluation of the shutdown risk issue. Through RAI 440.53, the NRC requested that Westinghouse perform a systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449 as applicable to the AP600 design. This assessment is documented in this SDER, WCAP-14837.

1.4 REFERENCES

1-1 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

1-2 DCP/WMS0331, *RAI Management Review*, RAI 440.53, July 29, 1994.

1-3 NUREG-1449, *Shutdown and Low Power Operations at Commercial Nuclear Power Plants in the United States*, September 1993.

1-4 NSD-NRC-97-4975 (DCP/NRC0731), *AP600 Shutdown Evaluation Report Outline*, February 5, 1997.

1-5 NSD-NRC-97-4936 (DCP/NRC0702), *AP600 Emergency Response Guidelines*, January 10, 1997.

1-6 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

2.0 MAJOR SYSTEMS DESIGNED TO OPERATE DURING SHUTDOWN

Westinghouse has considered shutdown modes, shutdown alignments, and industry issues related to shutdown in the design of the AP600 safety-related and nonsafety-related systems designed to operate or be available during shutdown. This section provides descriptions of the important systems designed to operate during shutdown and includes specific design features that have been incorporated for shutdown operations with a discussion of their operating modes or alignment during shutdown.

In this report, references are made to the various AP600 operating modes. The AP600 operating modes have been defined in the Technical Specifications (*AP600 Stcndard Safety Analysis Report* [SSAR] section 16.1, Table 1.1-1) (Reference 2.0-1). The mode definitions for the AP600 are similar to that of current Westinghouse pressurized water reactors (PWRs), with the difference being the definition of Mode 4, safe shutdown. In current plants, Mode 4 has traditionally been defined as hot shutdown and corresponds to the range of reactor coolant system (RCS) temperature between 350° and 200°F. The upper temperature limit corresponds to the temperature at which the safety-related residual heat removal system would be aligned to provide closed-loop cooling.

In the AP600, Mode 4 has been redefined as safe shutdown and corresponds to the range of RCS temperature between 420°F and 200°F. The upper temperature limit corresponds to the RCS temperature that can be achieved by the passive safety-related systems 36 hours after shutdown. The ability of the passive safety-related systems to achieve Mode 4 within 36 hours is shown in subsection 4.10.2 of this report.

2.0.1 References

2.0-1 *AP600 Standard Safety Analysis Report*, Chapter 16, "Te :hnical Specifications."

2.1 REACTOR COOLANT SYSTEM

2.1.1 System Description

The RCS is described in chapter 5 of the AP600 SSAR (Reference 2.1-1). The RCS consists of two heat transfer circuits – each with a steam generator, two reactor coolant pumps (RCPs), and a single hot leg and two cold legs – for circulating reactor coolant between the reactor and the steam generators. In addition, the system includes a pressurizer, interconnecting piping, and valves and instrumentation necessary for operational control and safeguards actuation. All system equipment is located in the reactor containment. Figure 2.1-1 (SSAR Figure 5.1-1) is a simplified sketch of the RCS. Figure 2.1-2 (SSAR Figure 5.1-2) illustrates the physical arrangement of the major components in the RCS.

During power operation, the RCPs circulate pressurized water through the reactor vessel and the steam generators. The water -- which serves as coolant, moderator, and solvent for boric acid (used for chemical shim control) – is heated as it passes through the core. The water next flows to the steam generators, where the heat is transferred to the steam generator system (SGS), and then is returned to the reactor by the RCPs to repeat the process. The steam generators have a vertical shell and U-tube configuration with integral moisture-separating equipment. The RCPs are high-inertia, high-reliability, and low-maintenance canned-motor pumps, which are integrated into the steam generator channel heads in the inverted position.

The pressurizer and its associated subsystems (spray, heaters, safety valves, and automatic depressurization valves) control RCS pressure by maintaining a single major water-steam interface in equilibrium under saturated conditions by electrical heaters and/or a water spray. The pressurizer, a vertical cylindrical vessel with hemispherical top and bottom heads, communicates with the RCS primary coolant loops via a surge line connected to one RCS hot leg. Electrical heaters are installed through the bottom head of the vessel and are removable for maintenance or replacement. Steam is formed by the heaters or condensed by the spray (circulated from the cold legs by the driving head of the RCPs) to control pressure variations due to expansion and contraction of the reactor coolant. The pressurizer pressure, temperature, and level instrumentation is provided as required by the protection and safety monitoring system (PMS) and the plant control system (PLS). For continuous monitoring of pressurizer/hot leg reactor coolant loop level, as the pressurizer and eventually the loops are drained to obtain an RCS level in the loop piping, the bottom tap of the pressurizer cold-calibrated wide-range level channel is connected to the bottom of the hot leg that communicates with the pressurizer. Surge line temperature is monitored to detect thermal stratification and pressurizer insurges from the RCS hot leg.

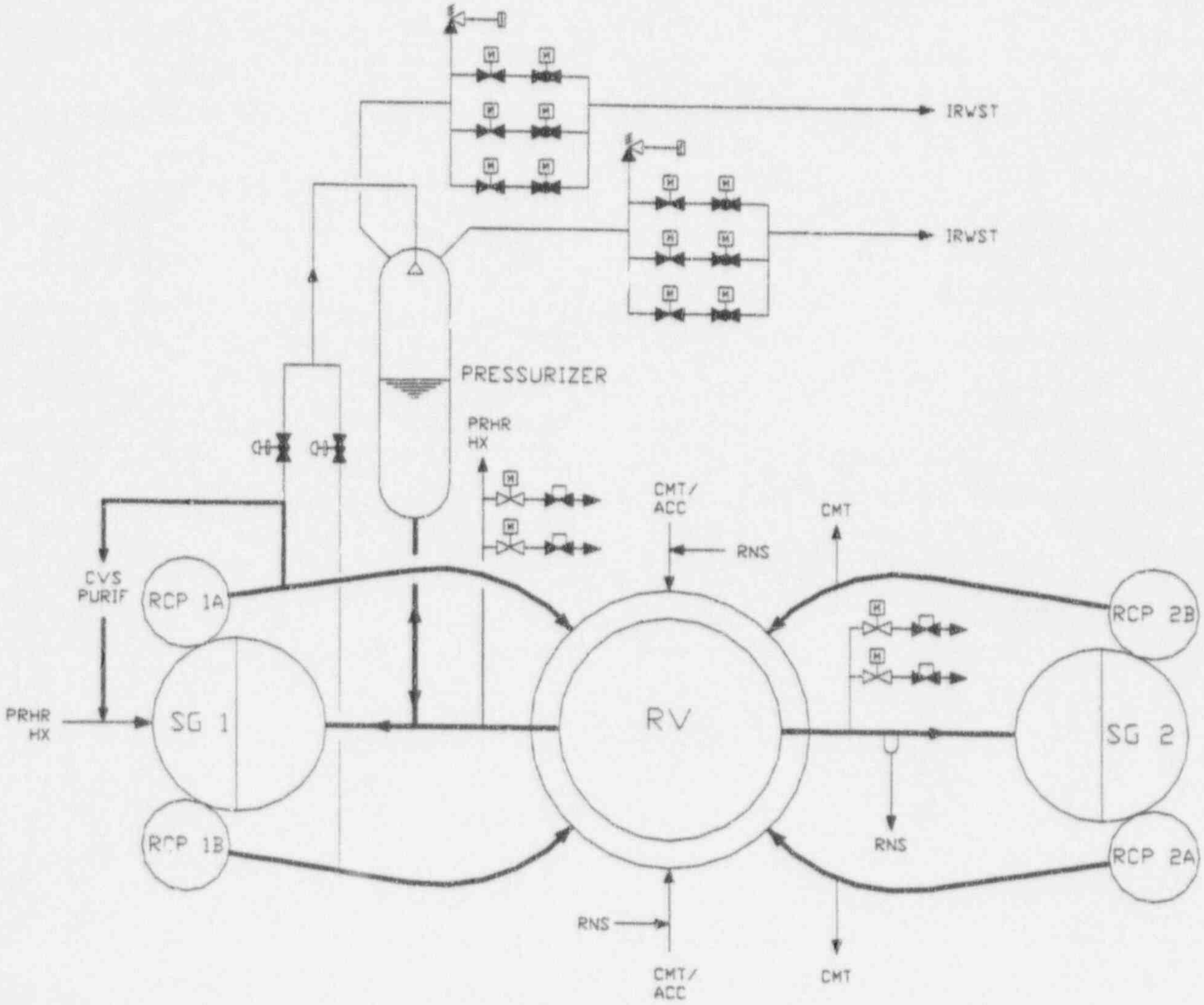


Figure 2.1-1 Reactor Coolant System Simplified Sketch

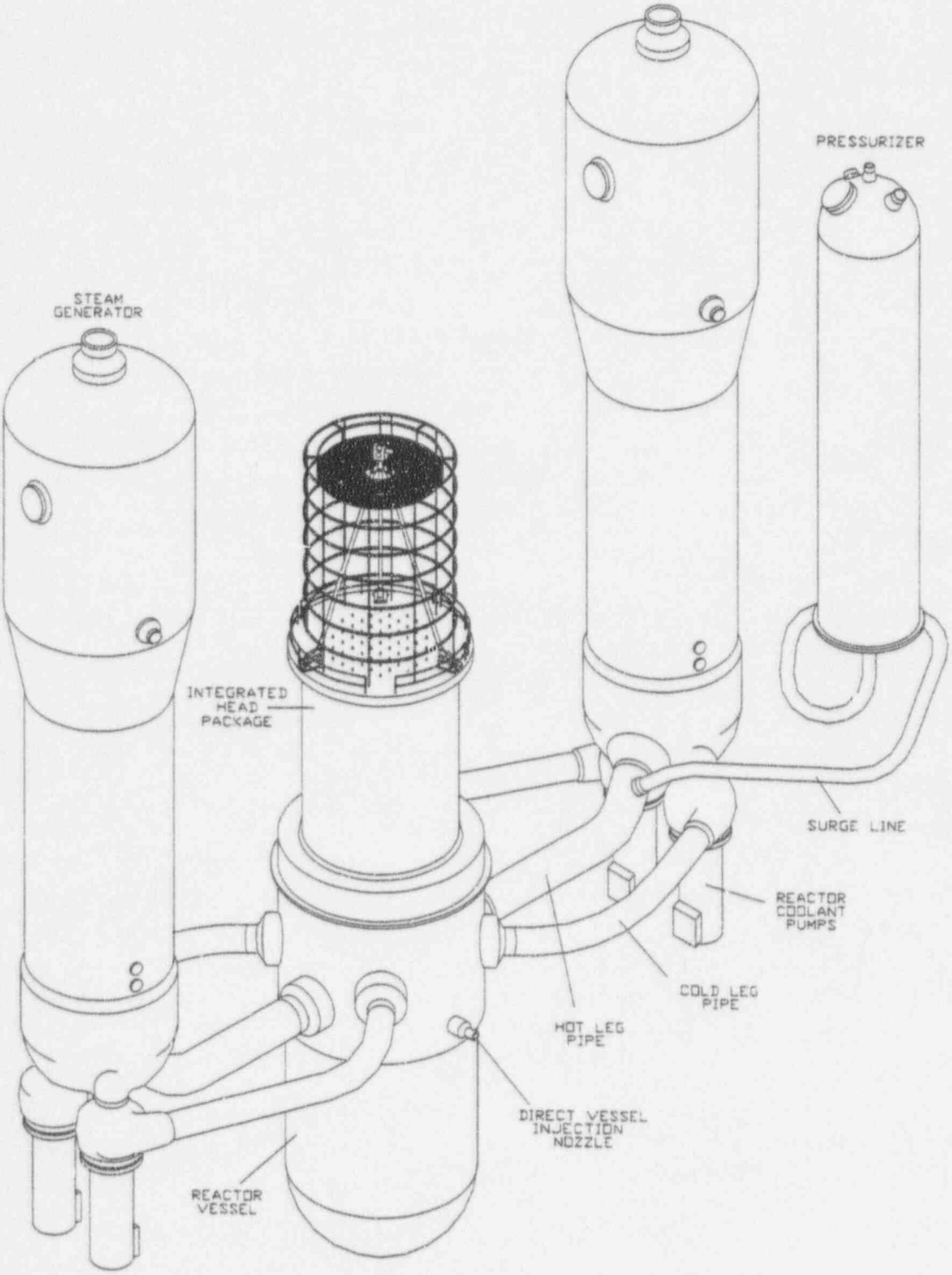


Figure 2.1-2 Reactor Coolant System Arrangement

Two spring-loaded safety valves – designed in accordance with American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section III – are located on the top of the pressurizer to provide overpressure protection for the RCS. One valve is installed on each of the two headers leading to a set of automatic depressurization valves.

The inlet piping does not contain a water-filled loop seal, which simplifies the discharge piping supports. This also will reduce the effects that water-filled loop seals can have on safety valve setpoint drift as engineered in operating plants. The downstream piping directs the valve discharge away from the pressurizer, automatic depressurization system (ADS) valves, and safety-related equipment and into the containment atmosphere (and eventually collected in either the in-containment refueling water storage tank [IRWST] or the containment sump). The downstream piping consists of a short length of piping fitted with a rupture disc to provide a closed volume (discharge chamber) in which valve leakage may cool and condense. A 1-inch cross-connect between the pressurizer safety valve discharge piping and the automatic depressurization valves discharge piping permits the pressurizer safety valve leakage to continuously drain to the reactor coolant drain tank via the discharge piping of the automatic depressurization valves. A temperature detector with a high alarm (in each discharge line) alerts the operator either of safety valve leakage or of actuation.

The automatic depressurization valve subsystem consists of four different valve stages. These stages open sequentially to reduce RCS pressure sufficiently so that long-term core cooling can be provided from the passive core cooling system (PXS).

ADS stages 1, 2, and 3 are arranged into two groups. Each group has a common inlet header connected to the top of the pressurizer and a common discharge line to one of the spargers in the IRWST.

For ADS stages 1, 2, and 3, each valve stage consists of two lines with each line containing two valves in series that are both normally closed. Each stage line is arranged with an isolation valve in series with (and upstream of) a control valve. When ADS is actuated, the isolation valve opens first; then the control valve subsequently opens to initiate and control the flow to the IRWST. The upstream ADS isolation valves for stages 1 through 3 are gate valves. The downstream ADS valves are globe valves.

ADS stage 4 is arranged into two groups. Each group has a common inlet header connected to one of the hot legs. Each stage 4 group discharges separately into a steam generator compartment at an elevation above post-accident flood-up level.

ADS stage 4 consists of four lines, each line containing two valves in series. Each line is arranged with a normally open isolation valve in series with (and upstream of) a squib valve. The normally open isolation valve is a motor-operated gate valve and is closed to perform maintenance on the ADS squib valves.

2.1.2 Design Features to Address Shutdown Safety

The AP600 has incorporated many design features that address issues related to shutdown operations. This subsection provides a detailed discussion of the RCS design features that are incorporated to address shutdown operations or that are important to minimizing the risk to plant safety during shutdown.

2.1.2.1 Loop Piping Offset

As described in SSAR subsections 5.3.4.1 and 5.4.7.2.1 (Reference 2.1-1), the RCS hot legs and cold legs are vertically offset. This permits draining of the steam generators for nozzle dam insertion with the hot leg level much higher than traditional designs. The RCS must be drained to a level sufficient to provide a vent path from the pressurizer to the steam generators. This is nominally an 80-percent level in the hot leg. This loop piping offset also allows an RCP to be replaced without removing a full core.

2.1.2.2 RCS Instrumentation

Instrumentation is provided to monitor the RCS process parameters as required by the PLS and PMS as discussed in chapter 7 of the SSAR (Reference 2.1-2). This subsection describes RCS instrumentation designed to accommodate shutdown operations.

RCS Hot Leg Level

There are two safety-related RCS hot leg level channels, one located in each hot leg. These level indicators are provided primarily to monitor the RCS water level during mid-loop operation following shutdown operations. These are totally independent of each other. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg as close to the steam generator as possible. The steam generator tap is located at the high point of the tubing run. The level tap for the instrument in the hot leg with the normal residual heat removal system (RNS) step-nozzle suction line connection is between the reactor vessel and the step-nozzle. Figure 2.1-3 shows a simplified sketch of the RCS level instruments.

These channels provide signals for the following protection functions:

- Isolation of letdown on low level on a one-out-of-two basis
- Actuation of IRWST injection on low (empty) hot leg level on a two-out-of-two basis
- Actuation of fourth-stage ADS valves on low (empty) hot leg level on a two-out-of-two basis

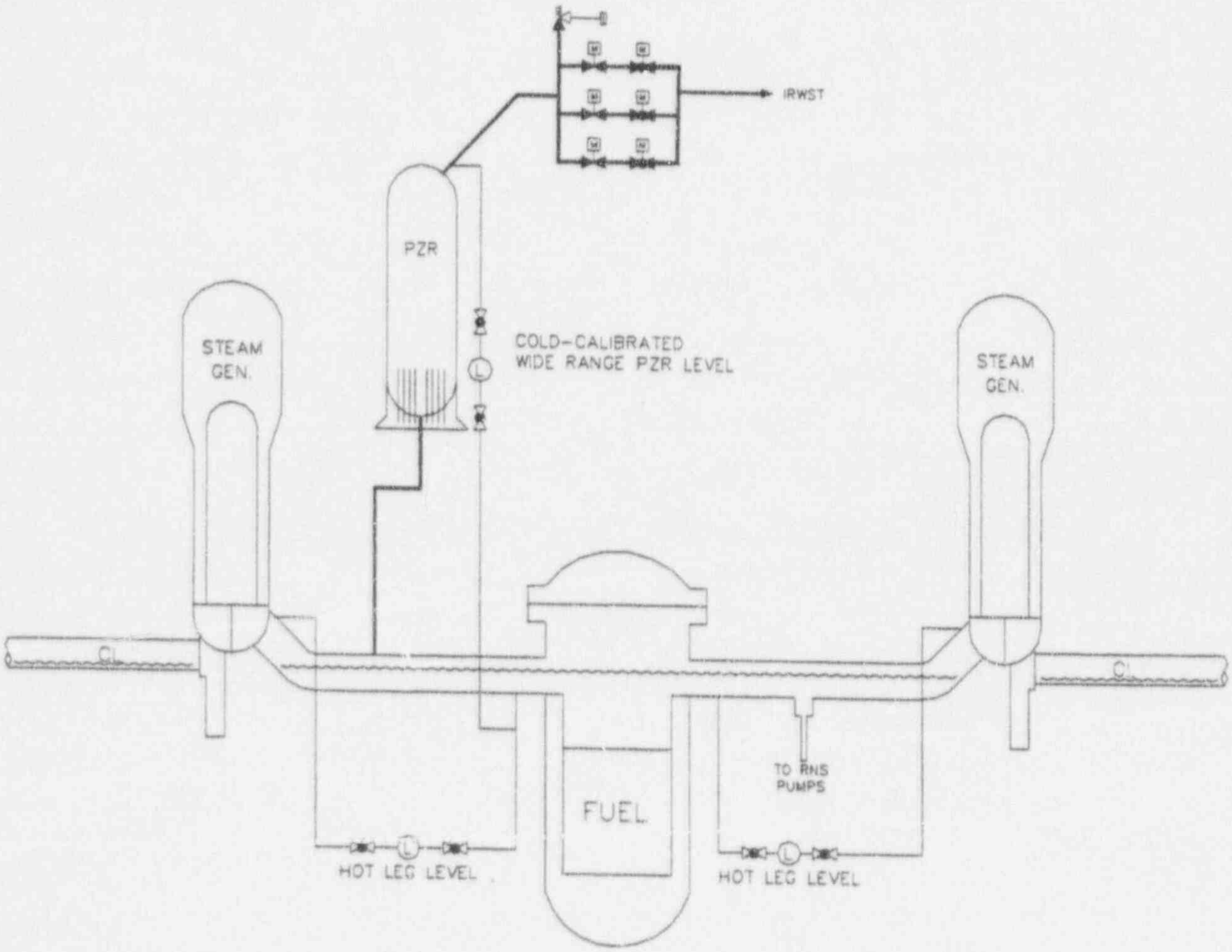


Figure 2.1-3 Reactor Coolant System Level Instruments Used During Shutdown

These functions protect the plant during shutdown operations. Letdown isolation assists the operators when draining the RCS to a mid-loop level. If the operators fail to isolate letdown, these channels send a signal to close the letdown valves and stop the draining process.

In the event of a loss of the RNS during shutdown, coolant inventory could be boiled away. When the hot leg water level indicates that the loops are empty, IRWST injection and fourth-stage ADS are actuated 30 minutes after receipt of the empty hot leg level signal.

These channels also provide signals to the letdown flow control valve to control the drain rate of the RCS via the letdown line during the transition to mid-loop operation. When the hot legs are full the drain rate can proceed at a high level. As the water level is reduced to the hot legs, the drain rate is automatically decreased to a rate of approximately 20 gpm.

These channels are also used to generate the alarms on low hot leg water level. The alarm setpoints are selected to give the operator sufficient time to take the manual actions necessary to prevent the automatic actuations described previously. Indication of these channels is retrievable in the main control room. This variable is used by the operator to monitor the status of RCS inventory following an accident and is, therefore, classified as a post-accident monitoring system (PAMS) variable as discussed in SSAR section 7.5 (Reference 2.1-2). Table 2.1-1 provides a summary of the various protection functions, control functions, and alarms associated with the hot leg level instruments.

The accuracy and response time of the hot leg level instruments are consistent with the standard engineered safety features (ESF) actuations discussed in SSAR section 7.3. As discussed in the Westinghouse response to request for additional information (RAI) 420.24 (Reference 2.1-3), concerns related to potential problems of noncondensible gases in the hot leg level instrument lines that have been raised in NRC Information Notice 92-54, Level Instrumentation Inaccuracies Caused by Rapid Depressurization (Reference 2.1-4), have been addressed in the layout of the instrument lines. In addition, as the hot leg level instruments are provided primarily for shutdown operations, off-gassing due to sudden depressurization of the RCS in shutdown modes is not a concern.

In the AP600, draining of the RCS to mid-loop conditions is achieved in a controlled manner as discussed in subsection 2.1.2.4. Due to the low RCS drain rate (20 gpm), and the RCS step-nozzle as discussed in subsection 2.1.2.3, the amount of air-entrainment, and therefore RCS level perturbation during mid-loop, is negligible. Draining of the RCS is conducted in a quasi-steady-state, and the reliability of an accurate level reading is high.

Table 2.1-1
AP600 Hot Leg Level Setpoints

Nominal Level	Elevation (in.)	Time[1] (minutes)
Top of Level Tap	54.37	–
Top of Hot Leg	31	0
Nominal Water Level for Mid-loop Operation	27.74	~30
Approximate Low Level Alarm Setpoint	22	~80
Approximate Auto-isolation of Letdown	18	~100
Hot Leg Centerline	15.50	–
Onset of Incipient Vortex Formation	10.64	~130
Potential 5-Percent Air Entrainment	8.60	~145
IRWST Actuation Setpoint	3	–

1. Times assuming nominal drain rate of 20 gpm.

Pressurizer Level

A fifth nonsafety-related independent pressurizer level transmitter, calibrated for low temperature conditions, provides water level indication during startup, shutdown, and refueling operations in the main control room and in the remote shutdown workstation. The upper level tap is connected to an ADS valve inlet header above the top of the pressurizer. The lower level tap is connected to the bottom of the hot leg. This provides level indication for the entire pressurizer and a continuous reading as the level in the pressurizer decreases to mid-loop levels during shutdown operations.

RCS Hot Leg Wide-Range Temperatures

The RCS contains two safety-related thermowell-mounted hot leg wide-range temperature detectors, one in each hot leg. The orientation of the resistance temperature detectors enables measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. Their range is selected to accommodate the low RCS temperatures that can be attained during shutdown. In addition, at least two incore thermocouple channels are available to measure the core exit temperature during mid-loop RNS operation. These two thermocouple channels are associated with separate electrical divisions.

Pressurizer Surge Line Temperatures

There are three nonsafety-related temperature detectors located on the RCS pressurizer surge line. These instruments monitor the pressurizer surge line fluid temperature during plant normal operations to detect thermal stratification in the surge line. Two of the temperature detectors are on a moderately sloped run approximately midway between the RCS hot leg and the pressurizer. One detector is on the bottom of the pipe and the other detector on the top. The third detector is located on the pressurizer surge line as close to the pressurizer nozzle as possible. This detector is used to monitor cold insurges to the pressurizer during transient operations.

The temperature is monitored at the three locations using strap-on resistance temperature detectors. Temperature indication is provided in the main control room. One low-temperature alarm is provided to alert the operator of thermal stratification in the surge line. This alarm is associated with the detector on the bottom of the pipe.

During shutdown operations, this temperature instrumentation will be monitored to detect possible surge line stratification. If stratification is detected, the operators can increase spray flow to increase the outsurge from the pressurizer and reduce stratification in the surge line.

2.1.2.3 Step-nozzle Connection

The AP600 RNS uses a step-nozzle connection to the RCS hot leg. The step-nozzle is a 20-inch schedule 140 pipe, approximately 2 feet long. A comparison of the AP600 step-nozzle to a typical residual heat removal nozzle for current plants is shown in Figure 2.1-4.

The step-nozzle connection has two effects on mid-loop operation. One effect is to substantially lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction as shown experimentally will be no greater than 5 percent (NTD-NRC-94-4191) (Reference 2.1-5). The step-nozzle thereby precludes air binding of the pump and will allow for RNS pump operations with low water levels in the hot leg.

Table 2.1-1 provides a comparison of the critical hot leg level during mid-loop to the various protection and control functions and alarms associated with the hot leg level instruments to demonstrate the margin available during mid-loop operation.

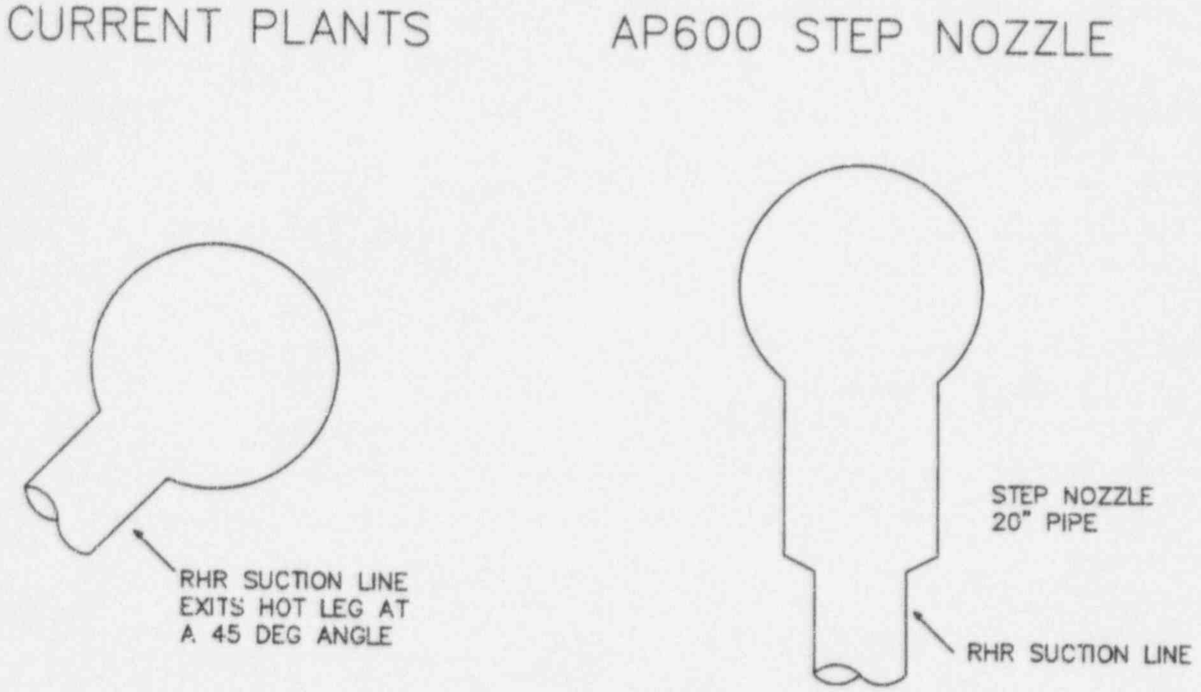


Figure 2.1-4 Comparison of AP600 Step-nozzle to Current Residual Heat Removal Nozzles

2.1.2.4 Improved RCS Draindown Method

During the cooldown operations, the RCS water level is drained to a mid-loop level to permit steam generator draining and maintenance activities. The AP600 has improved the reliability of draindown operations by incorporating a dedicated drain path to be used to reduce the water level in the RCS controlled in the main control room. In current plants, various drain paths can be used either locally or remotely from the control room. These drain paths include the safety-related residual heat removal system, loop drain valves, and letdown. The result is that draining of the RCS can be difficult to control, and perturbations in water level can occur due to inadvertent system manipulations of which the operators are not always aware.

The RCS drain path is via the CVS letdown line from the RNS cross-connect provided to maintain full RCS purification flow during shutdown. The letdown line flow control valve controls the letdown rate, which controls the RCS draindown rate. At the appropriate time during the cooldown, the operator will initiate the draindown by placing the CVS letdown control valve into a refueling draindown mode. At this time, the makeup pumps will be turned off and the letdown flow control valve will control the drain rate to the liquid radwaste system proceed at an initial maximum rate of 100 gpm and be reduced to 20 gpm once the level in the RCS is to the top of the hot leg. The letdown rate is manually controlled based upon the difference in flow instruments readings in the VS letdown line and injection line. The letdown flow control valve as well as the letdown line containment isolation valve will receive a signal to automatically close once the appropriate level is attained. Alarms will actuate in the control room if the RCS level falls below the automatic letdown valve closure setpoint so that the operator is alerted to manually isolate the letdown line. Furthermore, an automatic isolation of the letdown line is actuated on low hot leg level as shown in Table 2.1-1. This draindown method provides a reliable means of attaining mid-loop conditions.

2.1.2.5 ADS Valves

The ADS first-, second-, and third-stage valves, connected to the top of the pressurizer, are open whenever the core makeup tanks (CMTs) are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal were lost. This also allows the IRWST to automatically provide injection flow if it is actuated on a loss of decay heat removal. In addition, two of the four ADS fourth-stage valves are required to be available during reduced inventory operations to preclude surge line flooding following a loss of the RNS. The effectiveness of the ADS valves and IRWST injection to mitigate loss of the RNS during shutdown is shown in subsection 4.8.5 of this report.

2.1.2.6 Steam Generator Channel Head

The AP600 steam generator is a vertical-shell U-tube evaporator with integral moisture separating equipment. The generator is discussed in SSAR subsection 5.4.2 (Reference 2.1-1).

On the primary side, the reactor coolant flow enters the primary chamber via the hot leg nozzle. The lower portion of the primary chamber is spherical and merges into a cylindrical portion, which mates to the tubesheet. This arrangement provides enhanced access to all tubes, including those at the periphery of the bundle, with robotics equipment. This feature enhances the ability to inspect, replace, and repair portions of the AP600 unit compared to the more spherical primary chamber of earlier designs. The channel head is divided into inlet and outlet chambers by a vertical divider plate extending from the apex of the head to the tubesheet.

The reactor coolant flow enters the inverted U-tubes, transferring heat to the secondary side during its traverse, and returns to the cold leg side of the primary chamber. The flow exits the steam generator via two cold leg nozzles to which the canned-motor RCPs are directly attached.

The AP600 steam generator channel head has provisions to drain the head. For minimizing deposits of radioactive corrosion products on the channel head surfaces and for enhancing the decontamination of these surfaces, the channel head cladding is machined or electropolished for a smooth surface. The large primary manways provide enhanced manned access capability compared to the manways in previous model steam generators.

The steam generator is equipped with permanently mounted nozzle dam brackets, which are designed to support nozzle dams during refueling operations. The design pressure of the nozzle dam bracket and nozzle dam is selected to withstand the RCS pressures that can occur during the shutdown events. In particular, their design pressure is greater than that experienced during the loss of RNS analysis presented in subsection 4.8.5.

2.1.3 Shutdown Operations

The operation of the RCS for the various phases of shutdown operation is described in the following subsections.

2.1.3.1 Plant Startup

Plant startup encompasses the operations that bring the reactor plant from cold shutdown to no-load operating temperature and pressure.

The AP600 RCS uses a steam bubble heatup method traditionally used in most PWRs. Historically, plants have used both steam bubble heatups and water solid heatups. Both methods require careful monitoring of the RCS parameters during operation, and both could be used by the AP600. Operating plant experience has shown that steam bubble heatups are preferable. By maintaining a steam bubble in the pressurizer, the RCS is less vulnerable to pressure excursions due to inadvertent operations (such as an inadvertent starting of an RCP or chemical and volume control system [CVS] makeup pump). This section describes the steam bubble method of heatup for the AP600.

Before plant startup, the reactor coolant loops and the pressurizer are filled by the makeup pumps with coolant containing the proper concentration of boron. The secondary sides of the steam generators are filled to the normal startup level with water that meets the steam plant water chemistry requirements.

The RCS is filled using a vacuum refill system. At the conclusion of plant shutdown operations, the RCS is closed and the RCS water level is established near mid-loop. A vacuum refill system is connected to the manual vent located on top of the pressurizer. When started, the vacuum system transfers air from the RCS to the plant vent. Air is evacuated from the entire RCS including the reactor vessel head, inverted steam generator U-tubes, and pressurizer.

After the air is removed, the CVS makeup pump operates to fill the RCS to the pressurizer no-load level. The level then remains at or near this value throughout the heatup. The heatup is initiated by shutting off cooling water flow to the RNS and energizing the pressurizer heaters. This allows slow heating of the RCS with core residual heat coincident with controlled pressurizer heating. When the saturation temperature for the existing low pressure is reached in the pressurizer, the pressurizer heatup is suspended briefly to permit steaming off (through the automatic depressurization valves into the reactor coolant drain tank) of any gasses present in the pressurizer. After this venting, pressurizer heatup is resumed and continues until saturation conditions at the pressure required to provide adequate net positive suction head (NPSH) for reactor coolant pump operation are reached. Then all RCPs are started and RCS heatup proceeds on pump heat.

During heatup operations, the pressurizer spray valves are opened to provide partial pressurizer spray flow. This will cause a continuous outsurge from the pressurizer to thus reduce or eliminate the potential for surge line stratification.

During the initial RCS heatup phase, hydrazine is added to the reactor coolant to scavenge dissolved oxygen in the system. RCS temperature is not raised above 180°F until the oxygen content has been reduced below the specified maximum concentration.

After the steam bubble has been established at the desired RCS pressure, subsequent pressurizer heating is controlled to maintain adequate suction pressure for the pumps while minimizing the temperature difference between pressurizer and loops (to reduce the potential for thermal shock across the surge line). RCS heatup operations have been defined to limit the ΔT across the surge line to 320°F. Pressurizer spray operation is used when necessary for pressurizer pressure-temperature control. Figure 2.1-5 shows the RCS heatup operations as discussed in SSAR section 5. The RCPs are used to heat the coolant to the hot standby (no-load) temperature.

2.1.3.2 Plant Shutdown

Plant shutdown is defined as the operation that brings the reactor plant from no-load operating temperature and pressure to cold shutdown.

Before plant shutdown, a boric acid solution from the CVS is added to the RCS to increase the reactor coolant boron concentration to that required for cold shutdown. If the shutdown is for refueling or an operation that requires opening of the RCS, the hydrogen and any fission gases in the reactor coolant are reduced by degassing the coolant with the CVS and the liquid radwaste system. The pressurizer liquid level is reduced to the no-load value.

Plant cooldown is accomplished in two phases. The first is by the combined use of the RCS and the SGS, and the second is by the RNS.

During the first phase of the cooldown, with the RCS temperature above 350°F, residual core and reactor coolant heat is transferred to the steam system via the steam generators. The steam is dumped to the main condenser as long as a vacuum can be maintained. At least one of two RCPs in steam generator (SG) 1 is kept running to ensure uniform RCS cooldown.

At least one pump in the SG 1 loop is kept running because the pressurizer spray lines are connected to the cold legs in this loop. Two pumps may be operated to provide additional spray flow. One RCP will provide flow through both steam generators to assist in the cooling of the steam generators and will provide sufficient flow through the core for core decay heat removal and mixing.

The pressurizer heaters are de-energized and spray flow is controlled to cool the pressurizer while maintaining the required RCP suction pressure. When the reactor coolant temperature is below approximately 350°F and the pressure is in the range of 400 to 450 psig, the second phase of cooldown commences with the operation of the RNS. The RNS takes suction from the hot leg and returns flow to the vessel via the direct vessel injection nozzles.

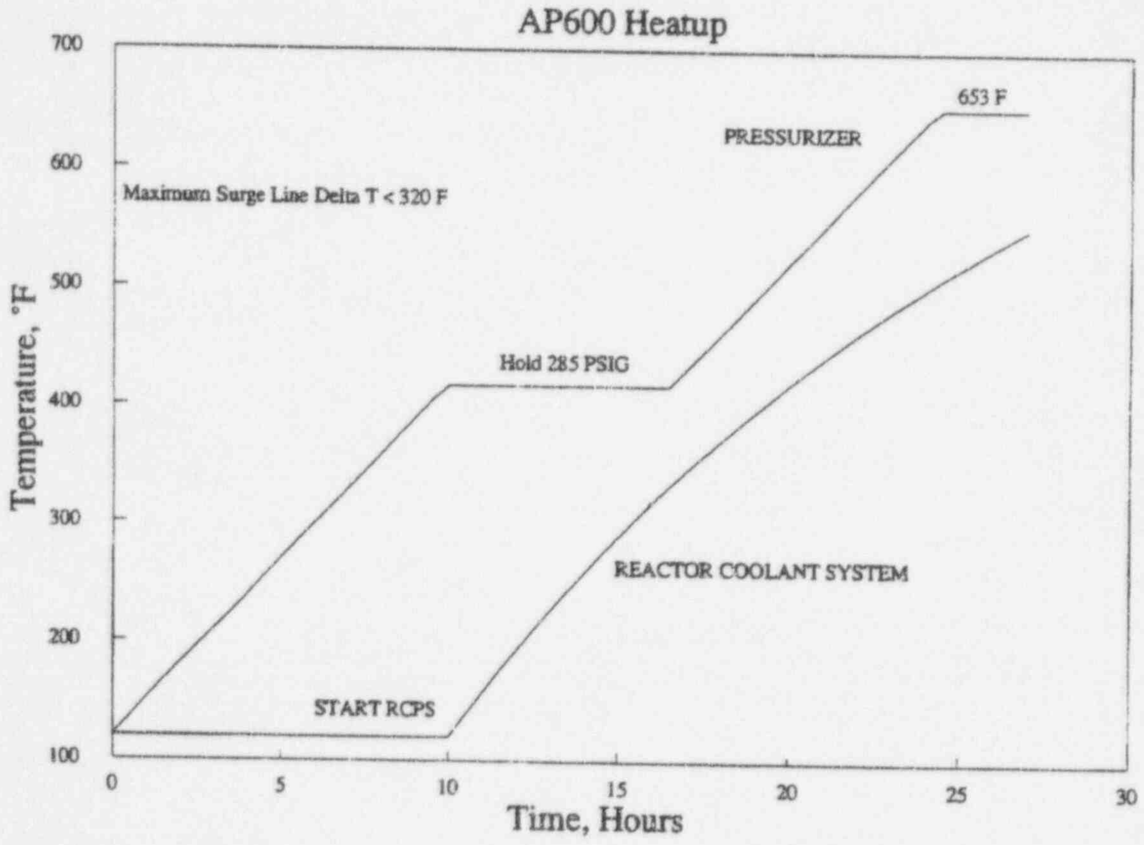


Figure 2.1-5 AP600 Heatup Profile

When the pressurizer has been cooled to the saturation temperature corresponding to the minimum pressure required for RCP operation, its pressure and temperature are maintained constant while cooling of the loops and reactor continues. During this period, the pressure is maintained at or above the minimum required for RCP operation. When the RCS temperature has been reduced to 180°F, hydrogen peroxide is added to the RCS (via the CVS) to improve activity reduction in the RCS. For minimizing the chances for collecting a hydrogen bubble in the pressurizer, the pressurizer is filled water-solid for hydrogen peroxide addition. This is accomplished by filling the pressurizer via the auxiliary spray lines. Heaters continue to operate to maintain system pressure necessary for RCP operations. Once the pressurizer is filled, pressure is controlled by the letdown flow control valve in the CVS. The pressurizer spray valves are then opened to circulate the contents of the pressurizer to maintain the pressurizer water chemistry in equilibrium with the rest of the system. An RCP continues to operate throughout the process to keep the RCS coolant chemistry in equilibrium. After the RCS temperature has been decreased to 160°F, the operating RCP is tripped, provided that the RCS activity levels have been reduced sufficiently to continue with the planned shutdown activities.

Figure 2.1-6 shows the RCS cooldown operations.

2.1.3.3 Mid-loop Operations

During plant shutdown, the RCS may be required to be drained to a reduced inventory state referred to as mid-loop. Mid-loop operations are required to facilitate maintenance operations associated with the steam generators.

The RCS has dedicated hot leg level instrumentation that provides the operator with readout in the main control room. All operations associated with mid-loop operations are controlled from the main control room. The following paragraphs describe the process to achieve mid-loop operations.

At the appropriate time during the cooldown, the operator can initiate the draindown by placing the CVS letdown control valve into refueling draindown mode. At this time, the letdown flow control valve will control the drain rate to the liquid radwaste system. The drain rate will proceed at an initial maximum rate down to a drain rate of 20 gpm once the level in the RCS is to the top of the hot leg. The operator can manually isolate the letdown control valve to stop the draindown at the appropriate setpoint. In addition, the letdown flow control valve as well as the letdown line containment isolation valve will receive a signal to automatically close once an appropriate level is attained. Furthermore, alarms will actuate in the control room if the level continues to drop so that the operator would be alerted to manually initiate isolation of the letdown line.

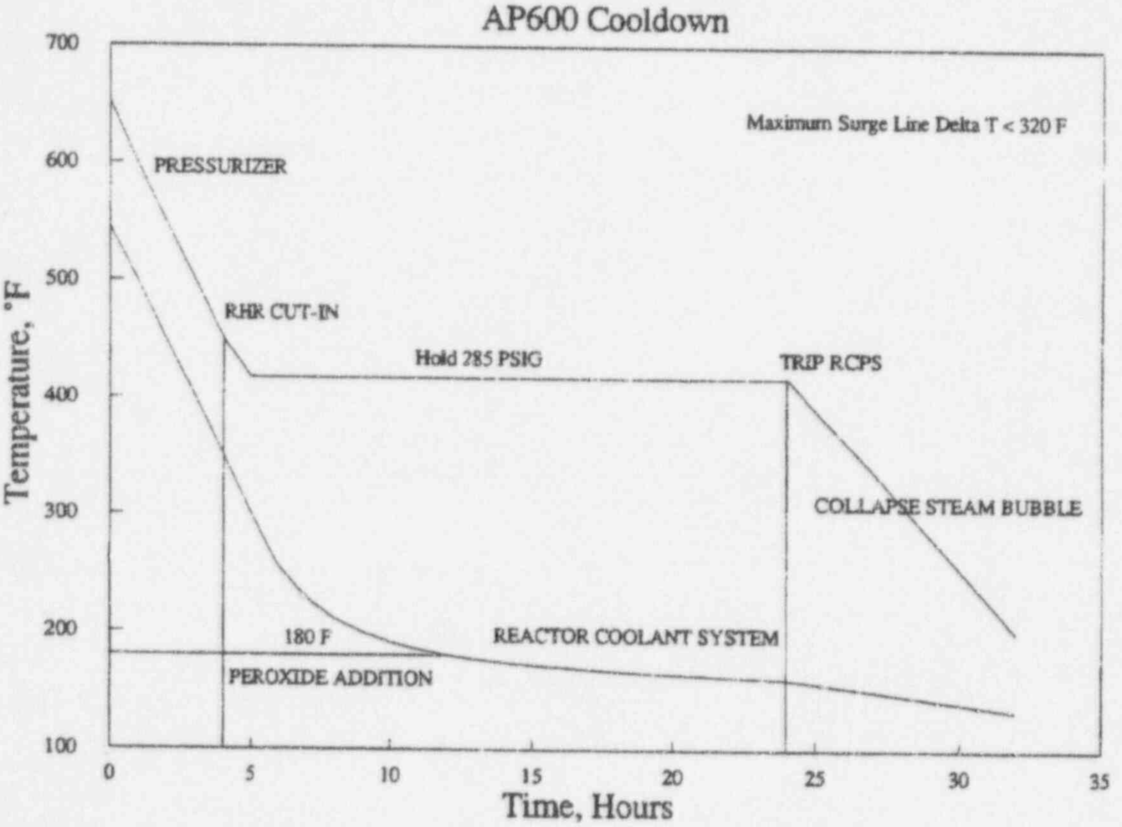


Figure 2.1-6 AP600 Cooldown Profile

Once mid-loop conditions are achieved, the required maintenance activity is performed. During refueling outages, nozzle dams are inserted in the steam generator inlet and outlet nozzles. The nozzle dams allow steam generator maintenance activities to continue during the refueling. Once the nozzle dams are in place, refueling operations may begin.

2.1.3.4 Refueling

Before removing the reactor vessel head for refueling, the system temperature is reduced to 120°F and hydrogen and fission products are removed. The pressurizer is vented, and the operation of draining the RCS begins. When the level instrumentation indicates that the coolant has been drained to below the reactor vessel head vent, the vessel head is vented. Draining then continues until the water level is below the reactor vessel flange. The refueling canal is then flooded by gravity, and then later, by the spent fuel pool cooling system (SFS) pumps. The SFS floods the canal directly to therefore bypass the need to flood up through the vessel. This reduces radiation doses during the refueling outage and improves the clarity of the refueling water. The vessel head is raised as the refueling canal is flooded. RCS cooling is provided by the RNS during refueling. Upon completion of refueling, the refueling cavity is drained, the reactor vessel head is replaced, and the system is refilled for plant startup.

2.1.4 References

2.1-1 *AP600 Standard Safety Analysis Report*, Chapter 5, "Reactor Coolant System and Connected Systems."

2.1-2 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

2.1-3 ET-NRC-93-3924 (NSRA-APSL-93-0249), "Westinghouse Responses to NRC Requests for Additional Information on the AP600," RAI 420.24, July 16, 1993.

2.1-4 NRC Information Notice 92-54, "Level Instrumentation Inaccuracies Caused by Rapid Depressurization," July 24, 1992.

2.1-5 NTD-NRC-94-4191 (DCP/NRC0124) APWR-0452, *AP600 Vortex Mitigator Development Test for RCS Mid-loop Operation*, July 6, 1994.

2.2 STEAM GENERATOR AND FEEDWATER SYSTEMS

2.2.1 System Description

This section discusses the AP600 steam generator system (SGS) and the main and startup feedwater system (FWS) designs as they relate to shutdown operations. These systems are discussed in chapter 10 of the AP600 SSAR (Reference 2.2-1). The SGS consists of the safety-related portions of the secondary side systems. The FWS consists of the main feedwater and startup feedwater subsystems designed to provide feedwater to the steam generators during normal power operations and following transient and accident events as desired. Figures 2.2-1, 2.2-2, and 2.2-3 are simplified sketches of the SGS and FWS based on SSAR sections 10.3 and 10.4 system descriptions.

2.2.1.1 Main Steam and Associated Lines

The primary function of the main steam line is to supply steam from the steam generators to the main steam system (MSS) and subsequently to the main turbine system (MTS) over a range of flows and pressures covering the entire operating range from system warmup to maximum calculated turbine conditions for full power operation. Each main steam line within the SGS has one main steam isolation valve (MSIV), three main steam safety valves, one power-operated relief valve (PORV), and one PORV block valve. The MSIV has a bypass valve for use when the MSIVs are closed to permit warming of the main steam lines prior to startup. A drain line with two isolation valves collects condensate upstream of the MSIVs and directs it to the turbine drain system. All of these valves are located in the auxiliary building within the penetration area.

2.2.1.2 Feedwater Lines

The function of the SGS feedwater subsystem is to transport feedwater to the steam generator as required to maintain steam generator level during the various modes of operation. The main feedwater portion of the SGS is designed to furnish feedwater flow at the required temperature, pressure, and flow rate to the steam generators during all modes of power operation above a minimum power level. The startup feedwater portion is designed to furnish feedwater flow to the steam generators under low flow conditions such as startup, hot standby, shutdown, or transient conditions or up to 10-percent power when the main feedwater system is unavailable.

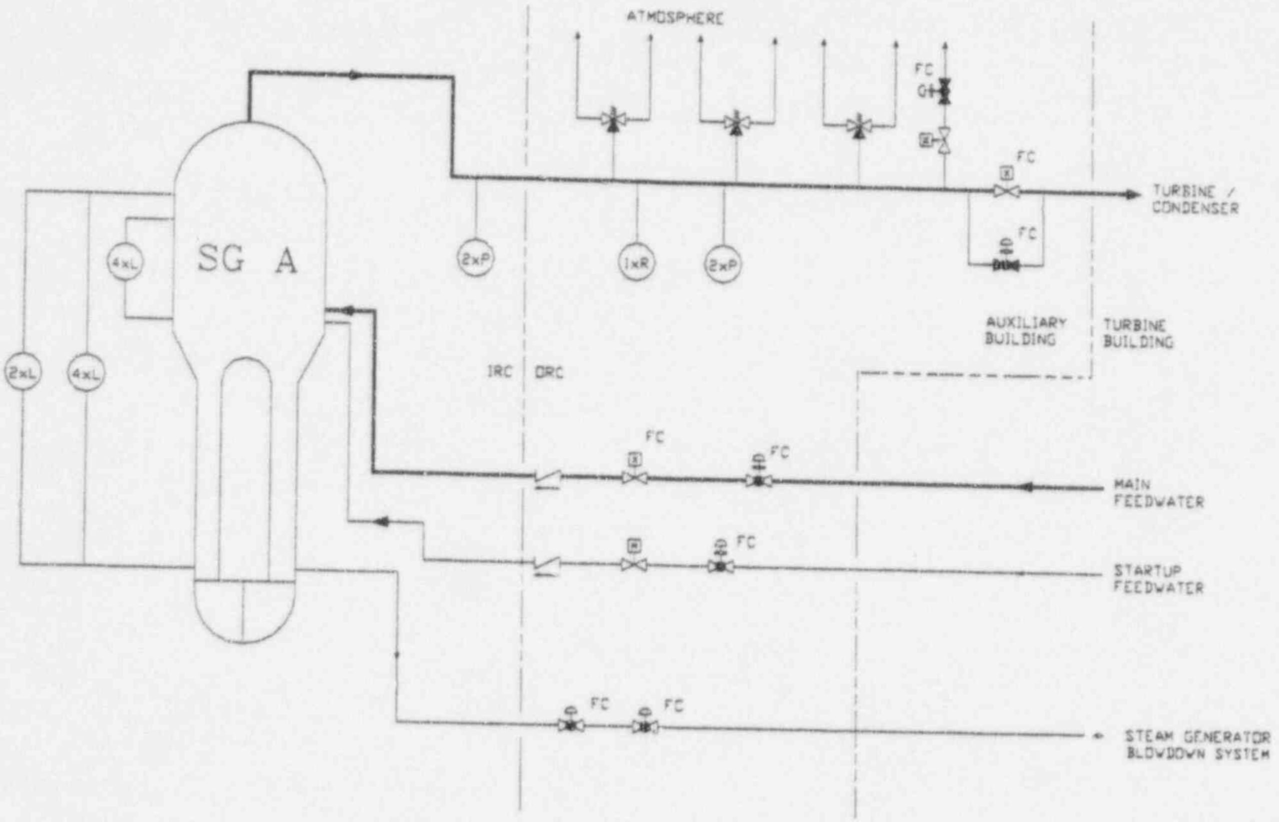


Figure 2.2-1 Steam Generator System Sketch

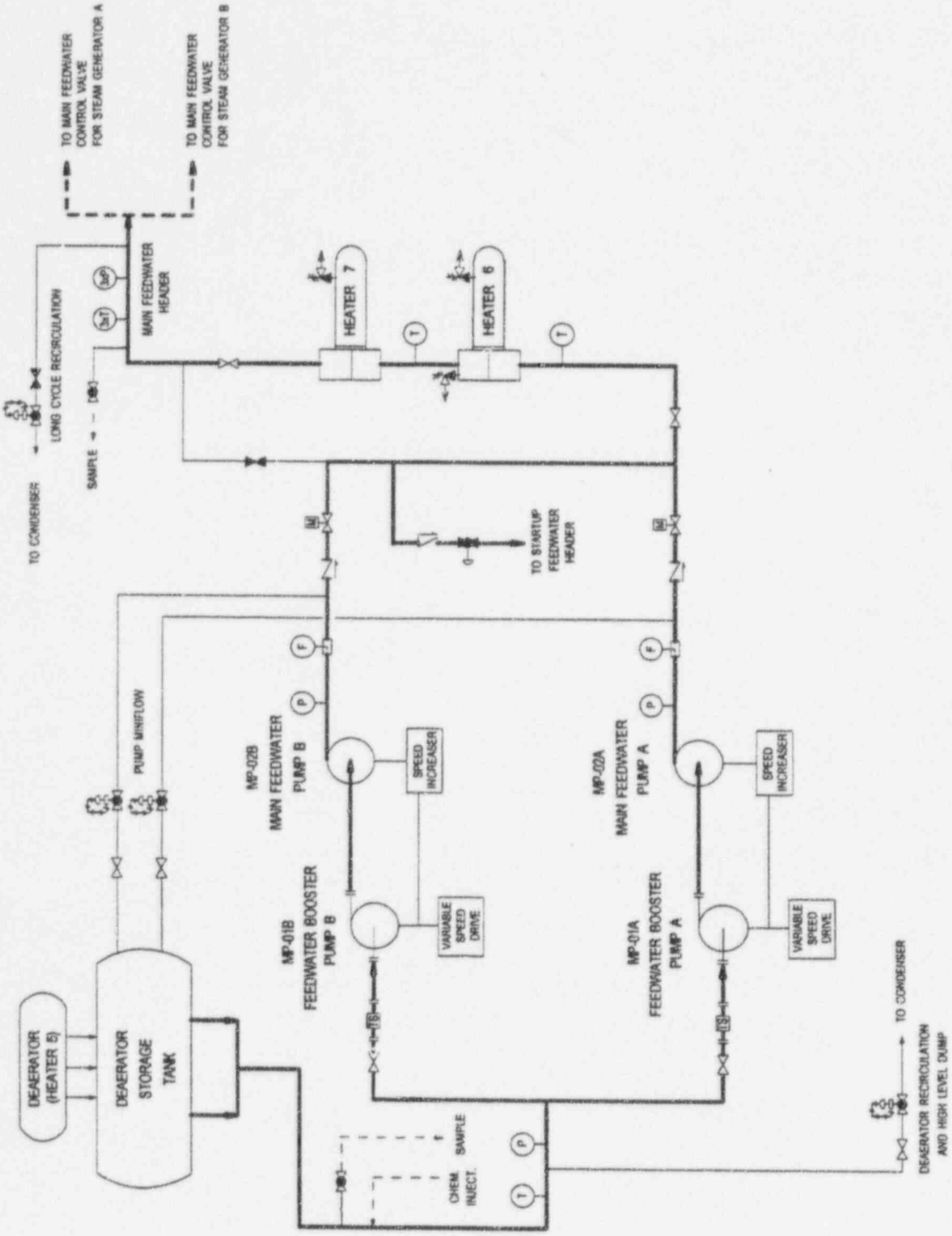

TO MAIN FEEDWATER CONTROL VALVE FOR STEAM GENERATOR A
TO MAIN FEEDWATER CONTROL VALVE FOR STEAM GENERATOR B
TO CONDENSER
LONG CYCLE RECIRCULATION
SAMPLE
ΔsT
ΔsP
MAIN FEEDWATER HEADER
HEATER 7
HEATER 6
T
T
M
M
TO STARTUP FEEDWATER HEADER
PUMP MINIFLOW
F
P
F
P
MP-02B MAIN FEEDWATER PUMP B
SPEED INCREASER
MP-02A MAIN FEEDWATER PUMP A
SPEED INCREASER
MP-01B FEEDWATER BOOSTER PUMP B
VARIABLE SPEED DRIVE
MP-01A FEEDWATER BOOSTER PUMP A
VARIABLE SPEED DRIVE
TS
TS
DEAERATOR (HEATER 5)
DEAERATOR STORAGE TANK
SAMPLE
CHEM. INJECT.
P
T
TO CONDENSER
DEAERATOR RECIRCULATION AND HIGH LEVEL DUMP

Figure 2.2-2 Feedwater System Sketch – Main Feedwater

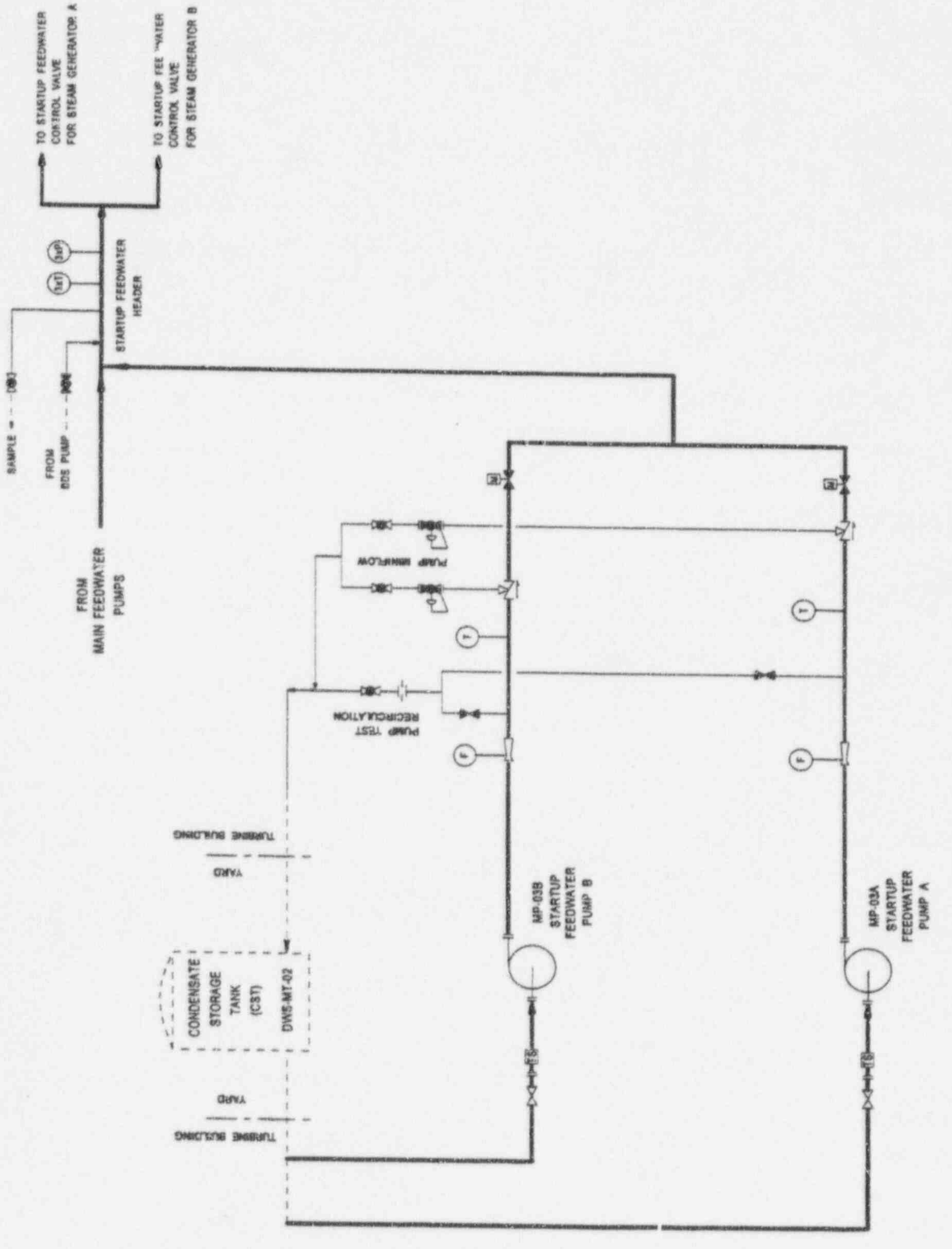


Figure 2.2-3 Feedwater System Sketch – Startup Feedwater

2.2.1.3 Main Feedwater

Main feedwater is delivered to the SGS from the FWS. Condensate from the deaerator is pumped via high pressure main feedwater pumps to the interface with the SGS. Each SGS main feedwater line includes one main feedwater control valve (MFCV), one main feedwater check valve, and one main feedwater isolation valve (MFIV), all located in the auxiliary building. There is also a manual isolation valve and a flow measuring feedwater venturi upstream of these valves in the turbine building. The manual valve permits isolation of the MFCV from the feedwater system for maintenance. Normal main feedwater sampling is not provided in the SGS, but rather is accomplished by secondary sampling system connections in the feedwater system within the turbine building.

2.2.1.4 Startup Feedwater Delivery From the Main Feedwater Pumps

After filling drained steam generators with startup feedwater pumps, the preferred source of startup feedwater is from the demineralized water storage tank through the booster/main feedwater pumps. The flow path is the same as that described for main feedwater up to a point on the main feedwater pump discharge piping; at this point, a startup feedwater cross-connect line allows feedwater from a booster/main feedwater pump train to be supplied to the SGS startup feedwater control valves (SFCVs). Startup feedwater flows through a single common line, called the startup feedwater header, to a location near the turbine/auxiliary building interface where the flow then splits into two individual lines to the steam generators. The individual lines are part of the SGS, and each line includes a flow measuring element, an SFCV, a check valve, and a startup feedwater isolation valve (SFIV). Startup feedwater is supplied to each steam generator through a startup feedwater nozzle connection, which is physically separate from the main feedwater nozzle connection.

The startup feedwater header can be supplied either by the main feedwater pumps as described previously or by the startup feedwater pumps. A check valve in the cross-connect supply piping from the main feedwater pumps restricts feedwater from the startup feedwater pumps from flowing to the main feedwater portion of the FWS. An air-operated isolation valve in the cross-connect piping opens to allow the main feedwater pumps to supply the startup feedwater header. The isolation valve is normally closed during full power operation and provides positive isolation of main feedwater. The cross-connect isolation valve also automatically closes, if open, in the event of a main feedwater isolation signal, based on the same isolation signal that trips the booster/main feedwater pumps, and closes the feedwater isolation valve. The isolation valve provides redundant protection to prevent the main feedwater pumps from delivering to the startup feedwater lines.

2.2.1.5 Startup Feedwater Delivery From the Startup Feedwater Pumps

The relatively low capacity startup feedwater pumps are normally used to fill the steam generators during startup following outages and during the early stages of plant startup while water chemistry in the main feedwater path is being adjusted. During power operation, the startup feedwater pumps and their associated flow paths primarily provide backup feedwater capability in the event the booster/main feedwater pumps or their associated flow paths are lost.

The startup feedwater pumps and their associated flow paths provide a nonsafety-related decay heat removal capability, mitigating loss of feedwater events. The PXS provides safety-related protection for loss of feedwater.

2.2.1.6 Blowdown Lines

The primary purpose of the steam generator blowdown system is to assist in maintaining acceptable secondary coolant water chemistry during normal operation and during anticipated operational occurrences of main condenser inleakage or primary to secondary steam generator tube leakage. It does this by removing impurities concentrated in the steam generator. The steam generator blowdown system accepts water from each steam generator and processes the water as required. The blowdown system also performs additional functions in support of the steam generator during shutdowns. It accepts water drained from the steam generator shell side, and it has a recirculation capability that can be used to cool the steam generator secondary side or to add chemicals for wet layup.

2.2.2 Design Features to Address Shutdown Safety

2.2.2.1 Feedwater Control

As discussed in the previous subsection, the AP600 provides improvements in feedwater control that minimizes the probability of loss of feedwater transients during low power and shutdown modes. The main feedwater pumps are capable of providing feedwater during all modes of operation, including plant startup and standby conditions. In addition, the startup feedwater pumps are automatically started in the event that the main feedwater pumps are unable to continue to operate. The startup feedwater pumps are also automatically loaded on the diesels for operation following a loss of offsite power.

2.2.2.2 Safety-Related Actuations in Shutdown Modes

The AP600 has various safety-related actuations associated with the SGS that are operable during shutdown modes. These include the PRHR HX actuation on low steam generator level during shutdown modes, and this is discussed in section 2.3 of this report. Also included is the isolation of the main steam line on a high (large) negative rate of change in steam pressure. This safety-related signal is provided to address a steam line break that could occur in Mode 3 or 4. If actuated, this signal causes the MSIVs to close to thus terminate the blowdown of the SGS following a steam line break. This signal is placed into service below the setpoint that disables the low steam line pressure signal (P11) that actuates steam line isolation as discussed in SSAR section 7.3 (Reference 2.2-2). When the operator manually blocks the low steam line pressure signal, the steam line pressure-negative rate high signal is automatically enabled.

This signal is operable during Mode 3 when a secondary side break or stuck open valve could result in the rapid depressurization of the steam line(s). In Modes 4, 5, and 6, this function is not needed for accident detection and mitigation. Subsection 4.2.3 discusses steam line break events that could occur in shutdown modes. Operability of this actuation logic is discussed in the AP600 Technical Specifications (Reference 2.2-3).

2.2.2.3 Steam Generator Cooling in Shutdown Modes

As discussed previously, the secondary side of the steam generators can be cooled during shutdown by recirculating their contents through the blowdown system heat exchanger. This feature reduces the challenges to low-temperature overpressure events. During RCS water-solid operation, heat input from the steam generators is capable of challenging the low-temperature relief valve. The Technical Specifications prevent the operators from starting an RCP with the steam generator secondary side temperature more than 50°F higher than the primary side, with the pressurizer water-solid. With the RCS water-solid, the heat input that could occur would cause the system to be pressurized to the low-temperature overpressure relief valve in the RNS.

When the RCPs are operating, the secondary side of the steam generator is cooled by steaming to the MSS. Once the RNS is aligned, and steaming to the MSS is decreased, the secondary side of the steam generators is cooled by operation of the RNS. However, once the RCPs are tripped, water does not circulate through the primary side of the tubes and the secondary side of the steam generators remains at elevated temperature. With the ability to cool the secondary side via the blowdown system, the AP600 reduces the probability that an RCP would be started with the secondary side of the generator at elevated temperature to thus reduce the risk of a low temperature overpressure event. This mode of cooling also makes the equipment available for maintenance at the earliest time in an outage.

The AP600 has also incorporated steam generator fluid thermocouples to monitor the temperature of the fluid in the secondary side of the steam generator. This improves the ability of the operators to monitor this temperature to prevent them from inadvertently starting an RCP with the secondary side at elevated temperatures.

2.2.3 Shutdown Operations

This subsection discusses shutdown operations associated with the SGS and feedwater systems.

2.2.3.1 Steam Generator Wet Layup

The steam generators are filled by the startup feedwater pumps using the condensate storage tank as a water source.

While the plant is in a cold shutdown condition, the SGS provides a recirculation flow to and provides a return flowpath from the blowdown system, which is used in a recirculation mode to maintain the steam generator fluid within the chemistry limits. The flow is provided to the blowdown system via the 4-inch steam generator system blowdown lines and is returned to the steam generator via the startup feedwater lines.

2.2.3.2 Plant Heatup

The initial water inventory in the steam generator will depend on the duration and the purpose of the shutdown. If drainage is required during shutdown, the steam generator is drained through the blowdown system. Normal levels will be established prior to startup.

Steam generator water level is maintained during startup/shutdown using the startup feedwater mode of the FWS. If the level of impurities in the steam generator exceeds the chemistry guidelines, operating the startup feedwater pumps at maximum blowdown flow allows for the impurity levels to be brought down to meet the secondary cycle chemistry operating guidelines within the shortest period of time.

Blowdown will be maintained at the maximum normal blowdown flow rate of 1 percent maximum steaming rate (MSR) during startup, except when a lower flow rate is required to achieve an adequate heatup rate using only the RCPs. The basis for this requirement is to facilitate stable feedwater control during this mode of operation. Because startup feedwater is in automatic control, responding to the steam generator level program, a continuous blowdown rate tends to create a continuous demand for startup feedwater, enhancing stable control. A continuous startup feedwater flow also reduces temperature transients on the startup feedwater nozzle, compared to slug feeding (start and stop flow).

Steam generated in the steam generator flows to the MSS via the MSIV bypass lines, during the time period before the MSIVs are opened, which warms the steam lines. This steam is also used for initial operation of various MSS subsystems.

As the RCS temperature increases during plant heatup, the temperature of the fluid in the steam generators also increases, causing a corresponding increase in main steam pressure. As the steam generator reaches a temperature of approximately 400°F, plant warmup and turbine roll may begin, with a continuous supply of feedwater being provided to the steam generator by the startup feedwater pumps, controlled by steam generator level demand. During this period, secondary side no-load temperature and pressure are maintained automatically by the turbine bypass system, which is placed in the pressure control mode. The bypass valves modulate to maintain steam header pressure.

As delivery of feedwater to the steam generator exceeds approximately 10 percent of the design feedwater flow, the main feedwater system will automatically come online.

2.2.3.3 Hot Standby

Hot standby conditions are defined as the reactor being subcritical at zero power and no-load pressure and temperature. During hot standby, a continuous supply of feedwater is delivered by the main or startup feedwater pumps through the startup feedwater lines in automatic control. Blowdown is maintained at 1 percent MSR to facilitate stable feed control and to minimize temperature transients on the startup feedwater steam generator nozzle.

Steam pressure is maintained by the condenser steam dump system operating in the pressure control mode automatically relieving steam as required.

2.2.3.4 Normal Cooldown

For performing a normal cooldown from power operation, the turbine load is decreased, the turbine is tripped, and the reactor is shut down. The turbine bypass system is placed in the cooldown mode of operation, which given operator inputs of initial and final temperatures and desired cooldown rate, automatically adjusts bypass valve position to cool the plant down to the point where the RNS can be placed in service.

Initially, feedwater is delivered continuously by the main feedwater pumps during cooldown to maintain steam generator inventories while heat is being removed. Decay and sensible heat are removed by supplying feedwater to the steam generator and releasing steam via the steam dump system to the condenser. Typically, feedwater flow rate demand during cooldown drops below 5 percent of design flow within 1 hour after reactor shutdown. Responsibility for feedwater supply is then transferred from the main feedwater lines to the startup feedwater lines with water provided by the main feedwater pumps. Blowdown is maintained at 1 percent MSR to facilitate stable feed control and to minimize temperature transients on the startup feedwater steam generator nozzle.

After approximately 4 hours, steam pressure is reduced to 125 psia at which point the RNS can be aligned to remove decay heat from the RCS and the blowdown system can be used to remove sensible heat from the steam generators.

2.2.3.5 Steam Generatcr Cooling

The SGS provides a flowpath to, and a return flowpath from, the blowdown system for use during shutdown operations when the steam generator pressure is less than 125 psig to cool the steam generator for inspection and maintenance. The flowpath within the SGS is the same as that used for steam generator wet layup.

2.2.4 References

2.2-1 *AP600 Standard Safety Analysis Report*, Chapter 10, "Steam and Power Conversion System."

2.2-2 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

2.2-3 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

2.3 PASSIVE CORE COOLING SYSTEM

2.3.1 System Description

The PXS is described in SSAR section 6.3 (Reference 2.3-1). The primary function of the PXS is to provide emergency core cooling following postulated design basis events. To accomplish this primary function, the PXS is designed to perform the following functions:

- Emergency core decay heat removal

  Provide core decay heat removal during transients, accidents, or whenever the normal heat removal paths are lost. This heat removal function is available at RCS conditions including shutdowns. During refueling operations, when the IRWST is drained into the refueling cavity, other passive means of core decay heat removal are used.

- RCS emergency makeup and boration

  Provide RCS makeup and boration during transients or accidents when the normal RCS makeup supply from the CVS is unavailable or is insufficient.

- Safety injection

  Provide safety injection to the RCS to provide adequate core cooling for the complete range of loss-of-coolant accidents (LOCAs), up to and including the double-ended rupture of the largest primary loop RCS piping.

- Containment pH control

  Provide for chemical addition to the containment during post-accident conditions to establish floodup chemistry conditions that support radionuclide retention with high radioactivity in containment and to prevent corrosion of containment equipment during long-term floodup conditions.

The PXS consists of a PRHR HX, two accumulators, two CMTs, an IRWST, two RCS depressurization spargers, pH adjustment baskets, and associated valves, piping, and instrumentation. Two simplified sketches, Figures 2.3-1 and 2.3-2 (SSAR Figures 6.3-3 and 6.3-4), include the four ADS stages because they functionally support the PXS. The PXS is designed to operate without the use of active equipment such as pumps and ac power sources. The PXS depends on reliable passive components and processes such as gravity injection and expansion of compressed gases. The PXS does require a one-time alignment of valves upon actuation of the specific components.

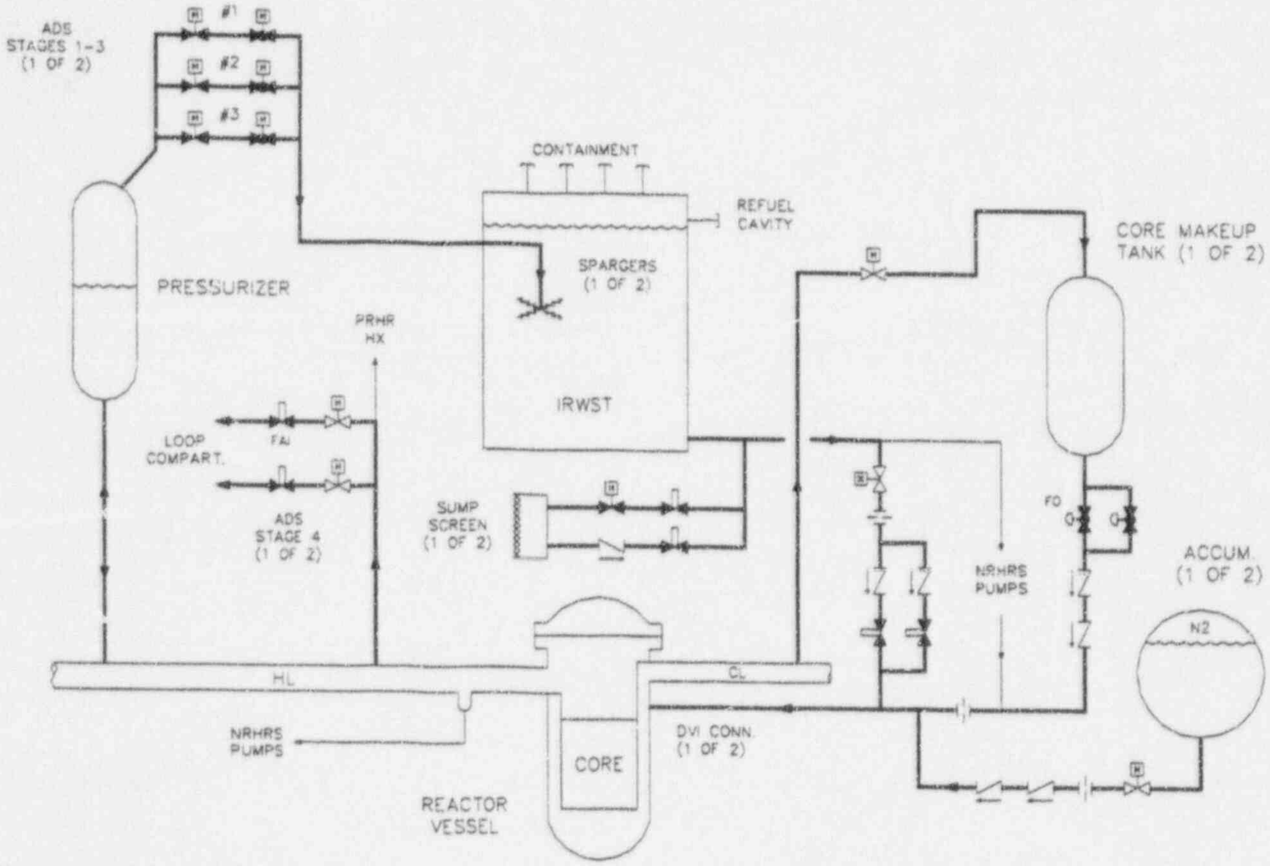


Figure 2.3-1 Passive Core Cooling System Sketch – RCS Injection Subsystem

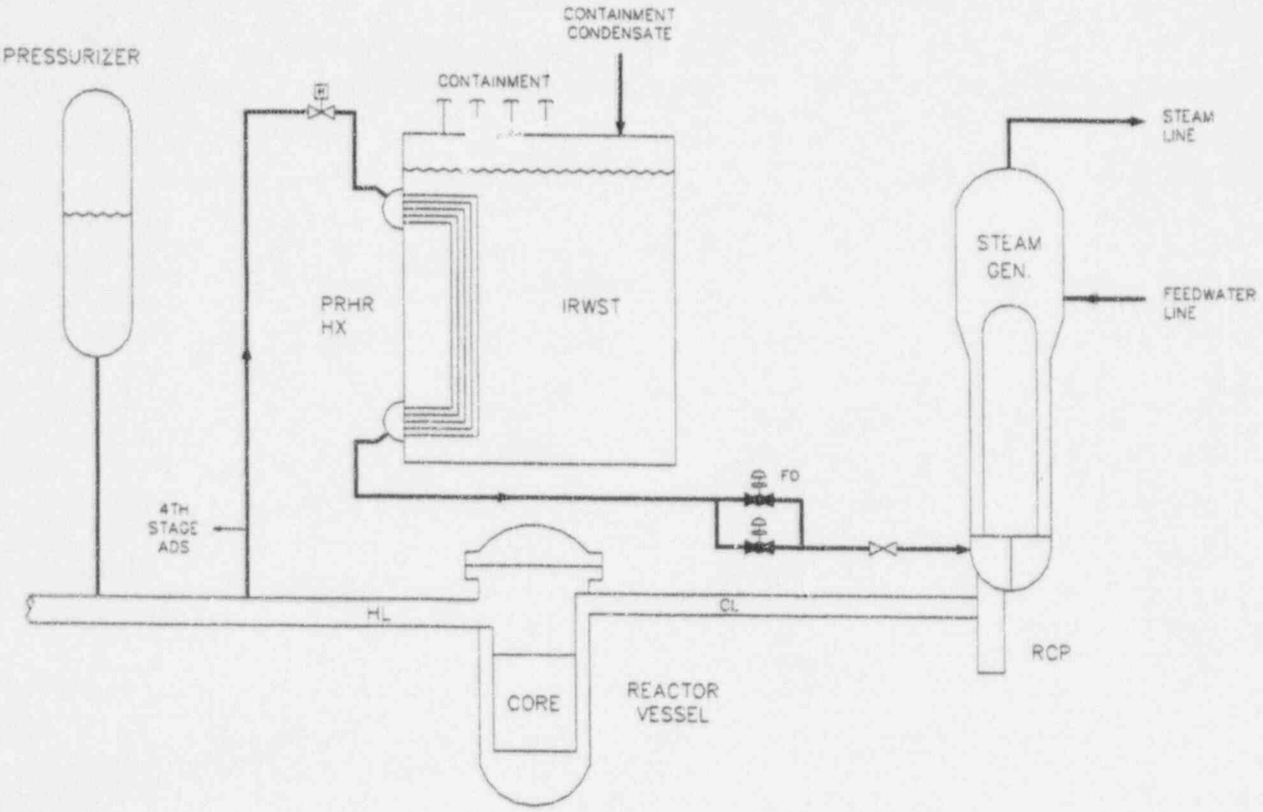


Figure 2.3-2 Passive Core Cooling System Sketch – Passive Residual Heat Removal Subsystem

The major subsystems of the PXS that are important to shutdown are described in the following subsections.

2.3.1.1 RCS Injection Subsystem

The RCS injection subsystem (Figure 2.3-1) consists of CMTs, accumulators, an IRWST, and associated valves, piping, and instrumentation.

The CMTs provide RCS makeup and boration for LOCAs and non-LOCAs when the normal makeup system is unavailable or insufficient. There are two CMTs located inside the containment at an elevation above the reactor coolant loops. During normal operation, the CMTs are completely full of cold, borated water. The boron concentration of the water is higher than that in the accumulators and the IRWST. The boration capability of these tanks provides adequate core shutdown margin following a steam line break and for safe shutdown events.

The CMTs are connected to the RCS through a discharge injection line and a cold leg inlet pressure balance line. The discharge line is blocked by two normally closed, parallel air-operated isolation valves that open on a loss of air pressure or electrical power. The cold leg pressure balance line is normally open.

The pressure balance line is normally open to maintain the CMTs at RCS pressure. The inlet lines contain normally open dc powered motor-operated valves (MOVs). The pressure balance line is well insulated and routed continuously upward from the top of the cold leg to a high point close to the top of the CMT. Water in the line will remain at or near the temperature of the cold legs, which will provide for natural circulation injection of the CMT water.

The outlet line from the bottom of each CMT provides an injection path to one of the two direct vessel injection lines, which are connected to the reactor vessel downcomer. Upon receipt of a safeguards actuation signal, the two parallel valves in each discharge line open to align the associated CMT to the RCS.

The CMTs can operate in two different modes, depending on the RCS conditions. If the cold legs are filled, then the CMTs will operate in a water recirculation mode with the driving force based on the density difference between hot water from the RCS cold leg versus the cold water initially in the CMT. If the cold legs become voided, as they do during LOCAs, the CMTs will operate in a steam drain down mode. In this mode, the driving force is based on the density difference between steam from the cold legs and water in the CMTs. The RCPs are tripped when the CMTs are actuated to allow steam and water to separate in the RCS and allow steam displacement drain down. As the CMTs drain, the ADS stages 1 through 3 valves are sequentially actuated on a low-1 CMT water level (~67 percent volume of span). As the CMTs continue to drain, the ADS stage 4 valves are actuated on a low-2 CMT water level (20 percent volume of span).

Downstream of the parallel discharge isolation valves, the CMT discharge line contains two check valves, in series, which are designed to be normally open even without flow. These valves prevent reverse flow through this line, from the accumulator, which would bypass the reactor vessel in the event of a larger LOCA in the cold leg or the cold leg pressure balance line. The use of normally open check valves improves the reliability of the CMT as modeled in the PRA.

An orifice in the CMT injection line allows for adjustment of the CMT injection flow rate. This orifice is located downstream of the CMT injection check valves. Between the check valves and the orifice is the connection from the RNS pumps. Upon decreasing CMT water level approaching the ADS actuation setpoint, the operators are instructed to start the RNS pumps to provide injection to the RCS. Operation of the RNS pumps increases the backpressure on the CMT such that its injection flow stops. Continued operation of the RNS pumps prevents actuation of the ADS stage 4 because the CMT level would not drop to the low level setpoint.

Although gas accumulation is not expected in the CMT inlet lines, vertical pipe stubs are located at the high point of each of the inlet lines to serve as gas collection chambers. Level detectors in each chamber indicate the presence of gases. There are provisions to allow the operators to locally open shielded manual valves to vent these gases to the reactor coolant drain tank during power operation.

The two accumulators contain borated water and a compressed nitrogen cover gas to provide rapid injection. They are located inside the reactor containment, and the discharge from each tank is connected to one of the direct vessel injection lines. These lines connect to the reactor vessel downcomer. A deflector is located in the downcomer at the end of the direct vessel nozzle to direct the PXS injection flow downward to minimize core bypass flow. The reactor vessel nozzles have a venturi shape which reduces the loss of reactor coolant in case of a break of the direct vessel injection (DVI) line and also minimizes the unrecovered pressure loss during PXS injection.

The accumulator water and gas volumes, and the discharge line resistance have been selected to provide a relatively long injection time, at least 2.5 minutes in a large LOCA. This long injection time reduces the injection flow required from the CMTs when they inject following emptying of the accumulators.

Each accumulator discharges through a normally open motor-operated isolation valve and two check valves in series. The check valves isolate the accumulators from the RCS during normal plant operation. An orifice is installed in the accumulator injection line to allow adjustment of the accumulator flow rate.

The IRWST contains cold borated water and is located in the containment at an elevation slightly above the RCS loop piping. The IRWST is connected to the RCS through two gravity injection lines, with each line connecting to a DVI line. Each gravity injection line is connected to the bottom of the IRWST and to a containment recirculation screen and contains a normally open motor-operated isolation valve and four isolation valves. The isolation valves are arranged in two parallel paths, each path having one squib valve backed up by one check valve. The squib valve provides leak-tight isolation and eliminates the normal back seating differential pressure across the check valve to thus reduce concerns of the check valves sticking. The check valve prevents a LOCA in case of an inadvertent opening of a squib valve. The IRWST injection valves are actuated on an ADS stage 4 actuation signal (low-2 CMT water level). In addition, for gravity injection during shutdown and reduced inventory operations, the IRWST squib valves are actuated on a two-out-of-two basis based on low (empty) hot leg water level.

The IRWST injection and the containment recirculation lines are protected by screens that prevent large particles from being injected to the reactor. These screens are designed to pass the maximum injection flow with one-half of their area blocked (as is required by Regulatory Guide 1.82) (Reference 2.3-2). The containment recirculation screens are located above the loop compartment floor elevation: one is in loop compartment A and the other is in the hallway between both loop compartments. Because of the large volume of IRWST and the minimum amount of open space below the RCS loops, there is no need for recirculation sumps.

Both containment recirculation paths are connected to an associated gravity injection line via two parallel flow paths. One path contains a squib valve backed up by a check valve. The other path contains a squib valve backed up by a normally closed motor-operated valve. The squib valves provide leak-tight isolation of the IRWST and eliminate the normal back seating differential pressure across the check valves. They also eliminate spillage of water into the containment and potential boric acid buildup during inservice testing of the MOVs. The containment recirculation paths are actuated on a low IRWST water level coincident with a safeguards actuation signal. The path with the MOV can also be opened to dump the IRWST water into the containment in case of an accident and complete failure to cool the core. Dumping the IRWST allows for cooling of the molten core while it is located inside the reactor vessel in severe accident scenarios.

2.3.1.2 Emergency Core Decay Heat Removal Subsystem

The emergency core decay heat removal subsystem consists of the PRHR HX and associated valves, piping, and instrumentation.

The heat exchanger is located in the IRWST, which provides the heat sink for the heat exchanger. The heat exchanger consists of a bank of C-tubes, connected at the top (inlet) and bottom (outlet) to a tubesheet and channel head that is mounted on the IRWST wall. The number of tubes installed provides for tube plugging margin. The PRHR HX is connected to the RCS through a normally open inlet line from one RCS hot leg. This line contains a normally open dc powered MOV. This line is shared with one of the fourth-stage automatic depressurization lines. The outlet line connects to the associated steam generator cold leg plenum (RCP suction). The outlet line contains normally closed air-operated valves that open on loss of air pressure or electrical power. These valves are opened on receipt of a PRHR actuation signal. Refer to SSAR chapter 7 (Reference 2.3-3) for a discussion of the plant parameters that actuate the PRHR HX.

The alignment of the PRHR HX (with a normally open inlet MOV and normally closed common outlet air-operated valves) maintains the heat exchanger full of reactor coolant at RCS pressure. The inlet line is well insulated and routed continuously upward from the top of the hot leg to a high point above the heat exchanger inlet. The water in the heat exchanger is stagnant and will be in thermal equilibrium with the water in the in-containment refueling water storage tank. This arrangement, which provides for the initial PRHR HX startup operation, maintains a thermal driving head during normal plant standby conditions.

The heat exchanger is elevated above the RCS loops to induce natural circulation flow through the heat exchanger when the RCPs are not available. The PRHR HX piping arrangement also allows actuation of the heat exchanger with RCPs operating. When the RCPs are operating, they provide forced flow in the same direction as natural circulation flow through the heat exchanger. If the pumps are operating and subsequently trip, then natural circulation provides the driving head for the heat exchanger flow.

Although gas accumulation is not expected, a vertical pipe stub is located on the top of the inlet piping high point that serves as a gas collection chamber. Level detectors in the chamber indicate if gases have collected. There are provisions to allow the operators to locally open shielded manual valves to vent these gases to the in-containment refueling water storage tank during power operation.

2.3.1.3 Valve Leak Test Subsystem

The PXS also includes a valve leak test panel which is used at shutdown conditions to leak test some RCS pressure boundary isolation valves. Four PXS valves and eight RNS valves are provided with connections that can be used to determine their seat leakage. All of these valves are located inside the containment. This testing is provided to reduce operational difficulties; it is not required by the inservice test program as discussed in SSAR subsection 3.9.6 (Reference 2.3-4).

The leak test is performed by pressurizing the RCS side of a valve and measuring the leak flow. For leak testing of MOVs and the first check valve interfacing with the RCS, the leak pressure is supplied by the RCS. As a result, these tests require the RCS to be pressurized to several hundred psig. For the second check valve from the RCS, the leak test pressure is supplied by the accumulators or the CVS makeup pumps through test lines provided as a part of this subsystem.

The test connection is routed to the test panel, which contains the small (3/8-inch) manual valves used to align the pressurization/leak flow test lines. It also contains a local flow meter and pressure gauge. The test valves are mounted such that their stems protrude through the front of the panel. The test valves are arranged and labeled to make it easy for the operator to align each test. The readouts of the local gauges are also on the panel.

The panel is placed in a location that is accessible during shutdown conditions.

2.3.2 Design Features to Address Shutdown Safety

A significant improvement in shutdown safety for the AP600 is the availability of a dedicated safety-related system that can be automatically or manually actuated in response to an accident that can occur during shutdown. In current plants, the safety-related systems that mitigate the consequences of an accident are also the front-line operating systems that are used for decay heat removal. In the AP600, nonsafety-related active systems provide the first level of defense, while the passive safety-related systems are available during shutdown modes to mitigate the consequences of an accident. This design approach results in the significant improvement in the AP600 shutdown risk, as quantified in the AP600 shutdown PRA (see PRA section 6) (Reference 2.3-5) and as demonstrated in the shutdown accident analysis provided in section 4 of this report.

Table 2.3-1 provides a summary of the availability of the passive safety-related systems during shutdown modes. The availability of the passive safety-related systems is controlled by the Technical Specifications (SSAR chapter 16) (Reference 2.3-6) and includes the availability of the mechanical components as well as appropriate automatic and/or manual actuations via the PMS. The availability of the PXS mechanical components and PMS instrumentation and controls is discussed in the following paragraphs.

2.3.2.1 Core Makeup Tanks

The CMTs provide RCS makeup. During shutdown, the CMTs are available in Modes 3, 4, and 5, until the RCS pressure boundary is open and the pressurizer water level is reduced. During power operation, the CMTs are automatically actuated on various signals including a

Table 2.3-1
Availability of Safety-related Components

Mode	ADS	CMT	PRHR HX	IRWST	Containment	Containment Cooling
Mode 1 - 4[1] Full power - safe shutdown	10 of 10 paths operable All paths closed	Both CMTs operable	PRHR HX operable	Both IRWST injection paths and both containment recirculating paths operable	Integrity	Both water flow paths operable
Mode 5 RCS pressure boundary closed	9 of 10 paths operable All paths closed	One CMT operable	PRHR HX operable	One IRWST injection path and one containment recirculating path operable	Closure [2]	
Mode 5 RCS pressure boundary open	Stages 1, 2, and 3 open; two Stage 4 paths operable	None	None	One IRWST injection path and one containment recirculating path operable	Closure [2]	Both water flow paths operable[3]
Mode 5 RCS pressure boundary open, reduced RCS inventory	Stages 1, 2, and 3 open; two Stage 4 paths operable	None	None	One IRWST injection path and one containment recirculating path operable	Closure [2]	Both water flow paths operable[3]
Mode 6 Reactor internals in place, refueling cavity not full	Stages 1, 2, and 3 open; two Stage 4 paths operable	None	None	One IRWST injection path and one containment recirculating path operable	Closure [2]	Both water flow paths operable[3]
Mode 6 Reactor internals removed, refueling cavity full	None	None	None	None	Closure [2]	None

[1] Both accumulators are required in Modes 1 through 3, above 1000 psig. The accumulators are not required in Modes 4 through 6.
[2] Containment closure is defined as the ability to close the containment prior to core uncovery following a loss of decay heat removal.
[3] PCS water flow paths required when shutdown is less than 100 hours.

safeguards actuation signal (low RCS pressure, low RCS temperature, low steam line pressure, and high containment pressure) and on low pressurizer water level. See SSAR chapter 7 (Reference 2.3-3) for a complete description of the AP600 PMS actuation logic. In shutdown modes, portions of the safeguards actuation signal are disabled to allow the RCS to be cooled and depressurized for shutdown. For instance, the low RCS pressure and temperature, and low steam line pressure signals are blocked in Mode 3 prior to cooling and depressurizing the RCS. Therefore, during shutdown Modes 3, 4, and 5, the primary signal that actuates the CMTs due to a loss of inventory is the pressurizer level signal. In Mode 5, with the RCS open (in preparation for reduced inventory operations), the low pressurizer level signal is blocked prior to draining the pressurizer. Therefore, in Mode 5 with the RCS open, the CMTs are not required to be available and the RCS makeup function is provided by the IRWST.

The CMTs also provide an emergency boration function for accidents such as steam line breaks. However, the signals that provide the primary protection for this function (low steam line pressure, low RCS pressure, and low RCS temperature) are blocked in Mode 3 as discussed above. Prior to blocking these signals in Mode 3, the Technical Specifications require that the RCS be sufficiently borated. For these events, the pressurizer level signal provides automatic actuation of the CMTs for a steam line break that might occur due to the RCS shrinkage that would occur. This event is discussed in more detail in subsection 4.2.3 of this report.

2.3.2.2 Accumulators

The PXS accumulators provide safety injection following a LOCA. In Mode 3, the accumulators must be isolated to prevent their operation when the RCS pressure is reduced to below their set pressure. The accumulator isolation valves are closed when the RCS pressure is reduced to 1000 psig to block their injection when the RCS pressure is reduced to below the normal accumulator pressure. Analysis is provided in section 4.7 of this report that shows the plant response to LOCAs that could occur at shutdown without the accumulators aligned.

2.3.2.3 In-containment Refueling Water Storage Tank

The IRWST provides long-term RCS makeup. During shutdown, the IRWST is available until Mode 6, when the reactor vessel upper internals are removed and the refueling cavity flooded. At that time, the IRWST is not required, due to the large heat capacity of the water in the refueling cavity.

The IRWST injection paths are actuated on a low-2 CMT water level. This signal is available in shutdown Modes 3, 4, and 5, with the RCS intact. When the RCS is open to transition to reduced inventory operations, the CMT actuation logic on low pressurizer level is removed, and the CMTs can be taken out of service. For these modes, automatic actuation of the IRWST can be initiated (on a two-out-of-two basis) on low hot leg level. However, manual actuation of the IRWST is relied upon to meet the design basis safety analysis case provided in section 4 of this report for loss of inventory/cooling events that occur during these conditions.

2.3.2.4 Passive Residual Heat Removal Heat Exchanger

The PRHR HX provides decay heat removal during power operation and is required to be available in shutdown Modes 3, 4, and 5, until the RCS is open. In these modes, the PRHR HX provides a passive decay heat removal path. It is automatically actuated on a CMT actuation signal, which would eventually be generated on a loss of shutdown decay heat removal, as shown in the analysis provided in section 4 of this report. In modes with the RCS open (portions of Mode 5 and Mode 6), decay heat removal is provided by "feeding" water from the IRWST and "bleeding" steam from the ADS.

2.3.2.5 Reduced Challenges to Low-Temperature Overpressure Events

Another design feature of the PXS that reduces challenges to shutdown safety is the elimination of high-head safety injection pumps in causing low temperature overpressure events. In current plants, during water solid operations that may be necessary to perform shutdown maintenance, the high-head safety injection pumps are a major source of cold overpressure events. To address this, plants are required to lock out safety injection pumps to prevent them from inadvertently causing a cold overpressure event. This eliminates a potential source of safety injection for a loss of inventory event that could occur at shutdown. With the AP600 PXS, the CMTs are never pressurized above RCS pressure and are, therefore, not capable of causing a cold overpressure event. Therefore, they are not isolated until the pressurizer is drained for mid-loop. Low-temperature overpressure events are discussed in section 4.10.1 of this report.

2.3.2.6 Discussion of Safe Shutdown for AP600

The functional requirements for the PXS specify that the plant be brought to a stable condition using the PRHR HX for events not involving a loss of coolant. For these events, the PXS, in conjunction with the passive containment cooling system (PCS), has the capability to establish long-term safe shutdown conditions, cooling the RCS to less than 420°F within 36 hours, with or without the RCPs operating.

The CMTs automatically provide injection to the RCS as the temperature decreases and the pressurizer level decreases, actuating the CMTs. The PXS can maintain stable plant conditions for a long time in this mode of operation, depending on the reactor coolant leakage and the availability of ac power sources. For example, with a technical specification leak rate of 10 gpm, stable plant conditions can be maintained for at least 10 hours. With a smaller leak, a longer time is available. However, in scenarios when ac power sources are unavailable for as long as 24 hours, the ADS will automatically actuate.

For LOCAs and other postulated events where ac power sources are lost, or when the CMT levels reach the ADS actuation setpoint, the ADS initiates. This results in injection from the accumulators and subsequently from the in-containment refueling water storage tank, once the RCS is nearly depressurized. For these conditions, the RCS depressurizes to saturated conditions at about 240°F within 24 hours. The PXS can maintain this safe shutdown condition indefinitely for the plant.

The basis used to define the PXS functional requirements is derived from section 7.4 of the *Standard Review Plan* (Reference 2.3-7). The functional requirements are met over the range of anticipated events and single failure assumptions. The primary function of the PXS during a safe shutdown using only safety-related equipment is to provide a means for boration, injection, and core cooling. Analysis is provided in subsection 4.10.2 of this report that verifies the ability of the AP600 passive safety systems to meet the safe shutdown requirements discussed previously.

2.3.3 Shutdown Operations

During shutdown operations at reduced temperatures and pressures, the PXS continues to provide core cooling capability. As the RCS temperature and pressure are reduced, some of the PXS features are isolated to prevent interaction with normal operation or to allow for PXS equipment maintenance as discussed previously.

2.3.3.1 Operation During Loss of Startup Feedwater During Hot Standby and Cooldown and Heatup Events

During normal cooldowns, the steam generators are supplied by the startup feedwater pumps and steam from the steam generator is directed either to the main condenser or to the atmosphere. There are two nonsafety-related diesel-generators in the event offsite power is lost. However, because the startup feedwater pumps are nonsafety-related, their failure is considered.

In the event of a loss of startup feedwater, the PRHR HX is automatically actuated on low steam generator water level to provide safety-related heat removal. The PRHR HX can maintain the RCS temperature, as well as provide for RCS cooldown to conditions where the RNS can be operated.

Because the CVS makeup pumps are nonsafety-related, they may also not be available. In this case, the CMTs automatically actuate as the cooldown continues and the pressurizer level decreases. The CMTs operate in a water recirculation mode to maintain RCS inventory while the PRHR HX operates.

The IRWST provides the heat sink for the PRHR HX. Initially, the heat addition increases the water temperature. Within 1 to 2 hours, the water reaches saturation temperature and begins to boil. The steam generated in the IRWST discharges to containment. Because the containment integrity is maintained during cooldown (Mode 4 and above), the PCS provides the safety-related ultimate heat sink. The:efore, most of the steam generated in the IRWST is condensed on the inside of the containment vessel and drains back into the IRWST via the condensate return gutter arrangement. This allows it to indefinitely function as a heat sink.

2.3.3.2 Operation During Loss of Normal Residual Heat Removal Cooling During Cold Shutdown With the Reactor Coolant System Pressure Boundary Intact

During normal shutdown conditions, the RNS is placed into service at about 350°F to accomplish RCS cooldown to refueling temperatures. Heat removed by the RNS is transferred to the component cooling water system (CCS) and then to the service water system. The entire heat removal path is powered by the nonsafety-related diesel generators in the event that offsite power is lost.

The RNS piping is safety-related and meets seismic Category I requirements to prevent pipe breaks that could result in a significant loss of reactor coolant during system operations. The RNS is designed so that with the single failure of an active component, it can maintain the plant in a hot shutdown condition (<350°F). It is also possible to perform an RCS cooldown, but at a slower rate than with full system capability. However, the pump motors and the electrical power supplies are nonsafety-related.

The RNS and its support systems are designed to be reliable. However, because they are not safety-related systems, their failure has to be considered. When the RCS pressure boundary is intact, the PRHR HX provides the safety-related heat removal flow path when the RNS is unavailable.

The PRHR HX is capable of functioning at low RCS temperatures and pressures. Their operation may result in a small increase in the RCS temperature, depending on the initial RCS conditions and decay heat values. They can remove sufficient heat to maintain the RCS within the RNS design limits (400°F). This permits the RNS to be placed back in operation when it becomes available.

With a loss of RNS cooling during shutdown operations, the RCS temperature will increase, which will result in an increase in pressure. Without operator action, the RNS relief valve would open. Continued operation would lead to automatic CMT and PRHR HX actuation on low pressurizer level.

For this event, RCS makeup can be provided by the CVS makeup pumps. They would provide automatic makeup, starting on a low pressurizer level and stopping on a higher level. However, their unavailability must be considered because they are nonsafety-related. Safety-related makeup is provided by the CMTs operating in the water recirculation mode. The CMTs would be automatically actuated as described previously.

2.3.3.3 Operation During Loss of Normal Residual Heat Removal Cooling During Mid-loop Events

During RCS maintenance, the most limiting shutdown condition anticipated is with the reactor coolant level reduced to the hot leg (mid-loop) level and the RCS pressure boundary opened. It is normal practice to open the steam generator channel head manway covers to install the hot leg and cold leg nozzle dams during a refueling outage. In this situation, the RNS is used to cool the RCS. The AP600 incorporates many features to reduce the probability of losing RNS. However, because the RNS is nonsafety-related, its failure has been considered.

In this situation, core cooling is provided by the safety-related PXS, using gravity injection from the IRWST, while venting through the ADS valves (and possibly through other openings in the RCS). Note that with the RCS depressurized and the pressure boundary opened, the PRHR HX is unable to remove the decay heat because the RCS cannot heat sufficiently above the IRWST temperature.

During plant shutdown, at 1000 psig, the accumulators are isolated to prevent inadvertent injection. Prior to draining the RCS inventory below the no-load pressurizer level, the CMTs are isolated by closing the inlet MOVs to preclude inadvertent draining into the RCS while preparing for mid-loop operation. Although these tanks are isolated from the RCS, the valves can be remotely opened by the operators to provide additional makeup water injection.

Prior to initiating the draindown of RCS to mid-loop level, the automatic depressurization first-, second-, and third-stage valves are opened. This alignment provides a sufficient RCS vent flow path to preclude system pressurization in the event of a loss of nonsafety-related decay heat removal during mid-loop operation. The ADS first- to third-stage valves are required to be opened before blocking the CMTs. They are required to remain open until either the RCS level is increased and the RCS is closed, or until the upper core internals are removed and the refueling cavity flooded. Note that the upper internals can restrict the vent flow path and prevent water in the refueling cavity from draining into the RCS unless ADS valves are open. With the CMTs blocked, there is no automatic actuation of the ADS valves.

The IRWST injection squib valves are automatically opened if the RCS hot leg level indication decreases below a low setpoint. A time delay is provided to provide time for the operators to restore nonsafety-related decay heat removal prior to actuating the PXS. The time delay with an alarm in the containment serves to protect maintenance personnel. Once the IRWST injection valves open, the IRWST provides gravity-driven injection to cool the core. Containment recirculation flow would be automatically initiated when the IRWST level dropped to a low level to provide long-term core cooling.

Subsection 4.8.5 provides the analysis of the loss of the RNS during mid-loop operations. Table 2.3-2 provides the results of calculations performed to demonstrate the amount of time between a loss of RNS that could occur at mid-loop until core uncovery. This calculation is performed with the RCS water level at the nominal mid-loop water level and is performed with conservative, design basis assumptions for decay heat. As described previously and shown in Table 2.3-2, the operators have a significant amount of time to actuate gravity injection before core uncovery. In addition, the PMS, on a two-out-of-two basis, provides a signal to actuate the IRWST when the hot legs empty.

This arrangement provides automatic core cooling protection, in mid-loop operation, while also providing protection (an evacuation alarm and sufficient time to evacuate) for maintenance personnel in containment during mid-loop operation.

Containment closure capability is required to be maintained during mid-loop operation, as discussed in subsection 2.6.2 of this report. With the containment closed, containment recirculation can continue indefinitely with decay heat generating steam condensed on the containment vessel and drained back into the IRWST and/or the containment recirculation.

2.3.3.4 Operation During Loss of Normal Residual Heat Removal Cooling During Refueling

The RNS is normally used for decay heat removal during refueling operation. Its failure is considered because it is not a safety-related system. In this case, it is assumed that the reactor vessel head is removed and the water from the IRWST has been transferred to the refueling cavity, which is flooded to its high-level condition. The PRHR HX is not available and containment integrity is expected to be relaxed with air locks and/or equipment hatches open.

Table 2.3-2
Evaluation of a Loss of RNS at Mid-loop with no IRWST Injection

Time After Shutdown	Time to Boiling	Time to Empty Hot Leg	Time to Core Uncovery
28 hours	17 minutes	59 minutes	102 minutes

Assuming that the refueling cavity has just been flooded when the RNS system fails, the refueling cavity water heats up to saturation temperature in approximately 9 hours. Boiling reduces the water level to the top of the fuel assemblies in approximately 5 days, assuming that the containment is not closed. If the containment is closed, water will not be lost from containment and long-term cooling can be maintained without a subsequent need for cooling water makeup.

Continued core cooling can be easily maintained by one of several methods. With the slow heatup of the refueling cavity water, there is ample time to close containment before the significant steaming to containment begins. In addition, there are multiple nonsafety-related systems – such as the CVS, the SFS, the demineralized water system, and the fire system – which can add water to the containment in this situation. In addition, temporary water supplies such as fire trucks can also supply water to containment.

2.3.4 References

2.3-1 *AP600 Standard Safety Analysis Report,* Chapter 6, "Engineered Safety Features."

2.3-2 *NRC Regulatory Guide 1.82,* "Water Sources for Long-Term Recirculation Cooling Following a Loss-of-Coolant Accident," Revision 2, May 1996.

2.3-3 *AP600 Standard Safety Analysis Report,* Chapter 7, "Instrumentation and Controls."

2.3-4 *AP600 Standard Safety Analysis Report,* Chapter 3, "Design of Structures, Components, Equipment, and Systems."

2.3-5 *AP600 Probabilistic Risk Assessment,* Chapter 6, "Success Criteria Analysis," September 30, 1996.

2.3-6 *AP600 Standard Safety Analysis Report,* Chapter 16, "Technical Specifications."

2.3-7 NUREG-0800, *Standard Review Plan,* July 1981.

2.4 NORMAL RESIDUAL HEAT REMOVAL SYSTEM

2.4.1 System Description

The RNS is discussed in section 5.4.7 of the SSAR (Reference 2.4-1). The RNS consists of two mechanical trains of decay heat removal equipment. Each train includes one RNS pump and one RNS heat exchanger located in the auxiliary building. The two trains of equipment share a common suction line from the RCS and a common discharge header which splits inside containment to return the flow to the RCS via the two PXS DVI lines. The RNS has direct connections to the spent fuel pool to allow its use to supplement or replace the normal SFS cooling. The RNS is also interconnected with the IRWST and the CVS to accomplish other support functions such as water transfer. In addition, the RNS includes the piping, valves, and instrumentation necessary for correct system operation. Figure 2.4-1 is a simplified sketch of the RNS (SSAR Figure 5.4-6).

The portions of the RNS piping that perform the reactor coolant pressure boundary outside containment have a design pressure and temperature such that full RCS system pressure is below the ultimate rupture strength of the piping. This feature greatly reduces the risk of a LOCA outside containment.

The RNS suction header is connected to an RCS hot leg with a single step-nozzle connection. The step-nozzle connection is used to minimize the likelihood of air induction into the RNS pumps during RCS reduced inventory operations (including RCS levels near the centerline of the hot leg pipe). The step-nozzle consists of a short section of 20-inch schedule 160 pipe attached to the hot leg (straight down from the bottom of the pipe) and connected by a reducer to the RNS suction line.

The suction header then branches into two parallel lines with each line containing two normally closed, motor-operated isolation valves in series which serve as reactor coolant pressure boundary valves. RCS pressure boundary isolation and decay heat removal initiation occur by allowing RNS initiation following a single failure of an isolation valve to open and also by allowing for RNS isolation following a single failure of an isolation valve to close. The isolation valve in each pair closest to the containment penetration also serves as a containment isolation valve. Each RNS/RCS suction isolation valve receives power from a class 1E power supply (125 Vdc) and is interlocked with RCS pressure to prevent the operator from opening the valve until RCS pressure is at or below the normal operating pressure of the RNS. These valves are also interlocked to prevent opening unless the isolation valves are closed from the IRWST to the RNS pump suction header and from the RNS pump discharge header to the IRWST. In addition, the power supply to each valve is blocked at the valve's motor control center during plant power operations. There is one check valve in both pressure relief lines between each pair of suction isolation valves from

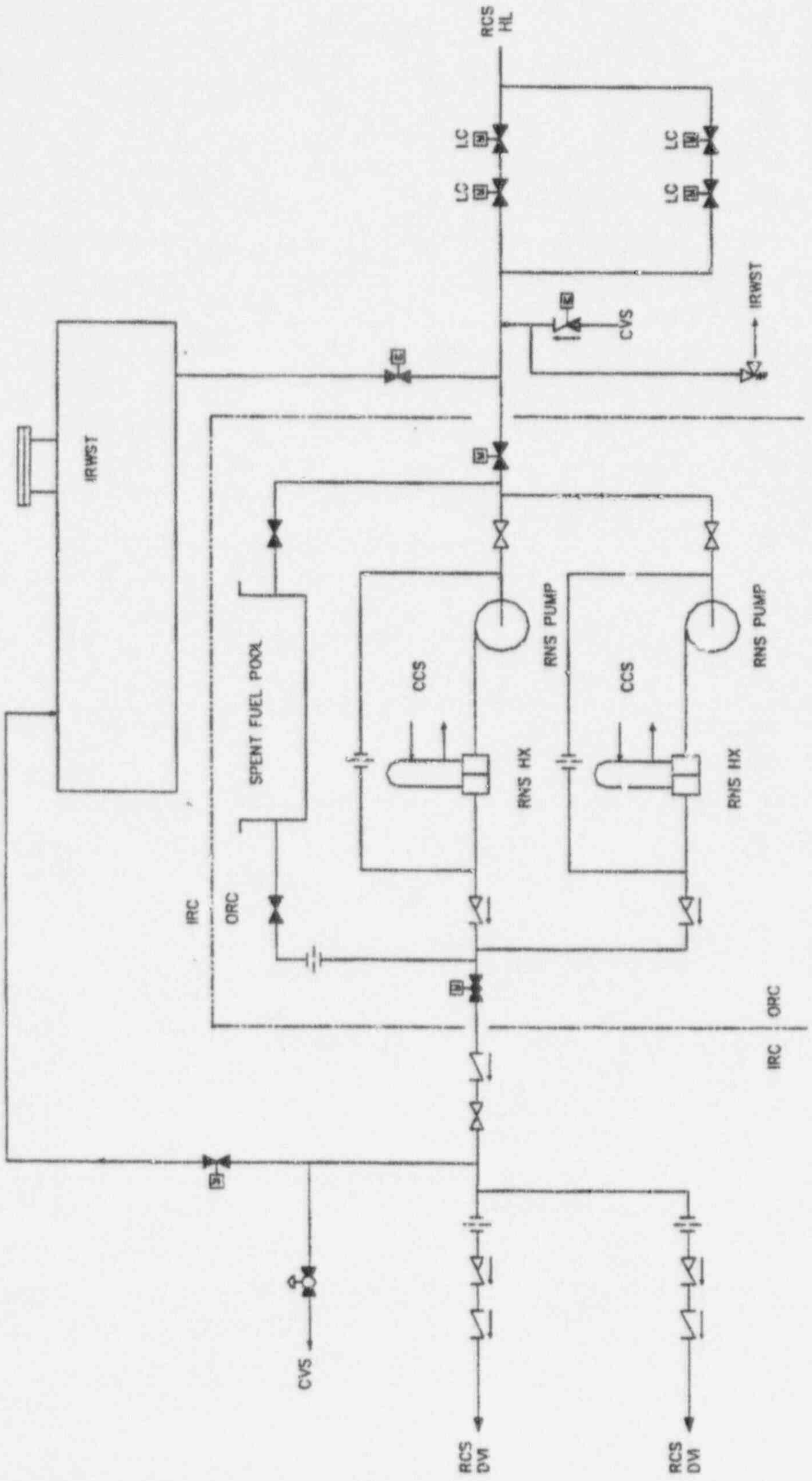


Figure 2.4-1 Normal Resi[illegible] Heat Removal System

the RCS. These check valves prevent the expansion of trapped water between the suction isolation valves from overpressurizing the valves and piping by relieving water back to the RCS. In addition, test connections are provided to perform leak rate testing of the RCS pressure boundary valves.

The lines are then joined into a common suction line inside containment. A single line from the IRWST is connected to the suction header upsteam of the containment penetration. The IRWST line contains one normally closed, motor-operated isolation valve which automatically closes on a high containment radiation signal for containment isolation.

In addition, the common RNS suction header inside containment serves as the return point (for eventual discharge to the RCS) for CVS flow during plant startup and shutdown operations when the RCPs are not operating (to enhance coolant mixing) and when nozzle dams are installed in steam generator RCS-MB01 for maintenance.

Immediately downstream of the RCS suction isolation valves is one pressure relief valve which protects the RNS from overpressurization by discharging to the IRWST during system operations when pressure in the suction line exceeds 563 psig. This relief valve also provides low temperature overpressure protection for the RCS components when the RNS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations.

Once outside containment, the suction header contains a single, normally closed, motor-operated isolation valve which also automatically closes on a high containment radiation signal for containment isolation. The RNS piping from the RCS up to and including this valve is designed for full RCS pressure. Downstream of the suction header isolation valve, the header branches into two separate lines, one to each pump. Each branch line has a normally open manual isolation valve upstream of the RNS pumps. This valve is provided for pump maintenance.

The RNS suction header has a continuous downward slope from the RCS hot leg to the pump suction. This eliminates any local high points where air could collect and cause a loss of residual heat removal capability due to RNS pump cavitation. This design feature has been incorporated because of mid-loop operation concerns. If the RNS pumps are stopped because of air-entrainment, this piping configuration allows the line to self-vent and immediately refill with water. The pumps can then be restarted once an adequate RCS water level is attained.

The discharge of each RNS pump is routed directly to its respective RNS heat exchanger. Immediately downstream of each pump is a pressure sensor with transmitter for main control room indication of pump discharge pressure. Upstream of each RNS heat exchanger is a temperature element with a transmitter for indication in the main control room to monitor RNS heat exchanger inlet temperature. This temperature instrument is also used for control of the flow of cooling water to the heat exchanger.

The discharge line from each RNS heat exchanger also has a temperature element, with a transmitter for indication in the main control room, to monitor RNS heat exchanger outlet temperature. A flow element with a transmitter provides indication and high and low alarm in the main control room to monitor RNS heat exchanger flow.

A miniflow line and orifice from the RNS heat exchanger outlet to the RNS pump suction are included for pump protection. This line is sized to provide a sufficient pump flow when the pressure in the RCS is above the RNS pump shutoff head.

The outlet of each RNS heat exchanger is routed to a common discharge header, which contains a normally closed, motor-operated isolation valve outside of the containment penetration. This valve closes automatically upon receipt of a high containment radiation signal for containment isolation. Upstream of the isolation valve in the common discharge header is a relief valve (that discharges to the effluent holdup tank) to protect the RNS discharge piping and equipment against overpressurization due to any RCS leakage or thermal expansion of trapped water.

Inside containment, the common discharge header contains a check valve which acts as a containment isolation valve. Downstream of the check valve, the discharge header branches into two lines routed to each PXS DVI line. These branch lines each contain a pressure-reducing orifice to provide the backpressure required to deliver the required purification flow through the cross-connect line to the CVS letdown heat exchanger. The RNS to RCS pressure boundary consists of a stop check valve followed by a check valve in series. Also branching from one of the DVI lines is a line to the CVS demineralizers which is used for shutdown purification of the RCS. Another line is routed from the discharge header to the IRWST for cooling operations.

The connections to the spent fuel pool are normally isolated by locked closed gate valves. These valves are opened only for abnormal situations where the RNS is used for spent fuel pool cooling. The line from the RNS discharge to the spent fuel pool includes a flow restricting orifice flange set to prevent pump runout. Spent fuel pool cooling by the RNS is permitted during normal plant power operation and also during shutdown when the entire reactor core has been off-loaded into the pool.

2.4.2 Design Features to Address Shutdown Safety

The AP600 has incorporated various design features to improve shutdown safety. The RNS features that have been incorporated to address shutdown safety are described in this subsection.

2.4.2.1 RNS Pump Elevation and NPSH Characteristics

The AP600 RNS pumps are located at the lowest elevation in the auxiliary building. This location provides the RNS pumps with a large available NPSH during all modes of operation including RCS mid-loop and reduced inventory operations. The large NPSH provides the pumps with the capability to operate during mid-loop conditions with saturated fluid in the RCS without throttling the RNS flow. This allows for the RNS pumps to be restarted and operated with saturated RCS conditions that might occur following a temporary loss of RNS cooling.

The plant piping configuration, piping elevations and routing, and the pump characteristics allow the RNS pumps to be started and operated at their full design flow rates without the need to reduce RNS pump flow to meet pump NPSH requirements. This eliminates the potential failure mechanism that exists in current PWRs, where failure of an air-operated control valve can result in pump runout and cavitation during mid-loop operations.

2.4.2.2 Self-Venting Suction Line

The RNS pump suction line is sloped continuously upward from the pump to the RCS hot leg with no local high points. This eliminates potential problems with refilling the pump suction line if an RNS pump is stopped due to pump cavitation and/or excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

2.4.2.3 IRWST Injection via the RNS Suction Line

During shutdown modes, initiating events such as the loss of the nonsafety-related RNS are postulated to occur. Such events would require IRWST injection as discussed in section 2.3 of this report, and as shown in the accident analyses provided in section 4 of this report. For initiating IRWST injection, the operation of PXS squib valves in the IRWST injection line is required. However, the operators can use the RNS pump suction line that connects to the IRWST to provide controlled IRWST injection. This flow path, shown in Figure 2.4-2, connects the IRWST directly to the RCS via the RNS hot leg suction isolation valves and provides a diverse method for IRWST injection. In addition, it would be the preferred method of providing IRWST injection because the flow would be controllable by the operation of the IRWST suction line isolation valve. This path provides IRWST injection regardless of whether the RNS pumps are operating.

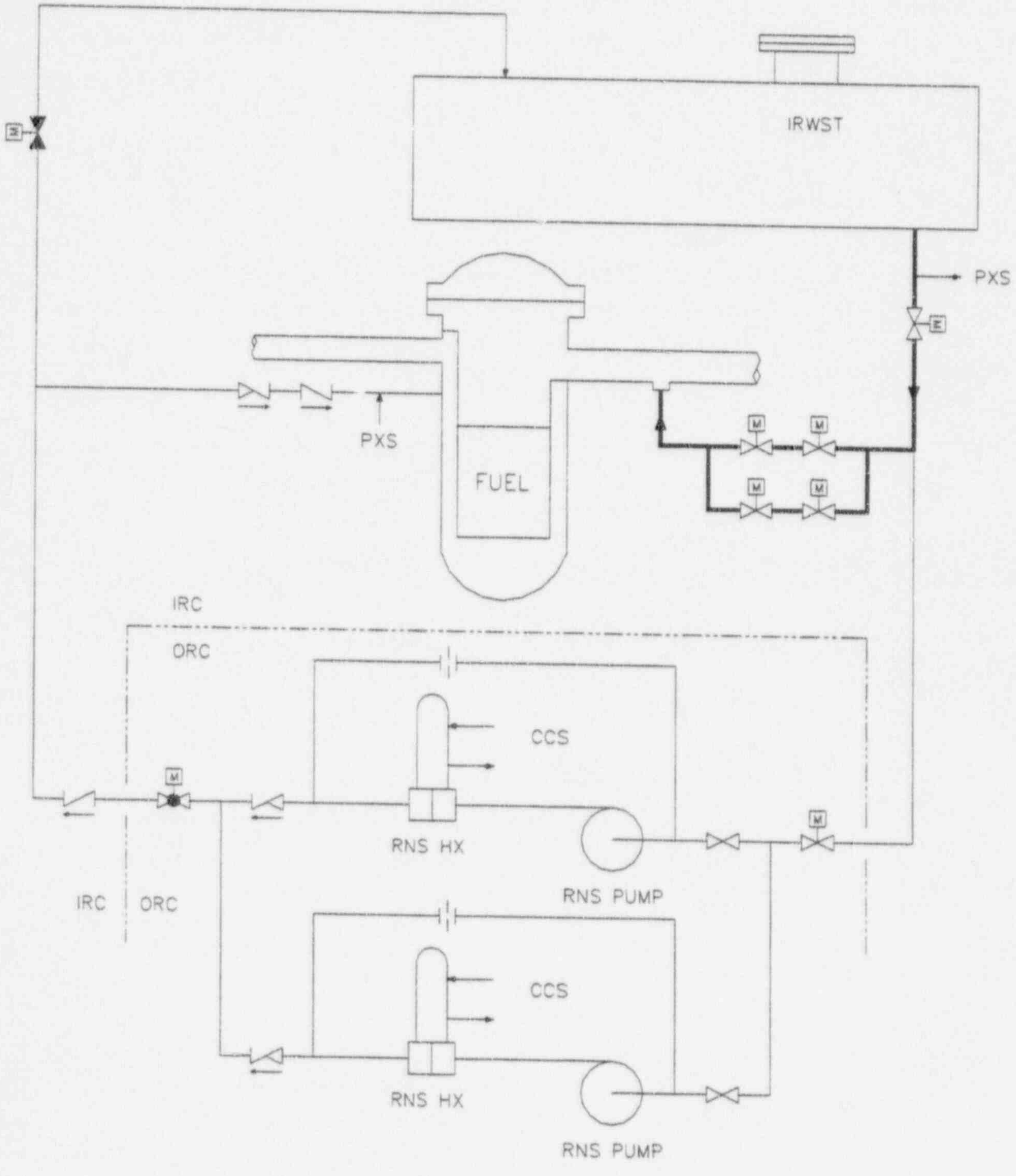


Figure 2.4-2 IRWST Injection Flow Path

2.4.2.4 Codes and Standards/ Seismic Protection

The portions of the RNS located outside containment (that serve no active safety functions) are classified as AP600 equipment Class C so that the design, manufacture, installation, and inspection of this pressure boundary is in accordance with the following industry codes and standards and regulatory requirements: 10 CFR 50, Appendix B (Reference 2.4-2); Regulatory Guide 1.26, quality group C (Reference 2.4-3); and ASME Boiler and Pressure Vessel Code, Section III, Class 3 (Reference 2.4-4). The pressure boundary is classified as seismic Category I.

2.4.2.5 Increased Design Pressure

The portions of the RNS from the RCS to the containment isolation valves outside containment are designed to the operating pressure of the RCS. The portions of the system downstream of the suction line containment isolation valve and upstream of the discharge line containment isolation valve are designed so that its ultimate rupture strength is not less than the operating pressure of the RCS. Specifically, the piping is designed as schedule 80S, and the flanges, valves, and fittings are specified to be greater than or equal to ANS class 900. The design pressure of the RNS is 900 psig, which is 40 percent of operating RCS pressure.

2.4.2.6 Reactor Coolant System Isolation Valve

The RNS contains an isolation valve in the pump suction line from the RCS. This motor-operated containment isolation valve is designed to the RCS pressure. It provides an additional barrier between the RCS and lower pressure portions of the RNS.

2.4.2.7 Normal Residual Heat Removal System Relief Valve

The inside containment RNS relief valve is connected to the residual heat removal pump suction line. This valve is designed to provide low-temperature, overpressure protection of the RCS as described in SSAR section 5.2.2 (Reference 2.4-1). The valve, connected to the high-pressure portion of the pump suction line, reduces the risk of overpressurizing the low-pressure portions of the system.

2.4.2.8 Features Preventing Inadvertent Opening of Isolation Valves

The RCS isolation valves are interlocked to prevent their opening at RCS pressures above 450 psig. SSAR section 7.6 (Reference 2.4-5) discusses this interlock. The power to these valves is administratively blocked during normal power operation.

In addition, these valves are interlocked with the RNS/IRWST isolation valves to prevent their opening with the RNS open to the IRWST. This precludes the blowdown of the RCS to the IRWST through the RNS upon system initiation.

2.4.2.9 RCS Pressure Indication and High Alarm

The AP600 RNS contains an instrumentation channel that indicates pressure in each normal residual heat removal pump suction line. A high-pressure alarm is provided in the main control room to alert the operator to a condition of rising RCS pressure that could eventually exceed the design pressure of the RNS.

2.4.3 Shutdown Operations

The operation of the RNS for the pertinent phases of plant operation is described in the following subsections. All system operations are controlled and monitored from the main control room, including mid-loop operations. The RCS is equipped with mid-loop level instrumentation with remote indication in the main control room. This instrumentation is used for monitoring mid-loop operations from the main control room.

2.4.3.1 Plant Startup

Plant startup is defined as the operations that bring the reactor plant from a cold shutdown condition to no-load operating temperature and pressure, and subsequently to power operation.

During cold shutdown conditions, RNS pumps and heat exchangers operate to circulate reactor coolant and remove decay heat. The RNS pump(s) are stopped when plant startup begins. The RNS remains aligned to the RCS to maintain a low-pressure letdown path to the CVS. This alignment provides RCS purification flow, low-temperature over-pressure protection of the RCS, and RCS low-pressure control when the RCPs are not operating. As the RCPs are started, their thermal input begins heating the reactor coolant inventory. Once the pressurizer steam bubble formation is complete, the RNS suction header isolation valves and the discharge header isolation valve are closed and tested for leakage. The valve arrangement is then set for normal power operation as shown in Figure 2.4-1.

2.4.3.2 Normal Cooldown

Plant cooldown is defined as the operation that brings the reactor plant from normal operating temperature and pressure to cold (ambient) conditions.

The RNS removes decay heat from the core and reduces the temperature of the RCS during the second phase of plant cooldown. The first phase of cooldown is accomplished by transferring heat from the RCS via the steam generators to the MSS. Following cooldown, the RNS continues to remove decay heat from the core during the entire plant shutdown until the plant is started up again.

The initial phase of plant cooldown consists of reactor coolant cooling and depressurization via the steam generators. Heat is transferred from the RCS to the MSS where the rate of steam dump is controlled to establish an RCS cooldown rate of approximately 50°F/hr. Depressurization is accomplished by spraying reactor coolant into the pressurizer, which cools and condenses the pressurizer steam bubble.

When the reactor coolant temperature and pressure have been reduced to 350°F and 450 psig respectively (approximately 4 hours after reactor shutdown), the second phase of plant cooldown is initiated with the RNS being placed in service.

Prior to starting the RNS pumps, the IRWST isolation valve is verified to be closed. The RNS suction header isolation valve and the discharge header isolation valve are then opened. When the pressure in the RCS has been reduced to below 450 psig, the inner/outer suction isolation valves are opened.

Once the proper valve alignment has been performed, and CCS flow is available to both RNS heat exchangers, RNS operation may begin.

Initially only one RNS pump and heat exchanger are started. Later, when the RCS cooling rate is restricted due to the temperature difference in the heat exchanger, the second RNS pump is started and the cooldown proceeds in accordance with the AP600 refueling outage plan. The cooldown rate is limited by the CCS flow being throttled through the shellside of both heat exchangers by CCS control/isolation valves. Operation of the system in this manner limits the RCS cooldown rate to less than 75°F/hr. RNS cooling continues for the duration of the cooldown until the RCS temperature is reduced to 140°F and the system is depressurized. The RCS may then be opened for either maintenance or refueling. Cooldown continues until the RCS temperature is lowered to 120°F (approximately 96 hours after reactor shutdown).

The system is designed so that any single failure of an active component during normal cooldown will not preclude the ability to cool down, but will lengthen the time required to reach 120°F. Furthermore, if a single failure occurs while the reactor vessel head is removed, the reactor coolant temperature remains below boiling.

2.4.3.3 Refueling Heat Removal

Following cooldown, the RNS removes heat from the core and the RCS during refueling operations. The system maintains the RCS at a temperature less than or equal to 120°F indefinitely.

Both RNS pumps and heat exchangers remain operating during refueling. All water transfers from the IRWST to the refueling cavity are performed by the SFS. This function has traditionally been performed by residual heat removal systems and that capability is available if the need arises. Using the RNS would involve flooding the refueling cavity through the reactor vessel. This method has contributed to clarity problems in the refueling cavity and has caused additional occupational radiation exposure (ORE). Therefore, the SFS is used to flood the refueling cavity without flooding through the reactor vessel.

As decay heat decreases and as fuel is moved to the spent fuel pool, one RNS pump and heat exchanger may eventually be taken out of service. All valves will remain aligned if the need would arise to start the standby pump quickly in case of a failure of the operating RNS pump.

2.4.3.4 IRWST Cooling

The RNS provides cooling for the IRWST during operation of the PRHR HX or during normal plant operations when required. The system is manually initiated by the operator within 2 hours of initiation of the PRHR HX. The RNS is designed to limit the IRWST water temperature to less than boiling during extended operation of the PRHR HX or to limit the IRWST water temperature to 120°F during normal operation.

2.4.3.5 Spent Fuel Pool Cooling

The RNS provides the capability of supplementing or taking over the normal cooling function of the SFS. With a failure of the one SFS train with a full-core off-load into a pool occupied by 10 years of spent fuel, one train of RNS is used to supplement the cooling and the pool temperature is maintained less than 120°F. When used to replace the normal SFS cooling, one RNS train is sufficient to maintain the spent fuel pool below boiling.

2.4.3.6 Post-Accident Closed Loop Cooling

Following an accident including all stages of ADS and IRWST injection, the RNS can be aligned to provide decay heat removal. For this mode of operation, the RNS can take suction from the PXS containment recirculation sump and inject into the direct vessel injection lines.

2.4.3.7 Low Pressure RCS Makeup

Makeup from IRWST

The RNS is capable of providing low-pressure makeup froni the IRWST to the RCS. The system is designed to be manually initiated by the operator following receipt of an ADS signal. If the system is available, it will provide RCS makeup once the pressure in the RCS falls below the shutoff head of the RNS pumps.

Following an ADS signal where a LOCA has not occurred, the RNS, if available, is designed to provide sufficient makeup flow such that the water level in the CMTs does not drain below the fourth-stage automatic depressurization valve setpoint. In this way, successful operation of the RNS will prevent the fourth-stage ADS valves (located off the RCS hot legs) from opening and thereby preventing substantial flooding of the containment. The RNS is designed to perform this function based on the following:

- The RNS is assumed to be initiated manually by the operator upon receipt of the appropriate signal.
- Both normal RNS pumps are assumed to operate.
- The hydraulic path for makeup flow is low pressure through the PXS DVI lines.

If an ADS signal has been generated as a result of a LOCA, the normal RNS pumps will be unable to prevent the CMTs from draining. However, if the RNS is available, the system will provide makeup from the IRWST to the RCS and provide additional core cooling margin.

The RNS will not jeopardize the ability of the passive safety systems to mitigate design basis accident. The system will not be operated if high radiation levels due to significant core damage are detected inside containment. Furthermore, if the RNS is providing makeup to the RCS from the IRWST, the level in the IRWST must be above specified limits to continue RNS operation.

Long-Term Makeup from Outside of Containment

After an accident including fourth-stage ADS, low-pressure makeup may be required from outside of containment. The flow path for this supply of water is through any of the RNS heat exchanger channel head drain connections.

2.4.3.8 Low-Temperature Overpressure Protection

The RNS provides low-temperature overpressure protection (LTOP) for the RCS during refueling and shutdown operations. The system is designed to limit the RCS pressure within the limits specified in 10 CFR 50 Appendix G, Fracture Toughness Requirements (Reference 2.4-6).

The RNS relief valve provides LTOP for the RCS. The valve is sized to limit the pressure of the RCS to below the minimum Appendix G pressure limit of 621 psig for the limiting design basis LTOP transients by relieving 555 gpm. The following two limiting transients were identified as the design basis LTOP transients:

- Mass injection – two CVS makeup pumps delivering at runout. This transient is postulated to occur over the range of RCS temperatures between 100°F and 350°F.

- Heat input – startup of an RCP with a 50 degree temperature difference between the RCS and the steam generator secondary side. This transient is postulated to occur over the range of RCS temperatures between 100°F and 200°F.

Because the RNS suction relief valve does not have a variable pressure/temperature lift setpoint, the analysis must show that, with the selected setpoint, the relief valve will pass flow greater than that required for the limiting LTOP transient while maintaining RCS pressure less than the pressure/temperature limit curve. The current analysis shows that up to a temperature of 205°F, the mass input transient is limiting, and above this temperature, the heat input transient is limiting.

For preventing the possibility of a heat input transient, and thereby limiting the required flow rate of the RNS suction relief valve, an administrative requirement has been imposed that does not allow an RCP to be started with the pressurizer water level above 92 percent and the RCS temperature above 200°F. Under these conditions, the transient created by the startup of an RCP when the RCS temperature is above 200°F can be accommodated without additional pressure relief.

With the RCS depressurized, a vent size of 5.4 in^2 is capable of mitigating an LTOP transient. The area of the vent is equivalent to the area of the inlet pipe to the RNS suction relief valve so the capacity of the vent is greater than the flow possible with either the mass or heat input transient, while maintaining the RCS pressure less than the maximum pressure on the pressure/temperatu:e limit curve.

2.4.3.9 Loss of Offsite Power

Loss of offsite power will start the plant emergency diesel generators. The RNS pump(s) will be automatically loaded onto the emergency diesel generators and restarted.

2.4.4 References

2.4-1 *AP600 Standard Safety Analysis Report*, Chapter 5, "Reactor Coolant System and Connected Systems."

2.4-2 Title 10, Code of Federal Regulations, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants," January 1, 1996.

2.4-3 NRC Regulatory Guide 1.26, "Quality Group Classifications and Standards for Water-, Steam-, and Radioactive-Waste-Containing Components of Nuclear Power Plants," Revision 3, February 1976.

2.4-4 American Society of Mechanical Engineers Boiler and Pressure Vessel Code, Section III, 1988 with 1989 Addenda.

2.4-5 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

2.4-6 Title 10, Code of Federal Regulations, Part 50, Appendix G, "Fracture Toughness Requirements," January 1, 1996.

2.5 COMPONENT COOLING AND SERVICE WATER SYSTEMS

The only system supported by the service water system is the CCS. They are normally operated such that when one train of the CCS is required for cooling plant components, only one train of the service water system is needed to dissipate its heat into the atmosphere. Two operating trains of the CCS will require operation of two trains of the service water system.

2.5.1 Component Cooling Water System Description

The CCS provides a reliable supply of cooling water to the following plant components:

- RCP motor and thermal barrier cooling
- RNS heat exchangers (shutdown and refueling modes)
- SFS heat exchangers
- Chilled water system chillers
- CVS letdown heat exchangers
- Primary sampling system (PSS) sample heat exchanger
- Liquid radwaste system reactor coolant drain tank heat exchanger
- CVS miniflow heat exchanger
- RNS pumps' seals
- Compressed air system plant air compressors
- CCS condensate pump motor bearing oil heat exchangers

Figure 2.5-1 is a simplified sketch of the CCS (SSAR Figure 9.2.2-1).

The CCS is a closed loop cooling system that transfers heat from various plant components to the service water system. The CCS operates during all plant modes, including normal power operation, normal cooldown, and refueling. The system includes two trains, each with a component cooling water pump and heat exchanger, one CCS surge tank, and associated valves, piping, and instrumentation.

Each train of equipment takes suction from a single return header. The surge tank is connected to a shared portion of the return header. Each pump discharges directly to its respective heat exchanger. A cross-connection at the discharge of each pump allows for either pump to feed either heat exchanger. A bypass line around each heat exchanger containing a manual throttle valve is provided to prevent overcooling the component cooling water. The discharge of each heat exchanger is routed directly to the common supply header.

Component cooling water is distributed to the components by this single supply/return header arrangement. The return lines from each user are provided with balancing flow orifices or flow control valves in the CVS letdown heat exchanger and RNS heat exchanger

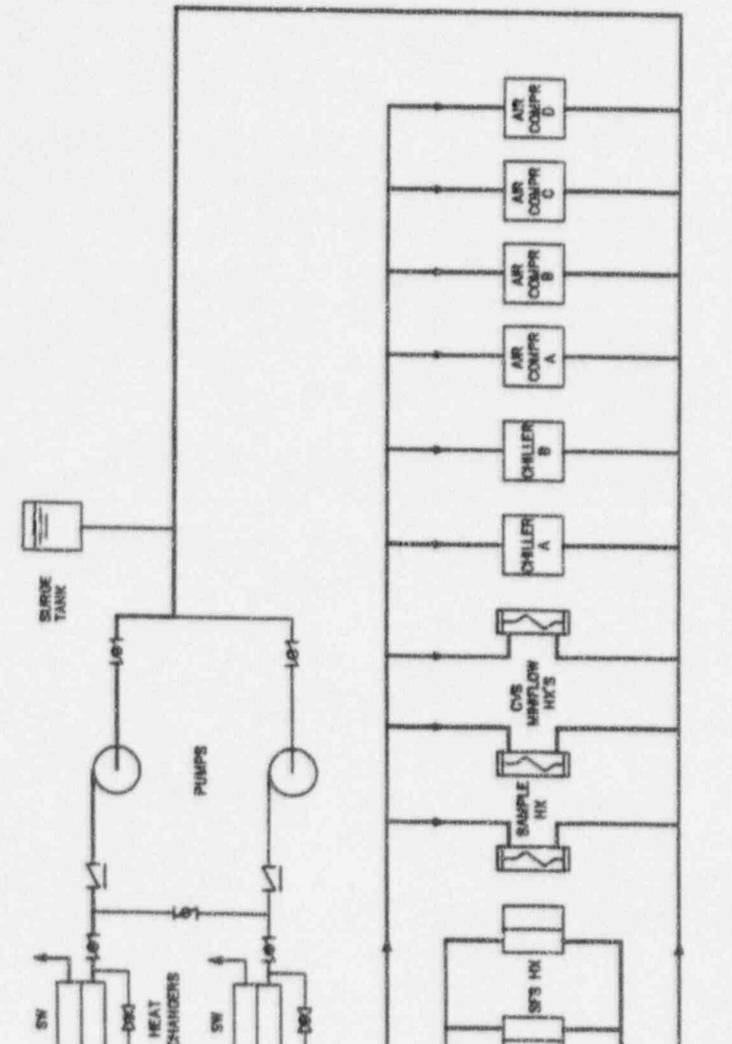


Figure 2.5-1 Component Cooling Water System Sketch

return lines. Components are grouped in branch lines according to plant layout. One branch line enters containment and supplies the RCPs (for motor and thermal barrier cooling via a 3-inch and 1-inch line, respectively), the letdown heat exchanger, the sample heat exchanger, and the reactor coolant drain tank heat exchanger. All loads inside containment are remotely isolated in response to a safety injection signal.

The safety injection actuation signal also trips the RCPs. The CCS sides of the RCPs and CVS letdown heat exchangers can be automatically isolated (on the return lines) in case of RCS leakage into the CCS. Check valves isolate the leakage in the supply lines. The CCS side of the RNS heat exchangers can be remotely isolated (on the return lines) by the operator in case of leakage into the CCS. Closure of the manual butterfly valves isolates the supply lines. All individually cooled components can be locally isolated for maintenance of the component while supplying the remaining components with cooling water.

The CCS surge tank accommodates thermal expansion and contraction from temperature changes in the CCS. The tank also accommodates leakage in to or out of the CCS until the operator can isolate the leak. Water makeup to the surge tank is provided by the demineralized water transfer and storage system. The normal makeup for initial fill of the system is capable of filling the system in approximately 4 hours. The surge tank is vented to the atmosphere.

A line is routed from the pump discharge header to the chemical addition tank. The chemical solution, through the chemical addition tank discharge line, is then discharged to the surge tank. The chemical addition line contains valves and piping that facilitate mixing chemicals into the system to control oxygen concentration and inhibit corrosion.

Each component heat exchanger cooled by the CCS is protected by a thermal relief valve in the CCS line between the isolation valves of the heat exchanger. The RCPs and letdown heat exchanger cooling lines, which are automatically isolated in case of a reactor coolant leakage, have relief valves suitable for overpressure protection of the heat exchanger and the CCS piping subjected to the RCS pressure.

The containment CCS supply penetration line is provided with one automatic MOV located outside containment and one check valve located inside the containment. The check valve performs the thermal relief function to prevent overpressurization of the piping between the inner and outer isolation valves. The containment CCS return penetration line is provided with two automatic MOVs located inside and outside containment. These valves are designed for controlled leaks to perform the thermal relief function to prevent overpressurization of the piping between the inner and outer isolation valves. Each penetration line is provided with test boundary valves, test connection lines, and test vent lines to allow leak testing.

The CCS is equipped with adequate instrumentation to provide complete control and supervision of the system functions during operation. Pressure and flow instruments monitor cooling water flow delivery to the various system users. CCS water inventory variations are monitored and controlled by supervising the surge tank level changes. The performance of the various CCS users can be assessed by evaluating the heat transfer process. This is done by monitoring the cooling water flow through each user and the cooling water temperature change across the individual heat exchangers. Any leakage of primary coolant into the CCS is detected and isolated by monitoring the high flow in the cooling water return lines from these users, a high radiation level on the common header at the pump suction, or a high surge tank level.

Chemicals are added to control CCS water chemistry as necessary. These include a corrosion inhibitor, biocide, oxygen scavenger, and pH adjustment.

2.5.2 Service Water System Description

The service water system includes two 100-percent-capacity service water pumps, automatic backwash strainers, a two-cell cooling tower with a divided basin, and associated piping, valves, controls, and instrumentation. Figure 2.5-2 is a simplified sketch of the service water system based on the SSAR chapter 9 service water system description.

The service water pumps, located in the turbine building, take suction from piping connected to the basin of the service water cooling tower. Service water is pumped through strainers to the component cooling water heat exchangers for removal of heat. Heated service water from the heat exchangers then returns through piping to an induced draft cooling tower where the system heat is rejected to the atmosphere. Cool water, collected in the tower basin, flows through fixed screens to the pump suction piping for recirculation through the system.

A small portion of the service water flow is normally diverted to the circulating water system. This blowdown is used to control levels of solids concentration in the service water system. An alternate blowdown flow path is provided to the waste water system.

The service water system is arranged into two trains of components and piping. Each train includes one service water pump, one strainer, and one cooling tower cell. Each train provides 100-percent-capacity cooling for normal power operation. Cross-connections between the trains upstream and downstream of the CCS heat exchangers allows either service water pump to supply either heat exchanger, and allows either heat exchanger to discharge to either cooling tower cell.

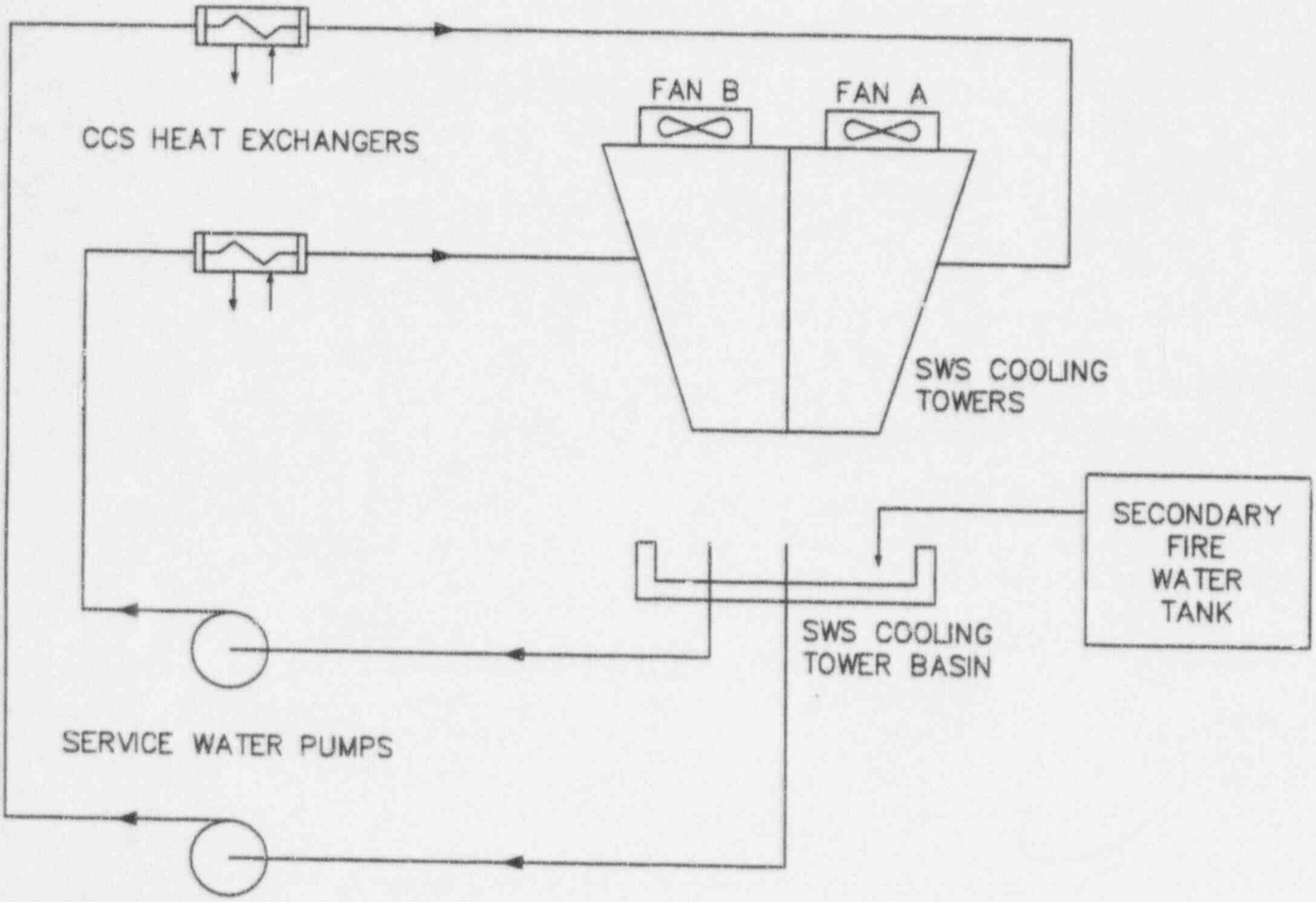


Figure 2.5-2 Service Water System Sketch

Service water system materials are compatible with the cooling water chemistry and the chemicals used for the control of long-term corrosion and organic fouling. Water chemistry is controlled by the turbine island chemical feed system.

2.5.3 Shutdown Operation

All system operations all monitored from the main control room. The operations to initiate or terminate the cooling to the users, in different operating modes, are performed by the operator locally by manual actuation of valves or remotely for those valves with power-operated actuators. The CCS and service water system pumps are controlled remotely from the main control room.

Plant shutdown is defined as the operations that bring the reactor plant from power operation to cold, subcritical conditions. During plant shutdown operations, both CCS and service water system mechanical trains normally operate. Operation of only a single CCS and service water system train results in an extended plant cooldown.

The initial phase of plant cooldown consists of reactor coolant cooldown and depressurization. Heat is transferred from the RCS via the steam generators to the MSS, where the rate of steam dump is controlled to establish an RCS cooldown rate of about 50°F/hr. Depressurization is accomplished by spraying reactor coolant into the pressurizer, which cools and condenses the pressurizer steam bubble.

When the reactor coolant temperature and pressure have been reduced to 350°F and 450 psig respectively (approximately 4 hours after reactor shutdown), the second phase of plant cooldown is initiated by placing the RNS in service.

Prior to starting the RNS pumps, the standby CCS pump and heat exchanger are placed in operation and component cooling water is initiated to the RNS heat exchangers. Following this, the RNS can be placed into operation by aligning valves and starting one RNS pump. The second RNS pump is started later and the cooldown proceeds in accordance with the AP600 refueling outage plan.

The CCS, in conjunction with the RNS and the service water system, cools the RCS to 120°F within 96 hours after shutdown consistent with the AP600 refueling outage plan. During the cooldown period, the component cooling water inlet temperature to the various components may not exceed 110°F, and the RCS cooldown rate may not exceed 75°F/hr. These conditions are maintained within limits by automatic control throttling of the CCS flow to the RNS heat exchangers.

The CCS provides cooling water at a temperature not greater than 95°F during normal operation based on a service water temperature not greater than 89°F.

2.5.3.1 Normal Plant Cooldown

The CCS, in conjunction with the RNS, is designed to remove both residual and sensible heat from the core and the RCS and reduce the temperature of the RCS during the second phase of plant cooldown. The first phase of cooldown is accomplished by transferring heat from the RCS via the steam generators to the MSS.

The CCS performs this function with both CCS pumps and heat exchangers operating. The unavailability of a pump or heat exchanger to operate during cooldown extends the required time for cooldown but does not prevent plant cooldown.

The CCS performs this function in a timely manner (96 hours) consistent with the AP600 refueling and maintenance outage schedule.

The CCS provides cooling water at a temperature not greater than 110°F from 4 hours after shutdown, based on a service water temperature not greater than 100°F.

The CCS provides cooling water at a temperature not greater than 87°F at the end of cooldown, based on a service water temperature not greater than 85°F.

2.5.3.2 Refueling

The CCS, during and after a partial core fuel shuffle refueling or a normal full-core off-load, is designed to supply cooling water to both spent fuel pool heat exchangers to cool the spent fuel pool water. Normally, the CCS performs this function with both CCS pumps and heat exchangers operating. The cooling of both SFS trains may be supported with only one CCS train when some of the normal heat loads are shed from the system. The CCS also cools one or both trains of RNS during refueling.

2.5.3.3 Plant Startup

Plant startup is defined as the operations that bring the reactor plant from a cold shutdown condition to no-load operating temperature and pressure, and subsequently to power operation.

During this period, both CCS trains of equipment are operating. Once the RNS heat exchangers are isolated, only one CCS train is required to remove the heat load. Plant heatup is initiated by starting the RCPs. Residual heat removal from the core is discontinued by stopping the RNS pumps. The letdown heat exchanger is placed on automatic temperature control to maintain a constant letdown temperature. When the RCS is heated to approximately 350°F, the RNS is isolated from the RCS and the CCS supply to the RNS heat exchangers is stopped. Throughout the plant startup procedure, cooling water flows and temperatures are monitored to verify that the values are within the required limits. Once startup is complete, one CCS pump and heat exchanger are taken out of service.

2.5.3.4 Operations During Plant Transients and Accidents

IRWST Cooling

Operation of the RNS to provide cooling for the IRWST limits the IRWST water temperature to prevent boiling during extended operation of the PRHR HX or limit IRWST temperature during normal operation. The CCS provides cooling water to the RNS to transfer the heat to the service water system.

Post-Accident Cooldown and Recovery

Operation of the RNS after ADS actuation, IRWST injection, and containment flood-up will permit removal of decay heat. The CCS provides cooling water to the RNS to transfer the heat to the service water system.

Loss of Offsite Power

Loss of offsite power will start the plant emergency diesel generators. Following a loss of offsite power, the CCS pumps are automatically loaded on the standby diesel generators and thus continue to provide the required cooling water flow. Power from the standby diesel generators is also provided to the service water and normal residual heat removal pumps. Therefore, after initial RCS cooldown and depressurization, the RNS can be aligned and core decay heat removed via the normal train of the RNS, CCS, and service water system.

2.6 CONTAINMENT SYSTEMS

2.6.1 System Description

The containment systems are described in SSAR section 6.2 (Reference 2.6-1). This section discusses the major design features of the containment systems as they apply to shutdown safety including the containment system (CNS) and the passive containment coolir g system (PCS).

2.6.1.1 Containment System

The CNS is the collection of boundaries that separates the containment atmosphere from the outside environment. The containment atmosphere for the AP600 includes all volumes on the inside of the containment vessel that would be exposed to radioactive releases subsequent to a breach in the RCS boundary. The outside environment under design basis assumptions includes any areas beyond the containment. The collection of boundaries and, therefore, the CNS, includes the steel containment shell, electrical and mechanical penetrations, fuel transfer penetration, equipment hatches and personnel airlocks, steam generator shells, steam generator steam side instrumentation connections, and steam, feedwater, and blowdown lines within the containment shell. The steam generator shells and instrumentation connections, and the steam, feedwater, and blowdown lines are part of the containment boundary because they are boundaries against activity leakage from inside containment after a LOCA. As such, these barriers serve the same purpose as the containment vessel and, therefore, become part of the containment itself. Containment isolation valves and test connections are an integral part of every system that penetrates the containment and not a part of the CNS. However, compliance is required with CNS criteria for these valves and connections. The CNS is designed to perform the following safety-related functions:

- Integrity

  The CNS acts as the third line of defense against the release of fission products to the atmosphere, with the fuel cladding and the RCS boundary being the first two barriers. The CNS is designed to withstand the maximum internal pressure and temperature resulting from postulated LOCAs, steam line breaks, and feedwater line breaks. The design also provides that adequate protection from external pressure conditions that may result from design basis events, including a loss of all ac power.

- Isolation

  The CNS provides containment isolation criteria to preserve the integrity of the containment boundary to prevent or limit the escape of fission products while allowing the normal or emergency passage of fluids through the containment boundary.

- Heat removal

  The CNS provides the interface with the PCS to reduce pressure and remove heat from the containment atmosphere following a LOCA, steam line break, feedwater break, IRWST steaming during PRHR HX operation, or ADS actuation.

2.6.1.2 Passive Containment Cooling System

The PCS is a safety-related system which is capable of transmitting heat directly from the containment vessel to the environment such that the containment design pressure (and temperature) is not exceeded following any postulated design basis event and the pressure is significantly reduced in the longer term. The heat transfer mechanism includes conduction, convection, radiation, and mass transfer (water evaporation). Figure 2.6-1, based on the SSAR section 6.2 PCS description, and Figure 2.6-2 (SSAR Figure 6.2-2) illustrate how the PCS makes use of the steel containment shell as a heat transfer surface. Cooling air is drawn from the environment via an "always open" air flow path over the containment vessel and returned to the environment after removing heat from the containment shell. The containment shell is wetted by passive draining of the water storage tank that is incorporated into the shield building structure above the containment.

The PCS consists of the integral shield building water storage tank, a cooling water delivery path to the containment shell, an air path formed within the shield building surrounding the containment (consisting of an air baffle between the shield building and containment, an air inlet, and an air/steam exhaust structure), and associated instrumentation, piping, and valves. The majority of the cooling water components directly associated with the storage tank are located in a valve room in the shield building above containment and underneath the water storage tank.

Heat removal by the PCS is initiated automatically by the PMS in response to a Hi-Hi containment pressure signal, as sensed by two out of four independent safety-related, pressure sensor instrumentation channels. Also, manual actuation can be accomplished by the operator from the main control room or the remote shutdown workstation via the PMS. Additionally, the DAS provides a diverse backup to the PMS actuating the PCS on high containment temperature. The DAS also provides for manual actuation of the PCS. The system actuation logic is documented further in section 7.3 of the SSAR (Reference 2.6-2).

As shown in Figure 2.6-2, actuation of the PCS initiates water flow by gravity from the PCS water storage tank contained in the shield building structure above the containment onto the containment dome outer surface, forming a water film over the structure. The water flow is automatically established by the opening of either of two parallel air-operated isolation

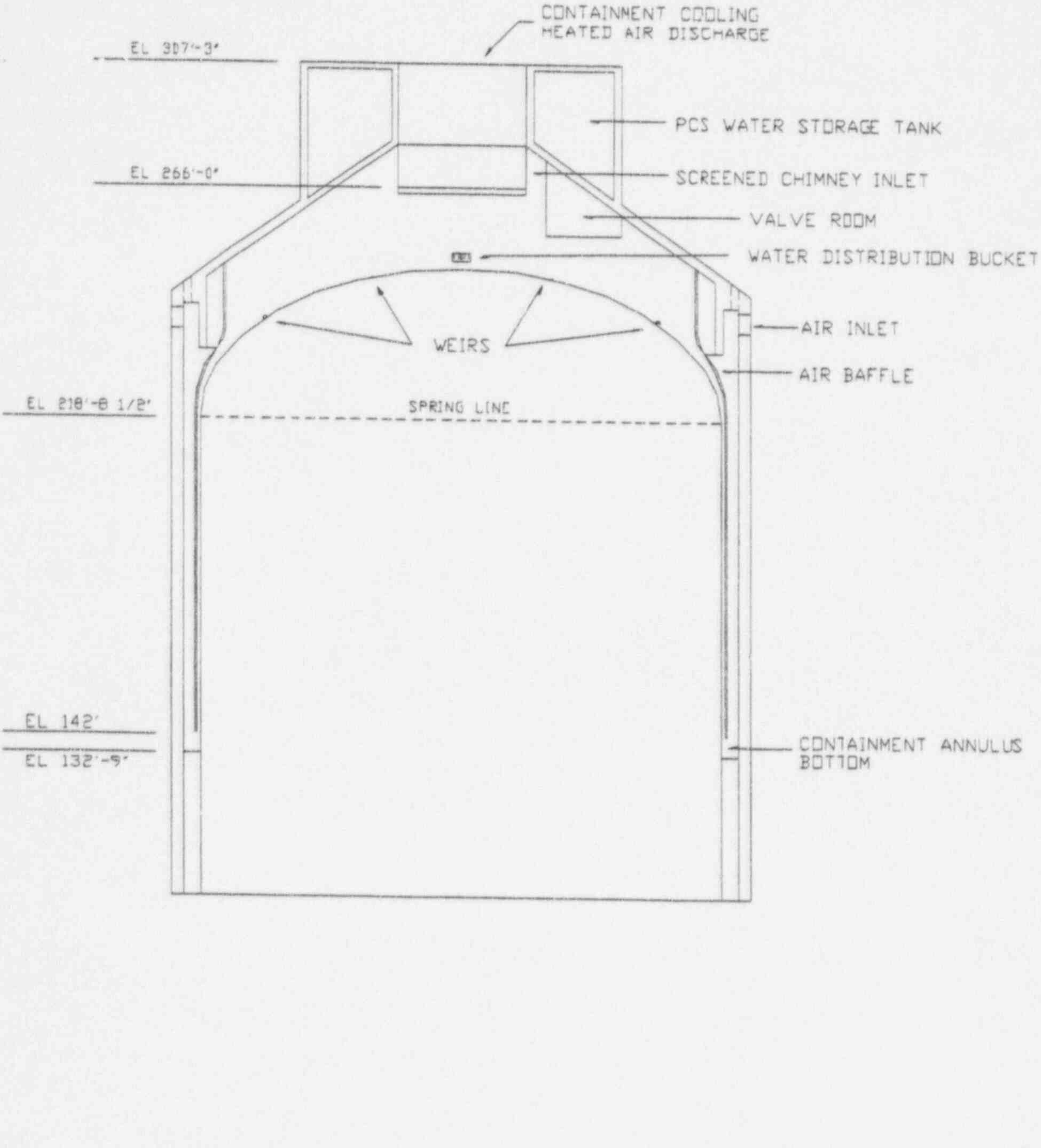


Figure 2.6-1 Passive Containment Cooling System Arrangement

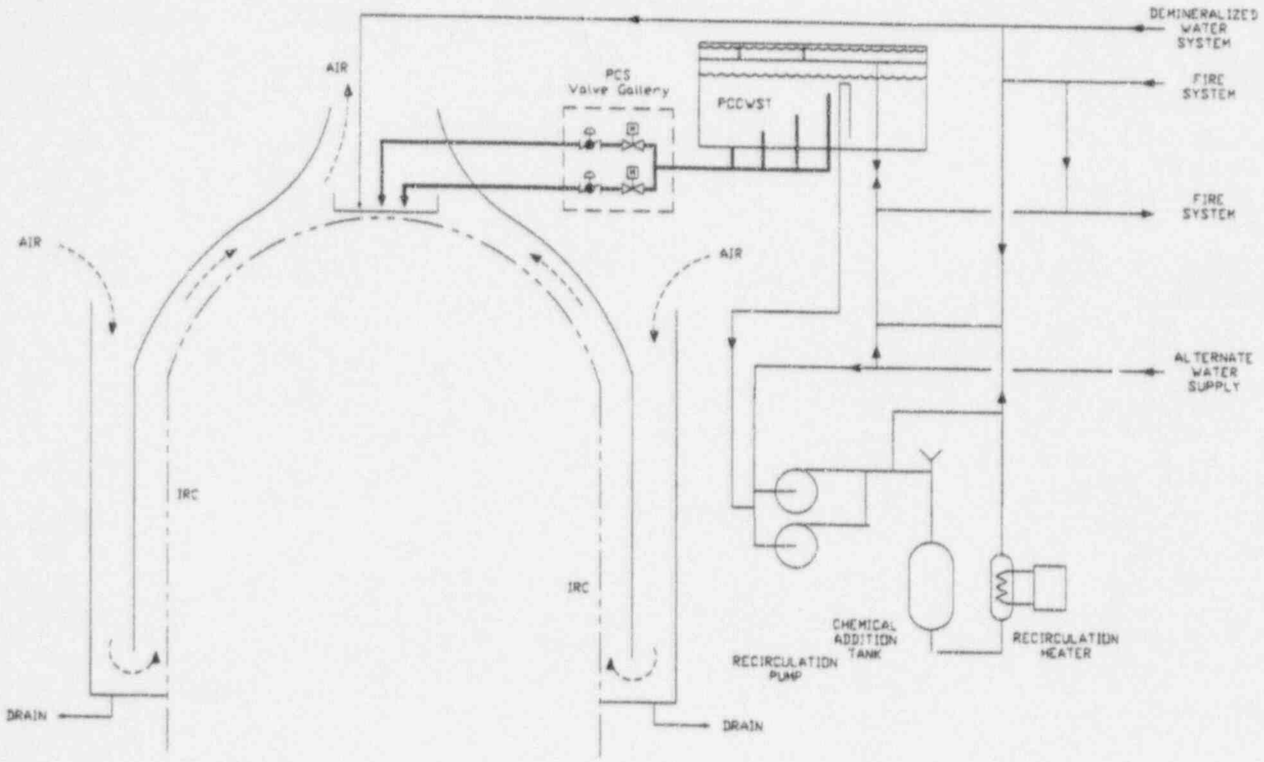


Figure 2.6-2 Passive Containment Cooling System Sketch

valves. The valves are safety-related, fail-open, and air-operated to enhance system reliability and ensure system availability. Opening of either or both of the isolation valves will result in acceptable system performance. Upstream of each isolation valve is a normally open safety-related motor-operated isolation valve, which is available to isolate cooling water flow in the event of inadvertent actuation. The MOVs receive a confirmatory opening signal from the PMS in response to a Hi-Hi containment pressure condition.

2.6.2 Design Features to Address Shutdown Safety

The AP600 has addressed the issue of containment closure at shutdown and incorporated the following requirements in the Technical Specifications (Reference 2.6-3). In shutdown Modes 3 and 4, containment status is the same as at-power. Specifically, containment integrity is required, the major equipment hatches are closed and sealed, and containment air locks and isolation valves are operable.

In Modes 5 and 6, containment closure capability is required during shutdown operations when there is fuel inside containment. Containment closure is required to maintain, within containment, the cooling water inventory. Due to the large volume of the IRWST and the reduced sensible heat during shutdown, the loss of some of the water inventory can be accepted. Further, accident analyses provided in section 4 of this report show that containment closure capability is not required to meet offsite dose requirements. Therefore, containment does not need to be leak- tight as required for Modes 1 through 4.

In Modes 5 and 6, there is no potential for steam release into the containment immediately following an accident. Pressurization of the containment could occur only after heatup of the IRWST due to PRHR HX operation (Mode 5 with RCS intact), after heatup of the RCS with direct venting to the containment (Mode 5 with reduced RCS inventory or Mode 6 with the refueling cavity not fully flooded), or after heatup of the RCS and refueling cavity (Mode 6 with refueling cavity fully flooded). The time from loss of normal cooling until steam release to the containment for these different conditions is shown in Figure 2.6-3 (duplicated from SSAR section 16.1, Figure B3.6.8-1) (Reference 2.6-3) as a function of time after shutdown. To limit the magnitude of cooling water inventory losses and because local manual action may be required to achieve containment closure, it is assumed that the containment hatches, air locks, and penetrations must be closed prior to steaming into containment.

The containment equipment hatches, which are part of the containment pressure boundary, provide a means for moving large equipment and components into and out of containment. If closed, the equipment hatch must be held in place by at least four bolts. If open, each equipment hatch can be closed using a dedicated set of hardware, tools, and equipment. A self-contained power source is provided to drive each hoist while lowering the hatch into position. Large equipment and components may be moved through the hatches as long as they can be removed and the hatch closed prior to steaming into the containment.

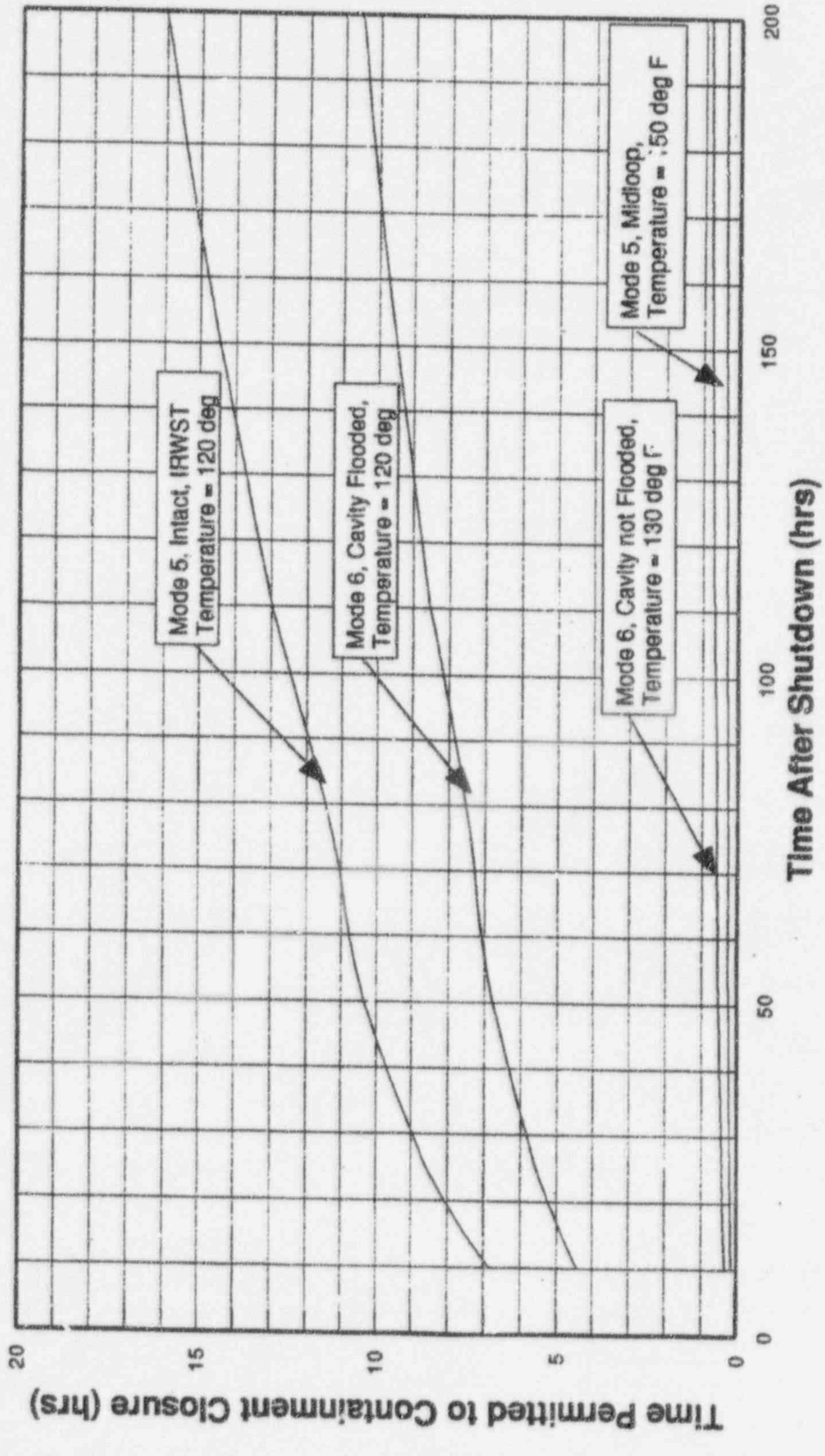


Figure 2.6-3 Time Permitted for Containment Closure

The containment air locks, which are also part of the containment pressure boundary, provide a means for personnel access during Modes 1, 2, 3, and 4 unit operation. Each air lock has a door at both ends. The doors are normally interlocked to prevent simultaneous opening when containment operability is required. During periods of unit shutdown when containment closure is required, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. Temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

Containment spare penetrations, which also provide a part of the containment boundary, provide for temporary support services (electrical, I&C, air, and water supplies) during Modes 5 and 6. Each penetration is flanged and normally closed. During periods of plant shutdown, temporary support systems may be routed through the penetrations; temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

The spare penetrations must be closed or, if open, capable of closure prior to reaching boiling conditions within reactor coolant inventory.

Containment penetrations, including purge system flow paths, that provide direct access from containment atmosphere to outside atmosphere must be isolated or isolatable on at least one side. Isolation may be achieved by an operable automatic isolation valve or by a manual isolation valve, blind flange, or equivalent.

The fuel transfer canal may be opened to provide for the transfer of new and spent fuel in to and out of containment during Modes 5 and 6. At times when the canal is opened, it must be isolatable on at least one side by closure of the flange within containment or the gate valve outside containment.

2.6.3 References

2.6-1 *AP600 Standard Safety Analysis Report*, Chapter 6, "Engineered Safety Features."

2.6-2 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

2.6-3 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

2.7 CHEMICAL AND VOLUME CONTROL SYSTEM

2.7.1 System Description

The CVS is described in SSAR subsection 9.3.6 (Reference 2.7-1). The CVS is designed to perform the following major functions:

- Purification – maintain RCS fluid purity and activity level within acceptable limits during all modes of operation including shutdown

- RCS inventory control and makeup – maintain the required coolant inventory in the RCS; maintain the programmed pressurizer water level during normal plant operations

- Chemical shim and chemical control – maintain the reactor coolant chemistry conditions by controlling the concentration of boron in the coolant for plant startups, normal dilution to compensate for fuel depletion and shutdown boration, and provide the means for controlling the RCS pH by maintaining the proper level of lithium hydroxide

- Oxygen control – provide the means for maintaining the proper level of dissolved hydrogen in the reactor coolant during power operation and for achieving the proper oxygen level prior to startup after each shutdown

- Borated makeup to auxiliary equipment – provide makeup water to the primary side systems that require borated reactor grade water

- Pressurizer auxiliary spray – provide pressurizer auxiliary spray water for depressurization during operation when the normal spray is not available

The CVS consists of regenerative and letdown heat exchangers, demineralizers and filters, makeup pumps, tanks, and associated valves, piping, and instrumentation. The CVS functions to fulfill the requirements of controlling RCS chemistry, purity, and inventory for continued operation of the plant. The CVS is functionally composed of the following:

- The purification loop includes the regenerative and letdown heat exchangers, demineralizers, reactor coolant filters, and associated valves, piping, and instrumentation. The purification loop is located inside containment and provides the direct interface with the RCS.

- The CVS makeup includes the makeup pumps with the associated suction and discharge piping. The makeup pumps, located outside containment in the auxiliary building, take suction from the boric acid tank and/or the demineralized water system through a common suction header. The makeup pump discharge piping penetrates containment downstream of the makeup filter and connects into the purification loop upstream of the point where the purification return flow returns through the shell side of the regenerative heat exchanger. The makeup pumps are used to provide inventory to the RCS for the introduction of chemicals to the RCS, filling and pressure testing the RCS, and for providing borated makeup for auxiliary pressurizer spray and auxiliary equipment.

- The CVS letdown line is connected to the purification loop downstream of the reactor coolant filters. The letdown flow passes through the letdown orifice prior to exiting containment to the liquid radwaste system. The letdown line functions to reduce RCS inventory during normal plant operations, power changes, startups, and shutdown.

- The CVS hydrogen injection line is connected to the purification loop upstream of the regenerative heat exchanger prior to the purification flow returning to the RCS. The hydrogen injection line is directly connected to a high pressure hydrogen bottle located outside containment. It provides hydrogen to the RCS during power operation and prior to startup after each shutdown to achieve the proper oxygen level.

- The safety-related portions of the CVS support containment isolation, reactor coolant pressure boundary, and inadvertent boron dilution protection.

Figure 2.7-1 is a simplified sketch of the CVS (SSAR Figure 9.3.6-1).

2.7.1.1 Purification

The primary function of the purification loop is to remove corrosion and fission products. The purification loop also provides the path for CVS makeup and letdown functions.

The normal CVS purification loop is entirely inside containment and operates at RCS pressure. The CVS uses the developed head of the RCPs as the motive force for the purification flow. During power operations, fluid is continuously circulated through the CVS from the discharge of the RCP. This connection to the RCS is shared with the pressurizer spray line. The CVS purification return to the RCS is connected to steam generator A on the suction side of the RCPs 1A and 1B. This connection to the RCS is shared with the PRHR HX return line.

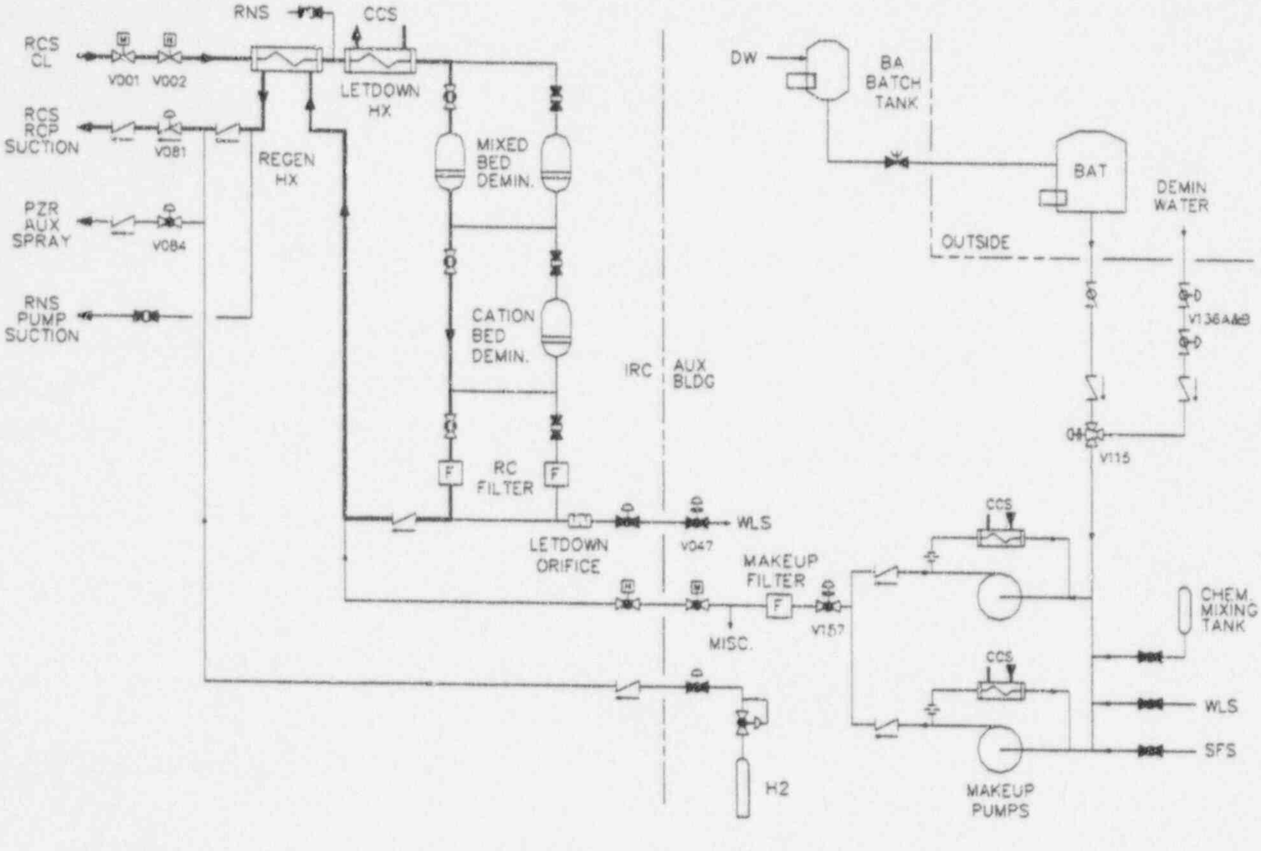


Figure 2.7-1 Chemical and Volume Control System Simplified Sketch

The coolant enters the CVS through the purification isolation valves and passes through the tube side of the regenerative heat exchanger where it is cooled by the returning CVS flow. The coolant is further cooled by component cooling water in the letdown heat exchanger to a temperature compatible with the demineralizer resins. The letdown heat exchanger outlet temperature is manually selected by the operator, who must remotely position a CCS flow control valve. A temperature detector with a high alarm in the purification line alerts the operator of a high temperature at the letdown heat exchanger. If a high temperature is detected in the letdown line downstream of the heat exchanger, the CCS flow control valve will receive a signal to automatically fully open and provide maximum CCS cooling flow to the heat exchanger. If the temperature continues to increase, the purification flow is isolated on high letdown heat exchanger outlet temperature to prevent damaging the demineralizer resins.

The purification flow continues through a mixed bed demineralizer, optionally through a cation bed demineralizer, and through a reactor coolant filter. The purification flow returns to the suction of an RCP after being heated in the shell side of the regenerative heat exchanger. Because the motive force for the purification loop is the RCP head, continuous purification is provided without operating any CVS makeup pumps.

The mixed bed demineralizers are provided in the purification loop to remove ionic corrosion products and certain ionic fission products. The demineralizers also act as filters. One mixed bed is normally in service, with a second demineralizer acting as backup in case the normal unit should become exhausted during operation. Each demineralizer is sized to provide a minimum of one fuel cycle of service without changeout. Therefore, remotely operated valves are not necessary.

The mixed bed demineralizer in service can be supplemented by intermittent use of the cation bed demineralizer for additional purification in the event of fuel defects. In this case, the cation resin removes mostly lithium and cesium isotopes. The cation bed demineralizer has sufficient capacity to maintain the cesium-136 concentration in the reactor coolant below 1.0 microcurie per cc with design basis fuel defects. Each mixed bed and the cation bed demineralizer is sized to accept the maximum purification flow.

The reactor coolant filters are provided downstream of the demineralizers to collect particulates and resin fines. One filter is normally in service while the other is in standby. Each filter is sized to provide one fuel cycle of service; therefore, remotely operated valves are not necessary.

During plant shutdowns when the RCPs are stopped, the RNS provides the motive force for the CVS purification. The purification flow is taken from just downstream of the RNS heat exchanger and enters the CVS between the regenerative and letdown heat exchangers. The purification flow then continues through the letdown heat exchanger for further cooling;

follows the normal purification loop through the demineralizer, reactor coolant filter, and shell side of the regenerative heat exchanger; and then returns to the RCS via the RNS pump suction. Boron changes and dissolved gas control are still possible by operating the CVS in a semi-closed loop arrangement as described in the following subsections.

2.7.1.2 Gaseous Purification

Removal of radiogases from the RCS normally will not be necessary because the gases will not build up to unacceptable levels when fuel defects are within normally anticipated ranges. If radiogas removal were to be required because of high fuel defects, the CVS would be operated by diverting flow to the liquid radwaste system degasifier. Degassing of the RCS is performed by diverting the purification flow through the letdown line to the liquid radwaste system after passing through the normal purification path of the regenerative and letdown heat exchangers, demineralizer, and the reactor coolant filter. As the flow exits the reactor coolant filter and continues through the letdown line, it is depressurized by flowing through the letdown orifice. The letdown flow then passes through the letdown isolation valves and is routed outside of containment to the liquid radwaste system degasifier for degassing. After degassing, the letdown is accumulated in one of the liquid radwaste system holdup tanks. The CVS makeup pumps are aligned to take suction from the liquid radwaste system holdup tank to return the coolant to the RCS following degassing. The makeup pumps return the flow to the RCS via the normal makeup path. This provides efficient gas removal and would be required only intermittently, even with high levels of fuel defects.

Removal of radioactive gas and hydrogen during shutdown operations is necessary to avoid extending the maintenance and refueling outages. For degassing during shutdown operations, the RCS pressure boundary cannot be opened to the containment atmosphere until the gas concentrations have been reduced to low levels. The shutdown degassing process will be accomplished by operating the CVS in the semi-closed loop configuration, as described previously. However, for shutdown degassing (when the RCS is depressurized), a line is provided to allow the letdown orifice to be manually bypassed, so gas removal can continue. The letdown flow control valve will be throttled to maintain the RCS pressure during shutdown operations when the RCS is water-solid and the letdown orifice is bypassed.

2.7.1.3 RCS Inventory Control and Makeup

Changes in the reactor coolant volume will be accommodated by the pressurizer level program for normal power changes, including transition from hot standby to full power operation and return to hot standby. In addition, the pressurizer has sufficient volume, within the deadband of the level control program, to accommodate minor RCS leakage for some time. The CVS provides inventory control to accommodate minor leakage from the RCS, expansion during heatup from cold shutdown, and contraction during cooldown. This inventory control is provided by letdown connections from, and makeup connections to, the CVS purification loop.

When required to reduce the pressurizer level, letdown is taken out of the purification loop at a point downstream of the reactor coolant filters. The letdown fluid is depressurized by flowing through the letdown orifice, then passing through the letdown isolation valves, out of containment to the liquid radwaste system. The letdown valves automatically open on a signal generated by the pressurizer level control.

On a low pressurizer level signal (relative to the programmed level), one of the CVS makeup pumps will start automatically to provide makeup. These centrifugal pumps normally take suction from the boric acid tank and the demineralized water tank. The makeup concentration is determined by the position of the three-way control valve in the pump suction header, which is controlled in conjunction with the makeup flow control valve to blend makeup to the proper concentration to match the RCS concentration. The makeup pump discharge flows through the makeup flow control valve and then through the makeup filter. The flow continues into containment through the makeup isolation valves and then joins the purification loop return piping into the shell side of the regenerative heat exchanger and then to the RCS. The makeup pump automatically stops when the pressurizer level increases to the correct value. Because the plant incorporates canned RCPs, there is no seal leakage and the normal leakage from the RCS will be small. Therefore, the CVS makeup pumps will operate infrequently (approximately once per day with 1 gpm leakage).

2.7.1.4 Chemical Control and Chemical Shim

The CVS provides the following functions to support the water chemistry and chemical shim requirements of the RCS:

- Means of addition and removal of pH control chemicals for startup and normal operation

- Means of addition and removal of soluble chemical neutron absorber (boron) and makeup water at concentrations and rates compatible with normal plant operation

RCS chemistry changes are accomplished with an open-loop feed-and-bleed operation. The letdown and makeup paths are operated simultaneously, and appropriate chemicals are provided at the suction of the reactor makeup pumps.

2.7.1.5 Chemical Shim

RCS boron changes are required to accommodate fuel depletion, startups, shutdowns, and refueling.

To borate the RCS, the operator sets the makeup control system to automatically add a preset amount of boric acid by fully diverting the three-way valve to the boric acid tank. The makeup pumps operate to deliver this flow through the normal makeup path to the RCS. The delivered flow is measured at the discharge of the makeup pumps.

If dilution is required, the operator will set the makeup control system to add a preset amount of demineralized water by positioning the three-way valve to the demineralized water source. The makeup pumps will operate in a similar fashion by delivering this flow to the RCS via the normal makeup path. In either case, if the pressurizer level exceeds its control point, the letdown path to the liquid radwaste system holdup tanks will automatically open.

Boric acid is provided to the boric acid tank by mixing 2.5 weight percent boric acid solution in the boric acid batching tank. Boric acid crystals are introduced into the boric acid batching tank through a fill connection on the top of the tank. A demineralized water connection is also located near the top of the tank. After the boric acid crystals and demineralized water are added to the tank, the solution is mixed with a mechanical mixer, while the mixture is heated by the batching tank's immersion heater. (Heating the tank provides more efficient mixing.) After the boric acid crystals have dissolved and the solution is sampled to determine if the mixture is acceptable, the solution is drained by gravity into the boric acid tank. No provisions are incorporated for boric acid recycle from the liquid radwaste system.

2.7.1.6 pH Control

The chemical agent used for pH control is lithium hydroxide (Li_7OH). This chemical is chosen for its compatibility with the material and water chemistry of borated water, stainless steel, nickel alloy, and zirconium systems. In addition, lithium 7 is produced in the core region because of irradiation of the dissolved boron in the coolant. A chemical mixing tank is provided to introduce the solution to the suction of the makeup pumps as required to maintain the proper concentration of Li_7OH in the RCS.

The solution is poured into the chemical mixing tank and is then flushed to the suction manifold of the makeup pumps with demineralized water. The demineralized water enters the mixing tank from the connection on the top of the tank. A flow orifice is provided on the demineralizer water inlet pipe to allow chemicals to be flushed into the RCS at acceptable concentrations.

The concentration of lithium 7 in the RCS is varied between 0.7 ppm and 2.2 ppm according to a pH control curve as a function of the boric acid concentration of the RCS. If the concentration exceeds the proper value, as it may during the early stages of core life when lithium 7 is produced in the core at a relatively high rate, the cation bed demineralizer is used in the letdown path in series with the mixed bed demineralizer to lower the lithium 7 concentration. Because the buildup of lithium is slow, the cation bed demineralizer is used only intermittently. Because this is a planned operation, the inlet valve to the cation bed demineralized is remotely operated. When letdown is being diverted to the liquid radwaste system, the letdown flow should be routed through the cation bed demineralizer to remove as much lithium 7 and cesium as possible.

2.7.1.7 Oxygen Control

The CVS provides control of the RCS oxygen concentration, both during startup by introducing hydrazine and during power operations by injecting hydrogen, which drives the equilibrium concentration of oxygen produced by radiolysis in the core toward zero.

During plant startup from cold conditions, hydrazine is used as an oxygen scavenging agent. The hydrazine solution is introduced into the RCS via the makeup flow and chemical mixing tank, in the same manner as described for lithium 7 addition. The oxygen scavenger is used for oxygen control only at startup from cold shutdown.

The hydrazine solution is poured into the chemical mixing tank and is then flushed to the suction manifold of the makeup pumps with demineralized water. The demineralized water enters the mixing tank from the connection on the top of the tank. An orifice is provided on the demineralizer water inlet pipe to allow chemicals to be flushed into the RCS at acceptable concentrations.

2.7.1.8 RCS Filling and Pressure Testing

RCS filling is accomplished by using the CVS makeup pumps to provide fluid at the proper boron concentration (refueling). The CVS makeup pumps take suction from both the boric acid tank and the demineralized water supply header through the three-way blending valve to provide the proper boron concentration. The makeup flow continues from the makeup pump discharge, through the makeup flow control valve, the makeup filter, and the normal makeup path to the RCS. If an RCS loop is drained to a clean liquid radwaste system holdup tank, this drained volume can be returned by opening the line to the makeup pumps from that holdup tank. The makeup pumps would then take suction from the liquid radwaste system holdup tank.

The CVS makeup pumps produce sufficient head to pressure test the RCS after maintenance and refueling. A temporary hydrotest pump will be required for initial hydrotesting, which will require higher pressures than can be achieved with the makeup pumps. Flanged connections are located on the makeup pump suction and discharge piping for a hydrotest pump. When the hydrotest pump is connected, it would be in a parallel arrangement with the makeup pumps.

2.7.1.9 Pressurizer Auxiliary Spray

The CVS makeup pumps provide auxiliary spray to the pressurizer through a connection on the pressurizer main spray header. The makeup pumps take suction from the boric acid tank and the demineralized water supply header to provide borated water at a selected boron concentration. The pumps use the normal makeup path to the RCS through the shell side of the regenerative heat exchanger and continue through the auxiliary spray isolation valve to the RCS and the connection on the main spray header.

2.7.2 Design Features to Address Shutdown Safety

The AP600 CVS is a nonsafety-related system. However, portions of the system are safety-related and perform safety-related functions, such as containment isolation, termination of inadvertent RCS boron dilution, RCS pressure boundary preservation, and isolation of excessive makeup.

Boron dilution events during low power modes can occur for a number of reasons, including malfunctions of the makeup control system. Regardless of the cause, the protection is the same. The CVS is designed to avoid and/or terminate boron dilution events by automatically closing either one of two series, safety-related valves in the demineralized water supply line to the makeup pump suction to isolate the dilution source. Additionally, the suction line for the CVS makeup pump is automatically realigned to draw borated water from the boric acid tank. The automatic boron dilution protection signal is safety-related and is generated upon any reactor trip signal, source-range flux multiplication signal, low input voltage to the Class 1E dc and uninterruptible power supply system battery chargers, or a safety injection signal.

The safety analysis of boron dilution accidents is provided in SSAR chapter 15 (Reference 2.7-2) and is discussed in section 4.5 of this report. For dilution events that occur during shutdown, the source-range flux-doubling signal is used to isolate the line from the demineralized water system by closing the two safety-grade remotely operated valves. The three-way pump suction control valve aligns the makeup pumps to take suction from the boric acid tank and, therefore, stops the dilution.

For refueling operations, administrative controls are used to prevent boron dilutions by verifying that the valves in the line from the demineralized water system are closed and locked. These valves block the flow paths that can allow unborated makeup water to reach the RCS. Any makeup required during refueling uses borated water supplied from the boric acid tank by the CVS makeup pumps.

During refueling operations (Mode 6), two source-range neutron flux monitors are operable to monitor core reactivity. This is required by the plant Technical Specifications (SSAR chapter 16) (Reference 2.7-3). The two operable source-range neutron flux monitors provide a signal to alert the operator to unexpected changes in core reactivity. The potential for an uncontrolled boron dilution accident is precluded by isolating all unborated water sources. This is also required by the plant Technical Specifications.

2.7.3 Shutdown Operations

2.7.3.1 Plant Startup

Plant startup is the operation that brings the reactor plant from a cold shutdown condition to no-load operating temperature and pressure, and subsequently to power operation.

The makeup pumps initially fill the RCS via the purification flow return line. During filling, makeup water is drawn from the demineralized water connection and blended with boric acid from the boric acid tank to provide makeup at the desired RCS boron concentration. The RCS is vented via the reactor vessel head and the pressurizer. A vacuum fill subsystem may be used to enhance the reactor coolant fill operation. The RCS fill and vent operations are discussed in subsection 2.1.3.1 of this report. The role of the CVS for these operations is discussed in the following paragraphs.

The auxiliary spray line may be used to fill the pressurizer and establish proper water chemistry in the pressurizer. If water-solid operation is desired, RCS pressure is controlled by operation of the letdown control valve and the makeup control valve. To accomplish this, a letdown flow path is established to the liquid radwaste system with the letdown orifice bypassed. The makeup flow rate is maintained by the makeup control valve at a constant value selected by the operators. These water-solid operations are not required if vacuum fill is used.

After the RCPs are started, chemical treatment, such as hydrazine addition, is performed. Hydrazine is added to the reactor coolant during the initial stages of heatup to scavenge oxygen in the system. Subsequently, hydrogen makeup to the RCS will be started and the RCS hydrogen level brought up to the normal operating point of approximately 30 cc/ kg.

The pressurizer heaters are used to heat up the water in the pressurizer and draw a steam bubble. As the steam bubble grows, effluent will continue to be diverted to the liquid radwaste system through the CVS letdown line. The makeup pumps will be operated to supply demineralized water, so the RCS boron concentration can be reduced to the level required for criticality. Following attainment of pressurizer normal water level, the letdown flow control valve and makeup pumps will be set to operate only as necessary to maintain pressurizer level or on demand from the operator.

Criticality is achieved as follows:

- The RCS boron concentration is reduced to the calculated level by dilution, routing effluent from the CVS purification loop to the liquid radwaste system, and by provision of unborated makeup with the makeup pumps taking suction from the demineralized water storage tank.

- Chemical analysis is used to measure water quality, boron concentration, and hydrogen concentration.

- Appropriate control rods are withdrawn.

- Further adjustments in boron concentration will be necessary to establish preferred control group rod positions and to compensate for xenon buildup.

2.7.3.2 Hot Shutdown

If required for periods of maintenance or following spurious reactor trips, the reactor can be maintained subcritical, with the capability to return to full power within the period of time required to withdraw the control rods. During hot standby operation, the average temperature is maintained at no-load T_{avg} by initially dumping steam to the condenser to provide residual heat removal or at later stages by running the RCPs to maintain system temperature.

Initially, the control rods are inserted and the core is maintained at or slightly above the minimum required shutdown margin (1% Δk/k). Following shutdown, xenon buildup occurs and increases the shutdown margin. The effect of xenon buildup increases the shutdown margin to a minimum of about 3 percent Δk/k at about 9 hours following shutdown. If rapid recovery is required, dilution of the system may be performed via the CVS to counteract this xenon buildup. A shutdown group of rods must be withdrawn during dilution to provide the capability for rapid shutdown if needed, and frequent checks are made on critical rod position.

2.7.3.3 Cold Shutdown

Cold shutdown consists of the operations that bring the reactor plant from normal operating temperature and pressure to a cold shutdown temperature and pressure for maintenance or refueling.

The CVS purification loop will continue to operate normally in advance of a planned shutdown. In addition, in the beginning of a shutdown, the CVS is designed so the letdown flow is routed out of containment to the liquid radwaste system, where it is stripped of gases and returned to the makeup pump suction. This gas stripping is effective and is required for approximately 48 hours to reduce the reactor coolant activity level and hydrogen level sufficiently to permit personnel access for refueling or maintenance operations.

Before cooldown and depressurization of the RCS is initiated, the reactor coolant boron concentration is increased to the cold shutdown value. The operator sets the reactor makeup control to "borate" and selects the volume of boric acid solution necessary to perform the boration. Correct concentration is verified by reactor coolant samples. The operator sets the reactor makeup control for makeup at the shutdown reactor coolant boron concentration.

Contraction of the coolant during cooldown of the RCS results in actuation of the pressurizer level control system to maintain normal pressurizer water level. Makeup continues to be automatic with the makeup pumps starting and stopping as required.

During shutdowns, after the RCPs are stopped, the RNS provides the motive force for the CVS purification loop. Whenever the RCS is pressurized, the CVS can be operated to provide purification. After the RNS is placed in service and the RCPs are shut down, further cooling and depressurization of the pressurizer fluids are accomplished by makeup through the auxiliary spray connection.

2.7.4 References

2.7-1 *AP600 Standard Safety Analysis Report,* Chapter 9, "Auxiliary Systems."

2.7-2 *AP600 Standard Safety Analysis Report,* Chapter 15, "Accident Analysis."

2.7-3 *AP600 Standard Safety Analysis Report,* Chapter 16, "Technical Specifications."

2.8 SPENT FUEL POOL COOLING SYSTEM

2.8.1 System Description

The SFS is discussed in SSAR subsection 9.1.3 (Reference 2.8-1). The SFS includes two mechanical trains of equipment (see Figure 2.8-1, based on the SSAR chapter 9 SFS description). Each train includes one spent fuel pool pump, one heat exchanger, one demineralizer, and one filter. In addition, the SFS consists of piping, valves, and instrumentation necessary for correct system operation. The two trains of equipment share common suction and discharge headers. Either train of equipment can be operated to perform any of its functions independently of the other train. One train can be continuously cooling and purifying the spent fuel pool while the other train can be available for water transfers and IRWST purification, or aligned as a backup to the operating train of equipment.

The two SFS trains use different power supplies, which are backed up by offsite and onsite supplies. This allows a higher system availability for the cooling function.

The SFS pumps take suction from the suction header and discharge directly to their respective heat exchangers. The heat exchanger outlet piping branches into parallel lines. The purification branch is designed for 250 gpm purification flow while the bypass branch passes the remaining 500 gpm.

Each purification branch is routed directly to an SFS demineralizer. The demineralizer is sized to provide a minimum of one fuel cycle of service before ion exchange media replacement. The outlet of the demineralizer is routed to a filter that collects particulates and resin fines passed by the demineralizer. The outlet of the filter is connected to the bypass branch to form a common line that leads to the discharge header.

Cooling and purification of the following pools is possible:

- The spent fuel pool has two connections. The main suction line connects to the spent fuel pool at an elevation 4 feet below the normal water level of the pool (6 feet below the operating deck). This line is also connected to two skimmer/strainer assemblies that take suction from the water surface of the spent fuel pool. The second connection is 4 feet below the SFS pump suction connection (10 feet below the operating deck). This line is seismically qualified, safety Class C piping, which leads to the RNS pump suction header. This lower connection is normally isolated. This suction arrangement prevents the spent fuel pool from being inadvertently drained below the minimum level needed to meet the safety design criteria.

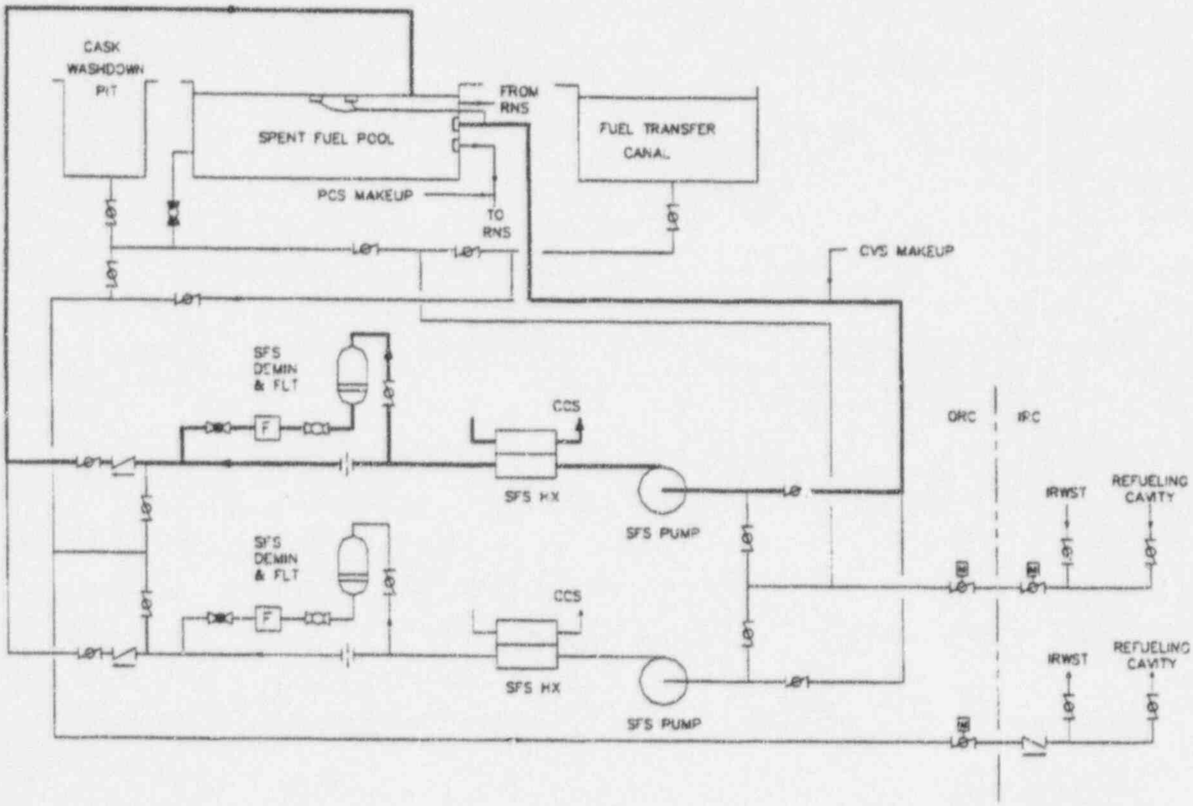


Figure 2.8-1 Spent Fuel Pool Cooling System

- The suction of the SFS pumps may be aligned to the IRWST and the refueling cavity. The SFS suction header from the refueling cavity is connected at two locations. The main line is located on the bottom of the cavity to ensure complete draining. The second line is connected to two skimmer/strainer assemblies, which take suction from the refueling cavity water surface. These connections enable purification of the refueling cavity and allow transfer of water between the IRWST and the refueling cavity. The SFS suction header from the IRWST is located at the bottom of the tank.

- The fuel transfer canal (FTC), the cask loading pit (CLP), and the cask washdown pit (CWP) all have bottom connections. These connections are provided primarily for the transfer of water from the FTC to the CLP and CWP for either maintenance of the FTC or for CLP operations. Water that is normally stored in the FTC can be sent to the CLP and vice versa.

The cooled water is returned to the following pools:

- The spent fuel pool has two connections. The SFS return is made at the opposite end of the pool from which suction is taken to recirculate the water for cooling and purification. The RNS return is seismically qualified, safety Class C piping, which leads from the RNS pump discharge header. The return line to this connection is normally isolated.

- The SFS pump discharge may be directed to the FTC to transfer back water from the CLP and CWP. The SFS pump discharge may be directed to the CLP and CWP. These pits may filled with borated water from the FTC for spent fuel assemblies underwater loading in the pit and cask washdown before shipment.

- The SFS pump discharge may be directed to the refueling cavity for water transfer from the IRWST and for refueling cavity purification during refueling operations. The SFS pump discharge may also be directed to the IRWST for water transfer from the refueling cavity to the IRWST after refueling and for IRWST purification prior to refueling.

- The SFS pump discharge may be directed to the integrated head storage stand (IHST). The IHST is filled with water from the IRWST during refueling outages before removing the vessel head. The water is used for radiation shielding when the integrated head package is on the stand and the incore instrumentation thimbles are submerged. A drain line at the bottom drains the water back into the IRWST via gravity.

Where necessary, these return lines are equipped with flow-limiting orifices to prevent pump runout.

The SFS suction and return lines to the IRWST and refueling cavity penetrate the primary containment and are arranged for the containment isolation function. Low-low water level alarm in the spent fuel pool will cause these containment supply and return lines to be isolated.

The containment penetration line on the pump suction has one automatic motor-operated butterfly valve located inside containment and one automatic motor-operated butterfly valve located outside the containment. The butterfly valve design permits a controlled leakage, which provides the thermal relief function in the piping portion between the containment isolation valves.

The containment penetration line on the pump discharge has one automatic motor-operated isolation valve outside of containment and one check valve inside containment. The check valve performs the thermal relief function in the piping portion between the containment isolation valves.

Each penetration line is provided with the test boundary valves, test connections, and test vent lines to allow leak-testing.

The normal makeup source of borated water for the spent fuel pool is provided by the CVS. The primary demineralized water source for compensating the water losses from evaporation is also provided by the CVS. An alternate source of demineralized water may be provided from the demineralized water transfer and storage system.

For postulated events, a safety-related, seismically qualified connection for emergency makeup from the PCS water storage tank is provided to guarantee a supply of water for 7 days after loss of normal cooling. (See Table 2.8-1.) This line is normally isolated by a locked, closed valve and closed spectacle flange set and is connected to the RNS pump suction line. Alignment of the emergency makeup flow path is performed in a protected area to permit the operator to align this connection in the suitable environmental and radiological conditions not affected by the pool boiling and by the lowered pool level.

The normal level in the spent fuel pool is 2 feet below the operating deck level to prevent flooding of the operating deck due to errors during makeup operation or water transfer. Prior to spent fuel pool overflow onto the operating deck, spent fuel pool overflow will be collected in the CLP because the tops of the gates between the spent fuel pool-FTC and spent fuel pool-CLP are purposely located 6 inches below the auxiliary building operating deck.

Table 2.8-1
Required Passive Cooling Water Sources

Case	Condition	Fuel in Spent Fuel Pool[1]	Water Supplies [2]				Notes
			Spent Fuel Pool	FTC and Gate	CWP[3]	PCS Tank	
1	Emergency Full-core off-load	1 Core at 150 hrs, 1/3 Core at 17 Days	X	X	X	X	PCS tank water not needed for containment cooling
2	Refueling	1 Core at 150 hrs	X	X	X	X	PCS tank water not needed for containment cooling
3	Refueling	1/3 Core at 150 hrs	X	X	X		Decay heat in spent fuel pool < 3.00 MWt[4]
4	Power	1/3 Core at 17 Days	X	X			Decay heat in spent fuel pool < 2.13 MWt[4]
5	Power	1/3 Core at 32 Days	X				Decay heat in spent fuel pool < 1.50 MWt[4]

[1] All scenarios include 10 years of spent fuel in pool. Normal spent fuel pool cooling is lost because of the station blackout and seismic event which breaks the SFS pump suction line. The pool is initially drained to 6 feet below operating deck. Time references are to moment of shutdown.

[2] Wa*er sources required to support passive cooling of spent fuel pool for 7 days following event

[3] CWP is assumed filled to level 2 feet below normal spent fuel pool level.

[4] Decay heat rate at start of event

Other piping lines that are a part of the SFS system are as follows:

- A line that allows draining the refueling cavity to the SGS compartment. This line is provided with an isolation valve that is closed only immediately before refueling operations. During the other plant conditions, it is locked open to prevent filling the refueling cavity during an accident. Hence, the valve operation is administratively controlled. The drain elevation allows accommodation of the possible estimated IRWST overflow (38,200 gallons) without draining to the SGS during the non-refueling plant conditions.

- A connection line from the spent fuel pool to the CVS makeup pump that allows use of the spent fuel pool borated water as a backup source of RCS makeup for the CVS.

The SFS is equipped with instrumentation to provide control and supervision of the system functions during all of its operating modes. Monitoring capability is provided for the heat transfer and purification processes, as well the status of the spent fuel pool water inventory and enthalpy. The possibility of loss of water from the system is also monitored and alarms are provided to alert the operators of the need to isolate and terminate a spent fuel pool water inventory depletion.

2.8.2 Design Features to Address Shutdown Safety

The AP600 has incorporated various design features to improve shutdown safety. The SFS features that have been incorporated to address shutdown safety are described in this subsection.

2.8.2.1 Seismic Design

The spent fuel pool, FTC, CLP, CWP, and gates from the spent fuel pool-CLP and FTC-spent fuel pool are all integral with the auxiliary building structure. The auxiliary building is seismic Class I design and will retain its integrity when exposed to a safe shutdown earthquake (SSE). The suction and discharge connections between the spent fuel pool and RNS are safety Class C, which is also seismic Class I. The emergency makeup water line from the PCS water storage tank to the spent fuel pool actually connects with the RNS pump suction line. This emergency makeup line is also safety Class C and seismic Class I. The spent fuel pool level instruments connections to the spent fuel pool are safety Class C, seismic Class I, and have 3/8-inch flow restricting orifices at the pool wall to limit the amount of a leak from the pool if the instrument or its piping develops a leak.

The refueling cavity, as discussed in SSAR subsection 3.8.3.1.3 (Reference 2.8-2), is integral with the containment internal structure, and as such, is seismic Class I, and will retain its integrity when exposed to an SSE. In addition, the AP600 has incorporated a permanently welded seal ring to provide the seal between the vessel flange and the refueling cavity floor. This refueling cavity seal is part of the refueling cavity and is seismic Class I.

2.8.2.2 Instrumentation

The spent fuel pool level is measured by three redundant, safety-related 1E, differential pressure level sensors. These instruments receive power from power divisions A, B, and C. Low-low level alarm from two out of three instruments is required to automatically close the SFS containment isolation valves. The three spent fuel pool level instruments are included in the post-accident monitoring system (PAMS).

2.8.2.3 Emergency Makeup

The normal supply of borated or demineralized makeup water to the spent fuel pool comes from the CVS, and an alternate source of demineralized water can be received from the demineralized water transfer and storage system. When these sources of makeup are not available, the PCS water storage tank is used for emergency makeup to the spent fuel pool. The emergency makeup line is safety Class C, seismic Class I. The PCS water is isolated from the spent fuel pool by a locked, closed globe valve and a closed spectacle flange set in the emergency makeup line. These provisions are necessary to prevent inadvertent draining of the PCS tank. Alignment of the emergency makeup flow path requires opening the spectacle flange set prior to opening the globe valve. The rate of makeup can be controlled by throttling the globe valve to prevent over filling the pool.

2.8.2.4 Diverse Cooling

The SFS has sufficient cooling capacity to maintain the spent fuel pool temperature at 120°F when the full core has been off-loaded into the spent fuel pool, which is occupied with 10 years of spent fuel when both trains are operating. In the event of a failure that causes the loss of one train, the RNS can be aligned to the spent fuel pool and share or take over the spent fuel pool cooling duty. Although the RNS is not a safety-related system, the RNS piping and components are safety Class C, seismic Class I, for RCS pressure boundary. If offsite power is available, the CCS and service water system are operational, and if the normal SFS cooling is not available, the RNS can perform the spent fuel pool cooling.

2.8.2.5 Containment Isolation

The safety-related functions of the SFS include containment isolation of the SFS lines that penetrate containment. The valves that perform this safety-related containment isolation function are described in the system description.

2.8.3 Shutdown Operation

2.8.3.1 Normal Plant Shutdown

Plant shutdown is defined as the operation that brings the reactor plant from normal operating temperature and pressure to cold (ambient) conditions. During this phase, one SFS train is aligned to provide spent fuel pool cooling and purification, while the other train is in standby or aligned to purify the refueling water in the IRWST to prepare this water for refueling.

2.8.3.2 Refueling

Both SFS mechanical trains are normally in operation during refueling. One train is aligned for spent fuel pool cooling and purification throughout the refueling. The other train performs various functions during the refueling.

When one train is in operation to purify the water in the IRWST, its pump is stopped when the refueling cavity is ready to be flooded. Valves are aligned to initially gravity-drain the IRWST to the refueling cavity. Eventually the drain rate will slow, and the IRWST and the refueling cavity will have the same water level. At this time, the pump and valves are aligned to transfer the remaining IRWST water into the refueling cavity.

The AP600 water transfer sequence has been developed to improve water clarity in the refueling cavity during refueling operations. Conventional PWRs have performed this function with their residual heat removal system by flooding up through the reactor vessel into the refueling cavity, which has caused water clarity problems. Using the SFS for this transfer reduces the chance of misaligning the RNS and losing core cooling.

Once the refueling cavity has been flooded, the train is re-aligned to purify the refueling cavity. Both trains of pumps and heat exchangers can be aligned at any time, if needed, to cool the spent fuel pool.

At the completion of the refueling, one pump is used to transfer the water in the refueling cavity back to the IRWST. Once this is complete, the train can be aligned to cool the spent fuel pool or may be placed in standby.

The standby train can be used to transfer water from the FTC to the CLP. This lined, reinforced concrete structure is provided for underwater loading of fuel into a shipping cask and cask draining/decontamination prior to cask shipment from the AP600 site.

2.8.3.3 Operation During Normal Plant Transients and Accidents

The AP600 SFS is not required to continue normal spent fuel pool cooling following design basis events. In the event of an accident involving loss of the normal spent fuel pool cooling by heat exchange to the CCS, the spent fuel cooling is provided by the heat capacity of the water in the pool. Connections to the spent fuel pool are made at elevations that preclude the possibility of inadvertently draining the water in the pool to an unacceptable level. The safety analysis has been performed assuming the spent fuel pool drains to the level of the SFS pump suction connection due to broken piping. In addition, a safety Class C connection from the PCS water storage tank permits emergency makeup to the spent fuel pool when needed following a design basis event (including seismic).

Recovery of normal SFS cooling, or use of RNS cooling of the spent fuel pool after the pool has been boiling, must be accomplished in the following steps:

1. Fill the pool to the normal high level (1 foot below the operating deck). If the pool level cannot be filled above the normal SFS pump suction line connection because a

seismic event has broken the piping, fill the pool to the level of the SFS pump suction connection.

2. Isolate the purification line to the demineralizer in the SFS train to be used for cooling. This step is not applicable for situations where the RNS will be used for pool cooling. This action prevents degradation of the demineralizer ion exchange resin due to exposure to high-temperature water.

3. Start the SFS pump to force the spent fuel poo' vater through the heat exchanger. If the RNS is to be used for spent fuel pool cooling, the normally locked closed isolation valves between the spent fuel pool and the RNS suction and discharge headers must be opened prior to starting an RNS pump.

The SFS pump suction connection has been set 4 feet below the normal spent fuel pool level and the RNS pump suction connection, 4 feet below the SFS pump suction connection to prevent saturated pool water from flashing when the flow starts.

Loss of Offsite Power

The SFS pumps are connected to the standby diesel in the event of a loss of offsite power. The supporting CCS and service water system are also loaded onto the standby diesel. The SFS is capable of providing spent fuel pool cooling following this event.

Station Blackout

- Required boiling water inventory

  The FTC is normally connected to the spent fuel pool with the gate between them open. The entire water inventory of the spent fuel pool plus the water above the gate and the water in the FTC above the level of the gate are available for heatup. This volume of water, less the amount in the spent fuel pool below the top of the fuel racks, is available for heat removal by boiling. The spent fuel pool water is the only water needed to maintain for spent fuel cooling the spent fuel pool for 7 days when the decay heat rate is <2.15 MWt. The FTC may be isolated and drained for maintenance of the fuel handling equipment if necessary.

  During refueling operations when the rate of decay heat into the pool is relatively high, > 3.00 MWt, the CWP must be filled with water and be available for emergency makeup. The CWP will drain by gravity into the spent fuel pool when the valves between the spent fuel pool and CWP are opened. If the spent fuel pool has drained to the level of the SFS pump suction connection due to broken piping, the valves are not aligned for gravity drain until the spent fuel pool level has boiled down about

2 feet below the SFS pump suction connection. Premature alignment of emergency water from the CWP will allow the CWP water to fill the spent fuel pool to the SFS pump suction connection level and spill the excess, making it unavailable for fuel cooling.

When one-third of the reactor vessel fuel has been moved into the spent fuel pool, the PCS water storage tank is no longer needed for containment cooling. If an accident occurs that requires closure of containment, air cooling of containment is sufficient to keep the containment pressure under the design pressure of the containment vessel. The PCS water must be available for spent fuel pool emergency makeup when one-third or more of the fuel has been transferred to the spent fuel pool.

Table 2.8-2 provides the times before boiling occurs in the pool and the depth of water above the fuel, 7 days after a station blackout or a seismic event for various scenarios. Table 2.8-2 also provides the minimum level requirement to keep the spent fuel covered, assuming the maximum heat load conditions is met in all scenarios.

Fuel cooling function after 7 days can be performed in either of two ways:

- Refilling the pool using the emergency makeup from the PCS water storage tank. Extended cooling will require pumping a supply of water into the PCS tank using a flow path located in a protected area where the environment and the dose are suitable for operator action.

- Restoration of normal SFS cooling. The remote start of one pump is sufficient because all the valves are already aligned.

- Fuel handling area ventilation

The normal ventilation of the auxiliary building fuel handling area contains provisions to cope with the steam produced by a boiling spent fuel pool. These provisions prevent pressurization of the building. Direct venting of the boiling spent fuel pool steam without filtering or other processing has been shown to be acceptable and in compliance with 10 CFR 20 (Reference 2.8-3) dose limits at the site boundary. This venting is described in SSAR section 15.7 (Reference 2.8-4) and in section 4.8 of this report.

Table 2.8-2
Spent Fuel Protection

Case	Condition	Time to Saturation (hours)	Fuel Cov.r at 7 days (feet)	Additional Time to Expose Top of Fuel
1	Emergency Full-core Off-load	4.6	8.25 [1]	3.4 days
2	Refueling	5.4	8.25 [1]	5.7 days
3	Refueling	14.6	0.48	4.3 hours
4	Power	20.1	6.69	2.3 days
5	Power	23.2	1.78	12.9 hours

[1] PCS makeup water can be throttled to provide any depth of cover above the fuel.

Abnormal System Conditions

- Failure of an SFS pump

  A high spent fuel pool temperature and/or a low-flow alarm during normal spent fuel pool cooling operations (that is, single-train operation) alerts the plant operators of an SFS pump failure. Due to the heat capacity of the water in the spent fuel pool, sufficient time exists for the operators to manually align the standby SFS train of equipment (pump/heat exchanger) to continue spent fuel pool cooling. In case both trains are operating, the low-flow alarm allows operators to identify the failed pump.

- Leakage from the spent fuel pool

  Leakage from the spent fuel pool is identified by a low-level alarm in the spent fuel pool. The operator can align the CVS to compensate for a 100-gpm leakage rate. Adding borated water from the CVS permits matching the boron concentration in the pool. The spent fuel pool is borated to preclude a positive reactivity excursion due to boron dilution when the spent fuel pool is joined to the refueling cavity during refueling operations. The spent fuel pool fuel storage racks will maintain the fuel at less than 0.95 reactivity when fuel positions are occupied with maximum enriched fuel and no boron is in the water. Adding demineralized water to the spent fuel pool from the demineralized water transfer and storage system results in boron concentration reduction.

  The connections to the spent fuel pool are located at an elevation such that piping leakage will not result in the pool water level falling to unacceptable levels. The heat capacity of the water in the pool is sufficient to allow the operators enough time to locate a leak and repair it. Normally, cooling will be maintained by operation of one train of equipment.

The spent fuel pool level instruments connections to the spent fuel pool are made at a level just above the top of the fuel racks. These connections have a 3/8-inch flow restricting orifices at the pool wall to limit the amount of a leak from the pool if the instrument or its piping develops a leak.

2.8.4 References

2.8-1 *AP600 Standard Safety Analysis Report*, Chapter 9, "Auxiliary Systems."

2.8-2 *AP600 Standard Safety Analysis Report*, Chapter 3, "Design of Structures, Components, Equipment and Systems."

2.8-3 Title 10, Code of Federal Regulations, Part 20, "Standards for Protection Against Radiation," January 1, 1996.

2.8-4 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

2.9 CONTROL AND PROTECTION SYSTEMS

The AP600 control and protection systems support the operations necessary for the AP600 to achieve shutdown. These systems consist of a nonsafety-related PLS, a safety-related PMS, and a nonsafety-related DAS. These systems and their significance for shutdown are discussed in the following subsections.

2.9.1 Plant Control System

The PLS provides the following functions:

- Reactor power control system

  The reactor power control system coordinates the responses of the various reactivity control mechanisms. The system enables daily load follow operation with a minimum of manual control by the operator. Load regulation and frequency control are compatible with the reactor power control system operation. Axial nuclear power distribution control is also performed by the reactor power control system.

- Rod control system

  The rod control system, in conjunction with the reactor power control system, maintains nuclear power and reactor coolant temperature, without challenges to the protection systems, during normal operating transients.

- Pressurizer pressure control

  The pressurizer pressure control system maintains or restores the pressurizer pressure to the nominal operating value following normal operating transients. The control system reacts to avoid challenges to the protection systems during these operating transients.

- Pressurizer water level control

  The pressurizer water level control system establishes, and maintains or restores pressurizer water level to its programmed value. The required water level is programmed as a function of RCS temperature and power generation to minimize charging and letdown requirements. No challenges to the protection system result from normal operational transients.

- Feedwater control system

  The feedwater control system maintains the steam generator water level at a predetermined setpoint during steady-state operation. It also maintains the water level within operating limits during normal transient operation. The feedwater control system restores normal water level following a unit trip. The various modes of feedwater addition are automated to require a minimum of operator involvement.

- Steam dump control

  The steam dump control system reacts to prevent a reactor trip following a sudden loss of electrical load. The steam dump control system also removes stored energy and residual heat following a reactor trip so that the plant can be brought to equilibrium no-load conditions without actuation of the steam generator safety valves. The steam dump control system also provides for maintaining the plant at no-load or low-load conditions to facilitate a controlled cooldown of the plant.

- Rapid power reduction

  For large, rapid load rejections (turbine trip or grid disconnect from 50-percent power or greater) a rapid nuclear power cutback is implemented. This results in a reduction of thermal power to a level that can be handled by the steam dump system.

- Defense-in-depth control

  The PLS provides control of systems performing defense-in-depth functions. SSAR Table 7.7-3 (Reference 2.9-1) provides a list of the defense-in-depth functions that are supported by the PLS.

Subsection 7.7.1 of the AP600 SSAR (Reference 2.9-1) is a detailed description of the functions performed by the PLS. The detailed description of the hardware that comprises the PLS is provided in SSAR subsection 7.1.3.

2.9.1.1 Design Features that Address Shutdown

The PLS provides control of nonsafety-related components required for shutdown operations. In general, PLS equipment that supports shutdown operations operates continually. For high system availability, the PLS is designed with internal redundancy and segmentation of major functions to separate hardware elements, and is powered by nonsafety-related, uninterruptible power. Portions of the PLS may be shut down when the functions performed by that portion of the PLS are not required, without affecting the portions of the PLS that remain operational.

Control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functicns performed by other controllers.

The distributed controllers receive process inputs and implement the system-level logic and control algorithms appropriate for the plant operating mode. The distributed controllers receive process inputs from, and transmit process control outputs to, the actuated components. The distributed controller also transmits and receives process signals via a redundant process bus. This process bus facilitates the receipt of process signals from the PMS via redundant signal selectors, provides for two-way communication between the individual distributed controllers, and provides for two-way communication between distributed controllers and the main control room and remote shutdown workstation.

Redundant signal selectors provide the PLS with the ability to obtain inputs from the integrated protection cabinets in the PMS. The signal selector function maintains the independence of the PLS and PMS. The signal selector subsystem redundancy serves two purposes: it protects against a failure disrupting the control system, and it provides the capability to remove one of the selectors from service for testing while maintaining normal control using data from the other selector.

2.9.1.2 Shutdown Operations

There are no special shutdown operations associated with the PLS. The PLS supports the shutdown operations of the other systems required to operate during shutdown including the following systems: reactor coolant, steam generator, feedwater, main steam, normal residual heat removal, passive core cooling, containment, passive containment cooling, chemical and volume control, and spent fuel cooling.

2.9.2 Protection and Safety Monitoring System

2.9.2.1 System Description

The PMS provides the safety-related functions necessary to control the plant during normal operation, to shut down the plant, and to maintain the plant in a safe shutdown condition. The PMS controls plant safety-related components that are operated from the main control room or remote shutdown workstation. In addition, the PMS provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97 (Reference 2.9-2).

Reactor Trip

Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip. Analog signals are converted to digital form by analog-to-digital converters within the integrated protection cabinets. Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if one channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system. Each division sends its partial trip status to each of the other three divisions over isolated multiplexed data links. Each division is capable of generating a reactor trip signal if two or more of the redundant channels of a single variable are in the partial trip state.

The reactor trip signal from each of the four integrated protection cabinets is sent to the corresponding reactor trip switchgear breakers.

Each of the four reactor trip actuation divisions consists of two reactor trip circuit breakers. The reactor is tripped when two or more actuation divisions output a reactor trip signal. This automatic trip demand initiates the following two actions. It deenergizes the under-voltage trip attachments on the reactor trip breakers, and it energizes the shunt trip devices on the reactor trip breakers. Either action causes the breakers to trip. Opening the appropriate trip breakers removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion causes the reactor to shut down.

Engineered Safety Features Actuation

Four sensors normally monitor each variable used for an engineered safety feature (ESF) actuation. (These sensors may monitor the same variable for a reactor trip function.) Analog measurements are converted to digital form by analog-to-digital converters within each of the four integrated protection cabinets. Following required signal conditioning or processing, the measurements are compared against the setpoints for the ESF to be generated. When the measurement exceeds the setpoint, the output of the comparison results in a channel partial trip condition. The partial trip information is transmitted over isolated data links to the ESF actuation cabinets to form the signals that result in an ESF actuation. The voting logic is performed twice within each ESF actuation cabinet. Each voting logic element generates an actuation signal if the required coincidence of partial trips exists at its inputs.

The signals are combined within each ESF actuation cabinet to generate a system-level signal. System-level manual actions are also processed by the logic in each ESF actuation cabinet.

The system-level signals are then broken down to the individual actuation signals through the protection logic cabinets to actuate each component associated with a system-level ESF. For example, a single safeguards actuation signal must trip the reactor and the RCPs, align CMT and IRWST valves, and initiate containment isolation. The interposing logic within each protection logic cabinet accomplishes this function and also performs necessary interlocking so that components are properly aligned for safety. Component-level manual actions are also processed by this interposing logic. The component level logic, performed within the protection logic cabinets, is triple redundant. The component actuation outputs from the logic processors are combined with the power interface cards in a two-out-of-three voting logic. The power interface also transforms the low level signals to voltages and currents commensurate with the actuation devices they operate. The actuation devices, in turn, control motive power to the final ESF component.

A detailed description of the functions performed by the PMS is described in sections 7.2, 7.3, and 7.5 of the AP600 SSAR (Reference 2.9-1). The detailed description of the hardware that comprises the PMS is provided in SSAR subsection 7.1.2.

2.9.2.2 Design Features that Address Shutdown

The PMS provides the safety-relatea functions necessary to shut down the plant and to maintain the plant in a safe shutdown condition. The PMS controls safety-related components. In addition, the PMS provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97 (Reference 2.9-2). The PMS consists of redundant and independent hardware elements powered by safety-related, uninterruptible power. The availability of the PMS is controlled by the plant Technical Specifications, SSAR chapter 16 (Reference 2.9-3). These Technical Specifications provide for the following:

- Portions of the PMS that support reactor trip must be operable during all modes in which the reactor trip breakers are closed and the PLS is capable of rod withdrawal.

- Portions of the PMS that support ESFs must be operable during all modes in which the engineered safety feature must be available. In general, this requires that these portions of the PMS are operable under all plant operating conditions in which the reactor vessel head is in place.

- Portions of the PMS that support plant monitoring must be operable during all modes in which the occurrence of an accident, which may require most accident monitoring, is credible. In general, this requires that these portions of the PMS are operable during reactor operation and during hot standby conditions.

The PMS provides a high degree of reliability and fault tolerance. This capability is provided by the following design features:

- Two-out-of-four coincidence logic on reactor trip and most ESFs actuations provide that any failure in a single protection channel or safety division cannot cause a spurious reactor trip or spurious system-level ESF actuation. This same two-out-of-four logic also provides that any failure in a single protection channel or safety division cannot prevent a required reactor trip or system level ESF actuation from occurring. This provides tolerance against failures ranging from the failure of a single instrument or component to the complete failure of an entire integrated protection or ESF actuation cabinet.

- Reactor trip and ESF actuation logic reverts to two-out-of-three coincidence logic if one channel is bypassed or in test. Therefore, a single failure while in test cannot cause a spurious reactor trip or spurious system-level ESF actuation. This same two-out-of-three logic also provides that any failure in a single protection channel or safety division cannot prevent a required reactor trip or system-level ESF actuation from occurring.

- The voting logic for reactor trip functions is contained within each integrated protection cabinet. The reactor trip breakers operate on a de-energize-to-trip principle.

- ESF actuation logic is performed redundantly in each ESF actuation cabinet. Redundant microprocessor-based subsystems perform this logic so that a component failure related to one subsystem cannot affect the other redundant subsystem. The system-level actuation outputs are transmitted to the protection logic cabinets over two redundant data highways. A single data highway failure cannot prevent ESF actuation. Extensive error checking is performed on these data highways to minimize failures from causing spurious actuation.

- Component-level logic, performed within the protection logic cabinets, is triple redundant. Four redundant logic processor boards are provided along with two data highway controller boards. Two logic processor boards are associated with each data highway controller board. The logic processors are programmed to respond to actuation signals received from the data highways. Failure of one data highway or one data highway controller board does not prevent component-level actuations. Extensive error checking on the data highways is provided to minimize data highway failures from generating spurious ESF component-level actuations. The component actuation outputs from the logic processors are combined with the power interface cards in a two-out-of-three voting logic. This prevents the failure of a single logic processor from causing spurious actuation or preventing a required actuation.

During maintenance, these features allow the system to continue to operate with one channel or certain boards out of service. Any single integrated protection cabinet, ESF actuation cabinet, or transmitter associated with one trip or actuation channel may be taken out of service for maintenance without plant shutdown. The data highways connecting the ESF actuation cabinets, protection logic cabinets, and multiplexers are redundant. One of the redundant highways may be out of service, for maintenance, without directly causing plant shutdown. Because the logic processors and data highway controllers in the protection logic cabinets are redundant, one logic processor or data highway controller can be out of service, for maintenance, while the overall system remains operational.

2.9.2.3 Shutdown Operations

There are no special shutdown operations associated with the PMS. The PMS supports the shutdown operations of the other systems by remaining available during all periods in which the supported systems perform their shutdown operations.

2.9.3 Diverse Actuation System

2.9.3.1 System Description

The DAS is a nonsafety-related system that provides a diverse backup to some functions provided by the PMS. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS is designed to minimize its potential for spurious operation by using a two-out-of-two voting logic for actuation. The automatic actuation signals provided by the DAS are generated in a functionally diverse manner from the PMS actuation signals.

The diverse automatic actuations are as follows:

- Trip rods via the motor generator set, trip turbine and initiate the passive residual heat removal on low wide-range steam generator water level

- Initiate passive residual heat removal on high hot leg temperature

- Trip rods via the motor generator set, actuate the CMTs, and trip the RCPs on low pressurizer water level

- Isolate critical containment penetrations and start passive containment cooling water flow on high containment temperature

Critical containment penetrations are those lines that connect directly to the RCS, the containment atmosphere, or the containment sump.

The manual actuation function of the DAS is implemented by wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the control room multiplexers, the ESF actuation cabinets, the protection logic cabinets, and the DAS automatic logic.

The diverse manual functions areas follows:

- Reactor and turbine trip
- Passive residual heat removal actuation
- CMT actuation
- Automatic depressurization system valve actuation
- Passive containment cooling actuation
- Critical containment penetration isolation
- Containment hydrogen igniter actuation
- Initiation of IRWST injection
- Initiation of containment recirculation
- Initiation of IRWST drain to containment

For support of the diverse manual actuations, sensor outputs are displayed in the main control room in a manner that is diverse from the protection system display functions. The indications that are provided from at least two sensors per function are as follows:

- Steam generator water level—for reactor trip and passive residual heat removal actuations, and for overfill prevention by manual actuation of the ADS valves

- Hot leg temperature—for passive residual heat removal actuation

- Core exit temperature—for ADS actuation and subsequent initiation of IRWST injection

- Pressurizer level—for CMT actuation and RCP trip

- Containment temperature—for containment isolation and PCS actuation

- Containment hydrogen—for containment hydrogen igniter actuation

Additional information on the DAS is provided in subsection 7.7.11 of the AP600 SSAR (Reference 2.9-1).

2.9.3.2 Design Features that Address Shutdown

The DAS is intended to be operable under all plant operating conditions in which the reactor vessel head is in place.

The DAS automatic actuation processors are provided with the capability for channel calibration and testing while the plant is operating.

The DAS uses sensors that are separate from those being used by the PMS and the PLS. This prohibits failures from propagating to the other plant systems through the use of shared sensors.

There is signal isolation between the two subsystems within the DAS, one for each input and output path. These isolators are characterized by a high common mode voltage withstand capability to provide the necessary isolation against faults. The configuration is set up such that the isolation devices are capable of protecting against fault propagation between the DAS subsystems.

The DAS actuation devices are isolated from the PMS actuation devices to avoid adverse interactions between the two systems. The actuation devices of each system are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function. This type of interface also prevents the failure of an actuation device in one system from propagating a failure into the other system.

The DAS and the PMS use independent and separate uninterruptible power supplies.

2.9.3.3 Shutdown Operations

There are no special shutdown operations associated with the DAS. The DAS remains operational and is capable of performing its functions during all plant operating conditions in which the reactor vessel head is in place.

2.9.4 References

2.9-1 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

2.9-2 NRC Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Revision 3, May 1983.

2.9-3 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

3.0 SHUTDOWN MAINTENANCE GUIDELINES AND PROCEDURES

This section presents an overview discussion of AP600 shutdown maintenance guidelines and procedures captured as part of the AP600 design and design certification program. Shutdown maintenance requirements and guidelines have been identified in various licensing submittals, such as the AP600 Technical Specifications, *AP600 Standard Safety Analysis Report* (SSAR), section 16.1 (Reference 3.0-1), the design reliability assurance program, SSAR section 16.2, the AP600 implementation of the regulatory treatment of nonsafety systems (RTNSS) process (WCAP-13856) (Reference 3.0-2), and the *AP600 Probabilistic Risk Assessment* (PRA) (Reference 3.0-3).

In addition, other insights have been made based on the past experience of operating pressurized water reactors (PWRs) as discussed in the various licensing and industry documents, such as Generic Letter 88-17 (Reference 3.0-4), NUREG-1449 (Reference 3.0-5), NUMARC 91-06 (Reference 3.0-6), and *EPRI Advanced Light Water Reactor Utility Requirements Document* (Rererence 3.0-7). Shutdown procedures have been addressed in the AP600 design certification program by the submittal of the AP600 Emergency Response Guidelines (ERGs) (Reference 3.0-8), which include shutdown emergency procedures.

While ultimately the responsibility of shutdown maintenance and shutdown risk management is the responsibility of the combined operating license (COL) applicant, this section summarizes the major shutdown maintenance guidelines and procedures that have been identified in the various submittals discussed above as part of the AP600 design and design certification program.

3.0.1 References

3.0-1 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

3.0-2 WCAP-13856, *AP600 Implementation of the Regulatory Treatment of Nonsafety Related Systems (RTNSS) Process Summary Report*, September 1993.

3.0-3 *AP600 Probabilistic Risk Assessment*, September 30, 1996.

3.0-4 NRC Generic Letter 88-17, "Loss of Decay Heat Removal," 10 CFR 50.54(f).

3.0-5 NUREG-1449, *Shutdown and Low Power Operations at Commercial Nuclear Power Plants in the United States*, September 1993.

3.0-6 NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," December 1991.

3.0-7 *EPRI Advanced Light Water Reactor Utility Requirements Document*, NP-6780-L, Revisions 5 and 6, December 1993.

3.0-8 NSD-NRC-97-4936 (DCP/NRC0702), *Submittal of AP600 Emergency Response Guidelines*, Revision 2, January 10, 1997.

3.1 MAINTENANCE GUIDELINES AND INSIGHTS IMPORTANT TO REDUCING SHUTDOWN RISK

This section presents an overview of AP600 shutdown maintenance guidelines and insights, captured as part of the AP600 design and design certification program, which are either required for plant safety or are effective at reducing shutdown risk.

3.1.1 Availability Requirements for Safety-Related Systems

Availability controls of the AP600 safety-related systems are provided by the SSAR Technical Specifications (Reference 3.1-1). Table 2.3-1 of this report summarizes the availability of the safety-related systems required by the Technical Specifications. These availability requirements cover all modes of operation including shutdown.

3.1.2 Availability Guidelines for RTNSS-Important Systems

As discussed in the AP600 Design Reliability Assurance Program, SSAR section 16.2 (Reference 3.1-1), the AP600 implementation of the RTNSS process (WCAP-13856) (Reference 3.1-2) identified short-term availability controls for those nonsafety-related systems, structures, and components that perform functions identified as important in the RTNSS process. These recommendations include the operational modes when the systems are risk-significant, recommended modes for extended maintenance operations on the systems, and remedial actions if the system is not available. While WCAP-13856 provides the designer with recommendations for the RTNSS-important systems as they relate to shutdown risk, Table 3.1-1 provides a summary of the top level requirements for short-term availability recommendations.

3.1.3 Reactor Coolant System Precautions and Limitations at Shutdown

Precautions and limitations for RCS operation at shutdown are considered to minimize the risk to plant safety at shutdown. The most important of these are captured in the AP600 Technical Specifications. However, other precautions and limitations associated with maintenance and operation at shutdown have been identified during the design of the AP600. These are based on both the past operating experience of PWRs, as well as the designer's experience of the unique AP600 design features. A summary of these precautions and limitations that apply to shutdown maintenance and operation is provided in this section.

Table 3.1-1 Summary of Designer Recommendations for RTNSS-Important Nonsafety-related Systems that Apply to Shutdown

System	Normal Operating Modes	Recommended Operating Mode to Perform Planned Maintenance	Short-term Availability Recommendations	Remedial Actions
Normal Residual Heat Removal System	4 - 6	1	Both RNS subsystems should be available during RCS reduced inventory operations[1] when they are required for decay heat removal.	If both RNS subsystems are not available, the plant should not initiate reduced RCS inventory operations. If both subsystems cannot be maintained operable throughout reduced inventory operations, actions should be taken to restore system conditions.
Component Cooling Water System	1 - 6	1	Both CCS subsystems should be available to remove heat from the RNS heat exchangers and pumps during reduced RCS inventory operations[1] when the RNS is required for decay heat removal.	If both CCS subsystems are not available, the plant should not initiate reduced RCS inventory operations. If both subsystems cannot be maintained operable throughout reduced inventory operations, actions should be taken to restore system conditions.
Service Water System	1 - 6	1	Both service water system subsystems should be available to remove heat from the CCS heat exchangers and pumps during reduced RCS inventory operations[1] when the RNS is required for decay heat removal.	If both service water system subsystems are not available, the plant should not initiate reduced RCS inventory operations. If both subsystems can not be maintained operable throughout reduced inventory operations, actions should be taken to restore system conditions.

1. Reduced RCS inventory operations are defined as Mode 5, with no visible water level in the pressurizer, and Mode 6, with the refueling cavity less than full, and the upper internals in place.

Table 3.1-1 (cont.)
Summary of Designer Recommendations for RTNSS-Important Nonsafety-related Systems that Apply to Shutdown

System	Normal Operating Modes	Recommended Operating Mode to Perform Planned Maintenance	Short-term Availability Recommendations	Remedial Actions
ac Power	1 - 6	Onsite standby diesel generators - Mode 1 Other power supplies (main step-up, unit auxiliary, and reserve auxiliary transformers) - Modes 2, 3, or 6 (without reduced RCS inventory conditions)	Power required for RNS operation and required support system operation should be available during reduced RCS inventory operations. A minimum of three of the following four power supplies should be available, including one standby diesel generator and one offsite power supply. • Main step-up transformer and unit auxiliary transformer supply from the transmission switchyard • Reserve auxiliary transformer supply from the transmission switchyard • Two onsite standby diesel generators	If these power supplies are not available as described under "recommendations," the plant should not initiate reduced RCS inventory operations. If the plant has already entered reduced inventory operations, then the plant should take action to restore power supply operation.

1. Reduced RCS inventory operations are defined as Mode 5, with no visible water level in the pressurizer, and Mode 6, with the refueling cavity less than full, and the upper internals in place.

3.1.3.1 General Shutdown

Precautions and limitations for general shutdown are as follows:

- To ensure thorough mixing, at least one reactor coolant pump (RCP) or a normal residual heat removal pump should be in service while chemicals are being added to the system or the boron concentration is being changed. This requirement is included in the AP600 Technical Specification 3.3.9 (Reference 3.1-1).

- Reactor coolant samples must be taken at the regular intervals to check coolant chemistry, activity level, and boron concentration as specified in the various appropriate Technical Specifications including 3.1.1, 3.4.11, and 3.1-1. In addition, during shutdown modes, more frequent checks on RCS boron concentration should be made when changes in RCS boron concentration are being made.

- When the RNS is in operation, the reactor coolant temperature should not exceed 350°F. The reactor coolant pressure should be limited to avoid approaching the RNS relief valve setpoint.

- The maximum allowable heatup and cooldown rates for the RCS are provided in the Technical Specifications. An administrative limit of 50°F/hour is recommended.

- During cooldown, the RCPs located in the loop containing the spray line should be operated to ensure adequate pressurizer spray.

3.1.3.2 Water-Solid Operation

Precautions and limitations for water-solid operation are as follows:

- The RNS inlet line cannot be isolated from the reactor coolant loop unless there is a steam bubble in the pressurizer or the makeup pumps are stopped. This precaution is to ensure there is a relief valve protecting the RCS when it is at low pressure and water-solid.

- Whenever the plant is water-solid and the reactor coolant pressure is being maintained by the low-pressure letdown control valve, the RNS should remain open to the reactor coolant loops to maintain sufficient letdown flow through the bypass line from the RNS to the letdown heat exchanger, until a steam bubble is formed in the pressurizer. During this mode of operation, the isolation valve in the bypass line from the RNS to the letdown heat exchanger should be in the full-open position and the letdown orifice bypass valve must also be open.

- If all RCPs are stopped and the reactor coolant temperature is greater than 200°F, the first pump cannot be restarted until a steam bubble has formed in the pressurizer. This precaution will minimize the pressure transient when the first pump is started. The steam bubble will accommodate the resultant expansion.

- When the reactor coolant pressure is being maintained by the low pressure letdown control valve, changes to the flow rate through the RNS loop by throttling of valves or starting and stopping the RNS pumps will result in changes to the reactor coolant pressure.

- Whenever the reactor coolant temperature is above 160°F, at least one RCP should be in operation.

3.1.3.3 Steam Generators

Precautions and limitations for steam generators are as follows:

- During cooldown, all steam generators should be connected to the steam header to ensure uniform cooldown of the reactor coolant loops.

- During steam plant warmup and at hot standby, draw steam slowly and regulate feedwater additions carefully to avoid rapid cooling of the reactor coolant.

- During cooldown, once RNS is in operation, and after the RCPs have been tripped, actions should be taken to cool the contents of the steam generator secondary side, either by recirculation and cooling of this water or by draining the contents via the blowdown lines.

3.1.3.4 Surge Line

During heatup and cooldowns, the temperature difference between the pressurizer and the hot legs should be less than 320°F. This prevents unacceptable stress levels in the surge line.

3.1.3.5 Reduced-Inventory Operations

Precautions and limitations for reduced-inventory operations are as follows:

- After maintenance operations that result in draining the RCS, the system should be refilled with borated makeup water at the prevailing RCS boron concentration via the chemical and volume control system (CVS) makeup pumps. If the RCPs are drained, the pumps should be refilled with borated water via the pump drain line so that the pump is completely filled with borated water. The operators should not inadvertently fill the pump with unborated demineralized water.

- After maintenance operations on the CVS purification loop (demineralizer, filters, and heat exchangers), the system should be purged, draining any potential unborated water to the liquid radwaste system, and refilling it with borated water from the RCS. These operations should not be conducted at mid-loop or reduced inventory operations to avoid an inadvertent drop in RCS water level during mid-loop.

- The RCS hot leg level instruments should be operable and available prior to reduced inventory operations. Their automatic actuation functions are required to be operable in shutdown modes as described in Technical Specification 3.3.2.

3.1.4 References

3.1-1 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

3.1-2 WCAP-13856, *AP600 Implementation of the Regulatory Treatment of Nonsafety Related Systems (RTNSS) Process Summary Report*, September 1993.

3.2 SHUTDOWN RISK MANAGEMENT

While a discussion of industry planning documents is not included in the scope of this report, this report contains insights of which Westinghouse is currently aware and which are related to AP600 design certification. A search for insights is included in the plant shutdown risk management program, which is a post-design certification activity.

3.3 SHUTDOWN EMERGENCY RESPONSE GUIDELINES OVERVIEW

The AP600 shutdown ERGs (Reference 3.3-1) provide functional guidance for responding to accidents and transients that affect plant safety during shutdown modes of operation (operational Modes 5 and 6). The shutdown ERGs consist of a shutdown safety status tree for monitoring the critical safety functions and six shutdown guidelines for responding to the respective challenges to plant safety.

The shutdown safety status tree provides a systematic method of explicitly determining the safety status of the plant. This status tree represents the critical safety functions that are of concern during plant shutdown conditions. Prior to this shutdown condition, the plant can be in any state ranging from heatup and pressurization (that is, from 200°F to no-load temperature) to full power operation. Under any of these conditions (that is, for plant Modes 4 to 1), plant monitoring and response to a reactor trip or requirement for safety injection are covered by the optimal recovery guidelines, status trees, and function restoration guidelines of the at-power ERGs (Reference 3.3-1).

By using the shutdown status tree, plant conditions are monitored during plant shutdown after entering Mode 5 while normal operating procedures are in use for plant shutdown operations. The status tree, SDF-0.1, shutdown safety status tree (Reference 3.3-1), is arranged so that the functions are checked in order of importance. Core cooling during shutdown conditions is addressed first. During plant shutdown conditions, the RNS provides core cooling, which requires adequate RCS inventory to operate properly. RCS inventory checks are made first to show core cooling will not be interrupted because of inadequate RCS inventory and as an early symptom to a loss of shutdown core cooling. After adequate RCS inventory is checked, RNS operation is checked to verify shutdown core cooling is being provided by the RNS. After RNS operation is verified, containment radiation is checked so that an unexpected uncontrolled release will not occur because containment integrity may be breached during plant shutdown maintenance activities. Core reactivity is then checked by monitoring source range flux doubling as an early symptom of an unintended RCS boron dilution, which should occur at a slow enough rate to allow appropriate action to be taken to reestablish shutdown margin. RCS cold overpressure symptoms of RCS pressure and temperature are monitored for maintaining the RCS pressure boundary integrity safety function.

Lastly, RCS temperature change, aside from any normal expected RCS temperature change, is used as an early symptom for potential degradation of the core cooling safety function and the RCS pressure boundary integrity safety function. The shutdown safety status tree is considered to be satisfied when all status tree blocks have been satisfied. If a challenge is identified during the monitoring of the tree, the tree directs plant operators to one of the appropriate six shutdown guidelines for mitigating actions.

The format and arrangement of the shutdown ERG documentation is similar to the at-power ERGs consisting of guidelines and background documents. Implementation of the shutdown ERGs into plant procedures will also be similar to the at-power ERGs with the task allocation between the man and the computer for doing this to be decided when designing features of the man-machine interface system.

The AP600 shutdown ERGs provide closure to *Draft Safety Evaluation Report* (Reference 3.3-2) open item tracking system (OITS) item 2304 with respect to ERGs for shutdown and low-power operations.

3.3.1 References

3.3-1 NSD-NRC-97-4936 (DCP/NRC0702), *Submittal of AP600 Emergency Response Guidelines*, Revision 2, January 10, 1997.

3.3-2 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

3.4 SHUTDOWN SYSTEM/ EVENT MATRIX

This section documents an evaluation of the validity of WCAP-13793 (Reference 3.4-1) for shutdown.

The AP600 system/event matrix describes how the systems protect the reactor core during different events, including events that could occur during shutdown. For each event, different safety- and nonsafety-related systems that are listed can protect the core. Systems that provide RCS makeup, core decay heat removal, and containment cooling are identified. WCAP-13793 provides flow charts for a wide variety of events. Each chart contains the appropriate first level of defense, the safety-related means of mitigating the event, and the contingencies for multiple-failure scenarios. These charts for shutdown are included in this evaluation as Figures 3.4-1, 3.4-2, and 3.4-3 for shutdown events.

These figures are for a loss of offsite power that occurs with the RCS intact, a loss of RCS inventory during mid-loop operation, and a loss of offsite power during refueling, respectively. These high-level flow charts provide an overview of the various system levels of defense for events that occur from shutdown operations.

3.4.1 References

3.4-1 WCAP-13793, *AP600 System/Event Matrix,* June 1994.

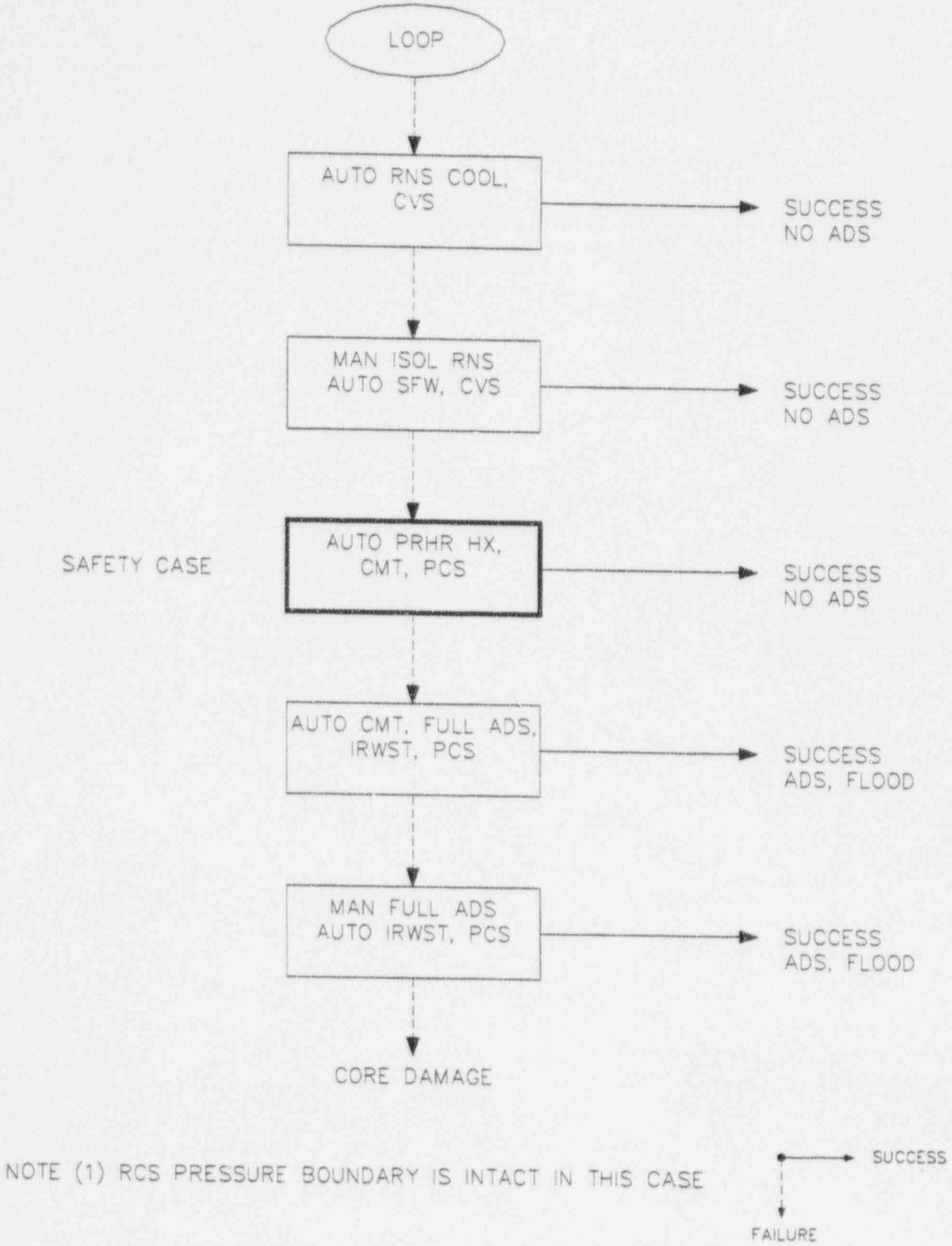
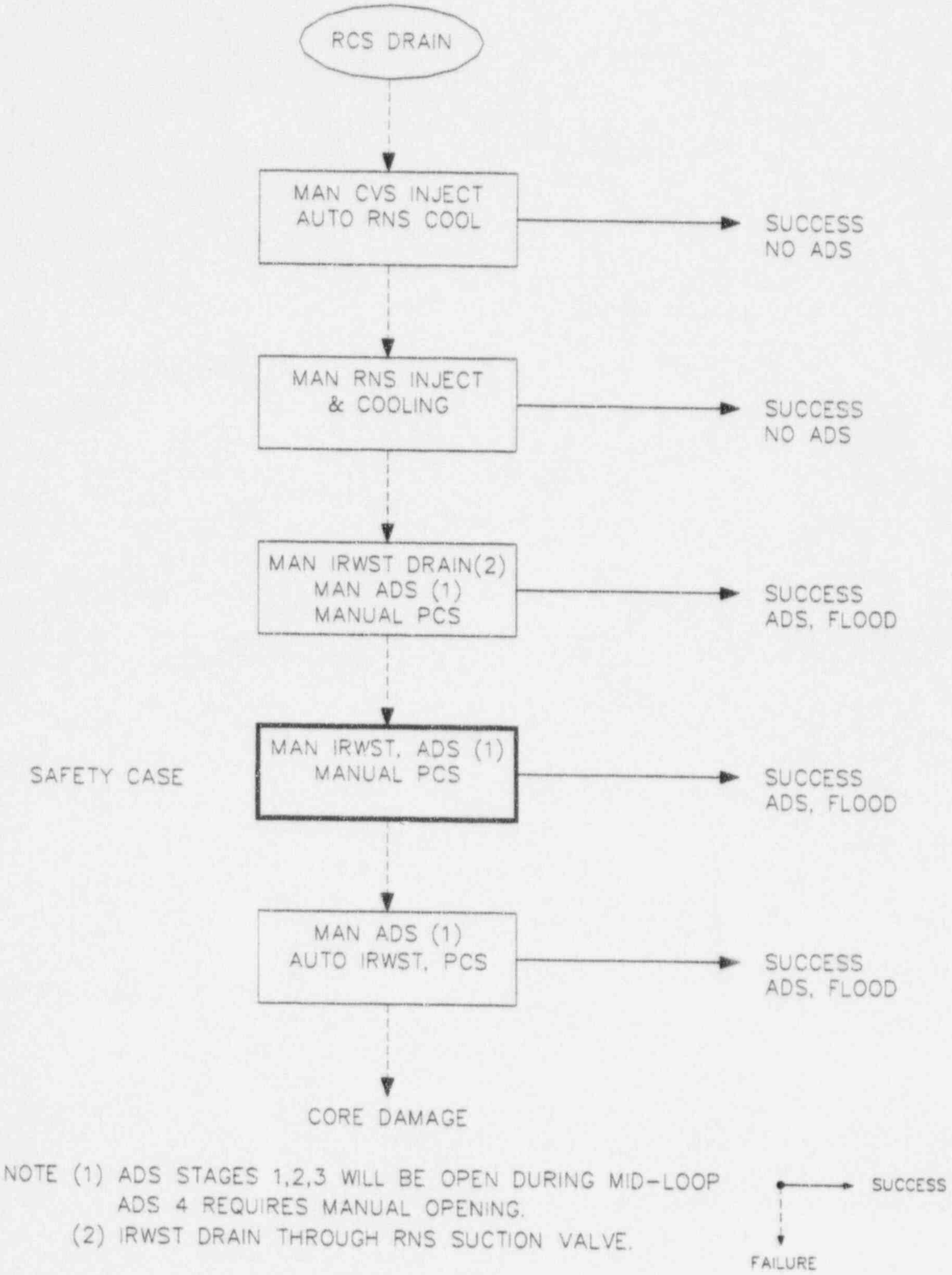
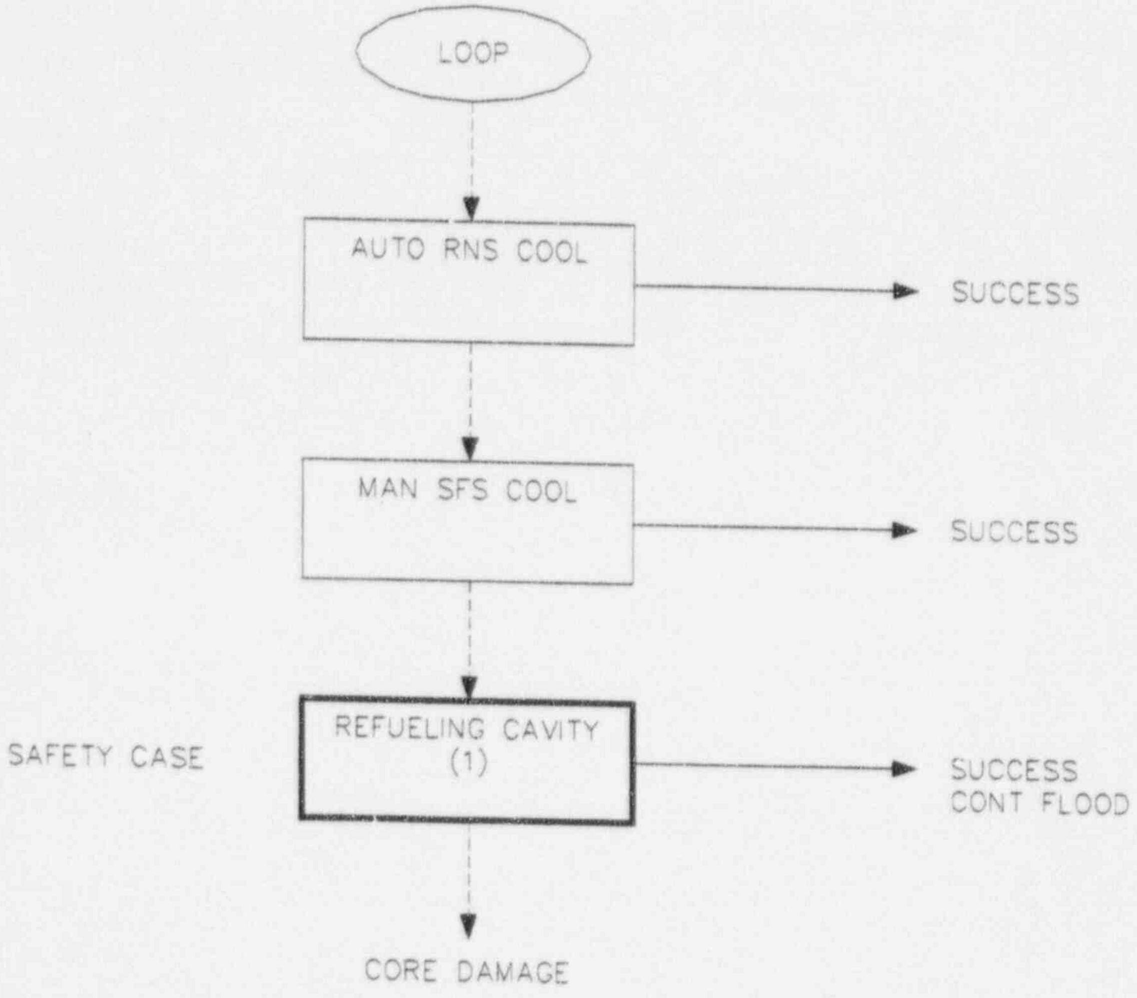


Figure 3.4-1 Loss of Offsite Power – RCS Intact



NOTE (1) ADS STAGES 1,2,3 WILL BE OPEN DURING MID-LOOP
ADS 4 REQUIRES MANUAL OPENING.
(2) IRWST DRAIN THROUGH RNS SUCTION VALVE.

Figure 3.4-2 Loss of RCS Inventory During Mid-loop Operation



NOTE (1) REFUELING CAVITY PROVIDE SEVERAL DAYS CORE COOLING. CONTAINMENT WILL BE CLOSED BEFORE STEAMING STARTS WHICH PROVIDES INDEFINATE CORE COOLING USING CONTAINMENT RECIRC. CONTAINMENT IS COOLED BY PCS WITH AIR ONLY COOLING.

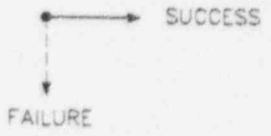


Figure 3.4-3 Loss of Offsite Power During Refueling

4.0 SAFETY ANALYSES AND EVALUATIONS

Section 4 of this *AP600 Shutdown Evaluation Report* (SDER) addresses *Draft Safety Evaluation Report* (Reference 4.0-1) open item tracking system (OITS) item 2294, a review of initiating *AP600 Standard Safety Analysis Report* (SSAR), chapter 15 (Reference 4.0-2), events in lower modes.

4.0.1 References

4.0-1 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

4.0-2 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.1 INTRODUCTION

SDER section 4 reviews each of the design basis accidents (DBAs) and transients presented in the AP600 SSAR, chapter 15 (Reference 4.1-1), with respect to lower power and shutdown modes. In SDER sections 4.2 through 4.9, evaluations or analyses are performed for each case of the transient and LOCA analyses for events occurring at low power and shutdown operations, including the reduced reactor coolant system (RCS) inventory and refueling operations. The evaluations discuss the effects of key plant parameters (for example, plant control parameters, neutronic and thermal hydraulic parameters, and engineering safety features [ESFs]) on plant transient response (such as departure from nucleate boiling ratio [DNBR], peak pressure, and peak cladding temperature). The limiting case for each event category is identified. For those limiting cases bounded by the cases analyzed at power conditions, supporting rationales are provided. These evaluations and analyses resolve OITS item 2294.

For those events where analyses are presented in the shutdown modes, a discussion of the adequacy of the codes used is presented in subsection 4.1.2. The discussion presented in SDER subsection 4.1.2 closes OITS item 1612.

In SDER section 4.10, additional analyses and evaluations demonstrate that the passive systems can bring the plant to a stable, safe condition and maintain this condition. The evaluations and analyses in this section resolve OITS item 2256.

4.1.1 Matrix of SSAR Chapter 15 Events

Table 4.1-1 provides a list of AP600 SSAR chapter 15 events. In response to *Draft Safety Evaluation Report* OITS item 2053, this table categorizes the events as "E" (requiring evaluation), "A" (requiring analysis), or "n/a" (not applicable). The "n/a" events are bounded by at-power analyses or current SSAR analyses.

The events denoted by an "n/a" in Table 4.1-1 are as follows:

- Boron dilution design basis transient explained in SSAR subsection 15.4.6 because it explicitly considers all modes such that no analysis or evaluation is required for this report

- Rod cluster control assembly (RCCA) withdrawal at-power explained in SSAR subsection 15.4.2 because this event occurs only at-power

Table 4.1-1
AP600 SSAR Accidents Requiring Shutdown Evaluation or Analysis

SSAR Section	Titles	Evaluation or Analysis Required
15.1	Increase in Heat Removal from the Primary System	
15.1.1	Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature	E
15.1.2	Feedwater System Malfunctions that Result in an Increase in Feedwater Flow	E
15.1.3	Excessive Increase in Secondary Steam Flow	E
15.1.4	Inadvertent Opening of a Steam Generator Relief or Safety Valve	E
15.1.5	Steam System Piping Failure	
15.1.6	Inadvertent Operation of the Passive Residual Heat Removal Heat Exchanger	E
15.2	Decrease in Heat Removal by the Secondary System	
15.2.1	Steam Pressure Regulator Malfunction or Failure that Results in Decreasing Steam Flow	E
15.2.2	Loss of External Electrical Load	E
15.2.3	Turbine Trip	E
15.2.4	Inadvertent Closure of Main Steam Isolation Valves	E
15.2.5	Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip	E
15.2.6	Loss of ac Power to the Plant Auxiliaries	E
15.2.7	Loss of Normal Feedwater Flow	E
15.2.8	Feedwater System Pipe Break	E
15.3	Decrease in Reactor Coolant System Flow Rate	
15.3.1	Partial Loss of Forced Reactor Coolant Flow	E
15.3.2	Complete Loss of Forced Reactor Coolant Flow	E
15.3.3	Reactor Coolant Pump Shaft Seizure (Locked Rotor)	E
15.3.4	Reactor Coolant Pump Shaft Break	E
15.4	Reactivity and Power Distribution Anomalies	
15.4.1	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition	E
15.4.2	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	n/a
15.4.3	Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)	E
15.4.4	Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature	E

Table 4.1-1 (cont.)
AP600 SSAR Accidents Requiring Shutdown Evaluation or Analysis

SSAR Section	Titles	Evaluation or Analysis Required
15.4.6	Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant	n/a
15.4.7	Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	E
15.4.8	Spectrum of Rod Cluster Control Assembly Ejection Accidents	
15.5	Increase in Reactor Coolant Inventory	
15.5.1	Inadvertent Operation of the Core Makeup Tanks (CMT) During Power Operation	E
15.5.2	Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory	E
15.6	Decrease in Reactor Coolant Inventory	
15.6.1	Inadvertent Opening of a Pressurizer Safety Valve or Inadvertent Operation of the ADS	E
15.6.2	Failure of Small Lines Carrying Primary Coolant Outside Containment	E
15.6.3	Steam Generator Tube Rupture	E
15.6.5	Loss of Coolant Accidents Resulting from a Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary	E/A
15.7	Radioactive Release From a Subsystem or Component	E

4.1.2 Adequacy of Codes Used for Analyses from Shutdown Conditions

Each analysis section in this section 4 discusses the appropriate code used for each analyses. Generally, LOFTRAN-AP is used for transient analyses, which require AP600 design features (core makeup tank [CMT] and passive residual heat removal heat exchangers [PRHR HX], etc.); LOFTRAN for transient analysis, which is independent of the special AP600 design features; LOFTTR2-AP for steam generator tube ruptures; NOTRUMP for small-break LOCAs; and WCOBRA/TRAC for large-break LOCAs.

The adequacy of LOFTRAN-AP, LOFTTR2-AP, NOTRUMP, and WCOBRA/TRAC to accurately represent shutdown conditions in the AP600 is discussed in this subsection to resolve *Draft Safety Evaluation Report* OITS item 1612.

The LOFTRAN-AP and LOFTR2-AP codes are not needed for AP600 safety analyses initiated in lower modes. Therefore, their adequacy is not discussed in this report. The LOCA codes (NOTRUMP and WCOBRA/TRAC) are used to analyze AP600 events at shutdown.

Shutdown events involve lower core power levels than full-power SSAR LOCA analyses. In that sense, the demands on a thermal-hydraulic computer code used to analyze the shutdown events are less than at full power. Codes that have been qualified for use in full-power AP600 events should capably evaluate the more benign transient conditions at shutdown. Moreover, as discussed below, specific qualification exists for application of the Westinghouse LOCA codes to AP600 shutdown cases.

The applicability of WCOBRA/TRAC to pressurized water reactor (PWR) large-break LOCA events has been established through an extensive set of test simulations (WCAP-12945, volumes 1-5) (Reference 4.1-2). The applicability of the models in WCOBRA/TRAC to AP600 large-break LOCA analysis has been documented in WCAP-14171, revision 1 (Reference 4.1-3). Through an extensive review of the pertinent phenomena, WCAP-14171, revision 1, shows that WCOBRA/TRAC can accurately represent a large-break LOCA for the AP600; it also provides specific validation of the downcomer injection location.

The Phenomena Identification Ranking Table (PIRT)-based (Reference 4.1-4) AP600 large break LOCA phenomena, for which the code has been shown applicable in WCAP-14171 at full power, to a large extent remain applicable at shutdown conditions. Items ranked high in importance remain so for a postulated large-break LOCA occurring at shutdown, and none of the phenomena that are not ranked high become highly important, with one exception: the reliance on a different passive safety system, the CMTs, to mitigate the event when the accumulators are isolated. As at full power, condensation of steam in the PRHR HX has a small effect on the AP600 large-break LOCA analysis and does not require specific validation. WCAP-14171 identifies the means by which the uncertainty associated with important parameters in the PIRT is quantified under the best-estimate LOCA methodology used for the full-power emergency core cooling system (ECCS) analysis. Instead of dealing with uncertainty methodology, a conservative prediction of the shutdown large-break LOCA ECCS performance is obtained by using the 10 CFR 50, Appendix K (Reference 4.1-5), decay heat function.

The CMT test facility is a scaled representation of the AP600 CMT design. The 300-series CMT tests are separate effects tests which specifically examine the steam/water condensation and mixing that would be expected following a postulated large-break LOCA. In MT01-GSR-003 (Reference 4.1-6), the phenomena pertinent to CMT injection under conditions of minimal cold leg recirculation are discussed in detail. Also, the WCOBRA/TRAC code is validated for analysis large-break LOCA CMT behavior by simulations of several of the 300 series tests facility experiments that address the pertinent phenomena.

A significant change at shutdown conditions is the low-power level in effect. WCOBRA/TRAC has been used to analyze the long-term cooling portion of the Oregon State University (OSU) facility integral tests (WCAP-14776) (Reference 4.1-7). This effort validates that at core decay power levels comparable to those which prevail during shutdown, WCOBRA/TRAC is qualified to analyze AP600 phenomena. The same version of WCOBRA/TRAC is used in both short-term large-break LOCA and long-term cooling analyses of the AP600. In summary, the WCOBRA/TRAC computer code has been shown not only to apply to large-break LOCA events for the AP600 but also to predict the phenomena associated with CMT draining during a large-break LOCA.

The NOTRUMP computer code has been shown (WCAP-14807) (Reference 4.1-8) to effectively model small-break LOCA phenomena of importance to the AP600. The phenomena ranked HIGH in importance in the WCAP-14807 PIRT are also highly important for a small-break LOCA occurring after the accumulators are isolated during Mode 3 in the AP600, except for the accumulator phenomena. In its validation against the OSU test data, NOTRUMP modeled AP600-specific tests which were initiated at power levels comparable to shutdown power values. All tests at the OSU facility were not initiated from a simulated full-power condition but instead from a simulated decay power level. Furthermore, the typical initial fluid pressure and temperature of 380 psia and 420°F in the OSU facility tests are similar to the AP600 RCS values during Mode 3 shutdown operations, the shutdown mode in which decay heat is at its highest.

Gravity drain phenomena predominate during small-break LOCA events. For analyzing such events in the lower shutdown modes, the NOTRUMP code validation performed against both single-effects tests, including the CMT test facility, and OSU remain applicable. At these lower modes, phenomena ranked high in the WCAP-14807 PIRT remain high in importance, until the reactor pressure becomes so low that critical flow modeling is no longer relevant. Further, there are no phenomena of high importance during small-break LOCA shutdown events that are not covered by the tests at OSU. Therefore, the NOTRUMP prediction of small-break LOCA events initiated from shutdown conditions in the AP600 has been validated by NOTRUMP simulations of single-effects tests and the OSU tests.

4.1.3 References

4.1-1 *AP600 Standard Safety Analysis Report,* Chapter 15, "Accident Analysis."

4.1-2 WCAP-12945, Volumes 1-5, *Code Qualification Document for Best Estimate LOCA Analysis,* 1992/1993.

4.1-3 Hochreiter, L. E., Kemper, R. M., Bajorek, S. M., and Zhang, J., WCAP-14171, Revision 1, *WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident,* October 1996.

4.1-4 Hochreiter, L. E., Loftus, M. J., Brown, W. L., WCAP 14727, *AP600 Scaling and PIRT Closure Report,* August 1996.

4.1-5 Title 10, Code of Federal Regulations, Part 50, Appendix K, "ECCS Evaluation Models," January 1, 1996.

4.1-6 MT01-GSR-003, "WCOBRA/TRAC Core Makeup Tank Preliminary Validation Report," February 1995.

4.1-7 WCAP-14776, *WCOBRA TRAC Long-term Cooling Final Validation Report,* November 1996.

4.1-8 WCAP-14807, Revision 1, *NOTRUMP Final Validation Report for AP600,* January 1997.

4.2 INCREASE IN HEAT REMOVAL FROM THE PRIMARY SYSTEM

4.2.1 Feedwater System Malfunctions Which Increase Heat Removal from the Primary System

Faults that decrease feedwater temperature or increase feedwater flow can be postulated in the feedwater system. These faults could increase heat removal from the primary system, which reduces RCS temperature. The reduction in RCS temperature could lead to an increase in core power generation (due to a negative moderator temperature coefficient) and result in a reduction in margin-to-core design limits. Unchecked, excessive feedwater flow could also result in overfilling the steam generators.

Discussions and analyses, initiated from Modes 1 and 2, of RCS cooldowns caused by feedwater system malfunctions are presented in the AP600 SSAR, subsections 15.1.1 and 15.1.2 (Reference 4.2-1). Subsection 15.1.1 covers reductions in feedwater temperature, and subsection 15.1.2 covers increases in feedwater flow. Modes 1 and 2 are the limiting initial conditions for feedwater system induced RCS cooldown transients.

Protection against feedwater system induced cooldown transients is provided by the protection and safety monitoring system (PMS) through automatic functions that trip the reactor and isolate the feedwater system. The protection functions are available in all modes during which the feedwater system is in operation. Reactor trip includes overpower Δt, high power-range nuclear flux, high intermediate-range nuclear flux, or high source-range nuclear flux. The PMS closes the main control valves on low-1 RCS average temperature signal. The PMS also closes the main feedwater isolation valves and trips the booster/main feedwater pumps when RCS average temperature decreases below the low-2 RCS T_{avg} setpoint. These protection functions are arranged to detect symmetrical plant transients with a channel out of service and a single channel failure.

Additional PMS functions are provided to detect and protect against asymmetrical feedwater system malfunctions. Automatic reactor trip, closure of the main feedwater control and isolation valves, closure of the startup feedwater control and isolation valves, tripping of the booster/main feedwater pumps, and tripping of the startup feedwater pumps occur if the level in a single steam generator is above the high-2 water level setpoint. Similar actions occur if cold leg temperature in a single RCS loop decreases below the low T_{cold} setpoint. The high-2 steam generator level setpoint is active in Modes 1 through 4 unless the various feedwater valves are closed. This ensures that the steam generators cannot inadvertently be overfilled. The low T_{cold} signal is available in Modes 1 through 3. In Mode 3 prior to blocking the low T_{cold} signal, the RCS must be borated to cold shutdown conditions. With the RCS borated, no feedwater malfunction can be postulated to cool the RCS such that a core power excursion would occur.

The feedwater malfunction associated with a drop in feedwater temperature is less severe as power level is decreased. Normal operating feedwater temperature decreases as plant power level decreases. Therefore, if a fault suddenly reduces the feedwater temperature, the maximum change in feedwater temperature will occur if the plant is operating at full power. Also feedwater flow is reduced as load is reduced, and the reduction in feedwater temperature will have less effect at lower power levels or in Modes 2 and below.

As discussed in section 2.2 of this report, in Modes 2 and below, feedwater entering the steam generators is routed through the startup feedwater control valves. The maximum achievable flow rate through the startup feedwater path is much less than when flow is being controlled by the main feedwater control valves. Therefore, failure of a main feedwater control valve in Mode 2 and below is not likely. The assumption of a failed open startup feedwater control valve, in Mode 2 and below, will result in a relatively slow transient due to low feedwater flow rate.

The most severe RCS cooldowns caused by feed system malfunctions will occur in Modes 1 or 2. In Modes 3 or 4, RCS cooldowns due to feedwater malfunctions would be precluded, inconsequential, or less severe than in Modes 1 or 2. The analyses presented in the AP600 SSAR bound the consequences of this class of events initiated in the shutdown modes.

4.2.2 Excessive Increase in Secondary Steam Flow

An excessive increase in secondary steam flow (excessive load increase) is caused by a rapid increase in steam flow that results in a power mismatch between the reactor core power and the steam generator load demand. The plant control system (PLS) is designed to accommodate a 10-percent step load increase in steam flow in the range of 25 to 100 percent of full power. Analyses results for a 10-percent step increase in steam flow are presented in SSAR subsection 15.1.3. The analyses are performed for Mode 1 from full-power initial conditions. Depending upon the plant and PMS characteristics (setpoint uncertainties), a reactor trip signal may or may not be generated for an excessive load increase from full power.

An excessive load increase in Mode 1 is considered limiting because an excessive load increase at full power will put the plant at the highest achievable power level. Load increases at less than full power, or during startup (Mode 2), will not reach as high a power level. The excessive load increase, in Mode 2, will not be as severe as the Mode 1 excessive load increase.

In Mode 3, the excessive load increase may be considered to be a simple steam release because there can be no load, per se, when the turbine is off-line and the core is subcritical. The Mode 3 load increase will be less limiting than the Mode 1 or Mode 2 case because the core is already subcritical. Automatic safeguards actuation signals may not be available if blocked by the operator (blocking is necessary to depressurize and cool down the RCS). However, the RCS must be borated to meet shutdown margin requirements at cold shutdown (200°F) prior to blocking automatic safeguards actuation signals to prevent a return to criticality in the event of a cooldown.

The Mode 4 situation is bounded by Mode 3 because pressure and temperature conditions in the primary and secondary systems are reduced. At some point in Mode 4, the RNS will be placed in service, disconnecting the steam generators from the heat removal path. In Modes 5 and 6, the RNS should be in operation. Any steam release, if possible, will have little or no effect upon the core.

4.2.3 Credible and Hypothetical Steamline Breaks

The spurious opening of a steam generator safety or relief valve is a Condition II event and referred to as a credible steam line break. This event affects the core like a load increase but the analysis assumptions that are applied are different. The credible steam line break is usually assumed to be an unisolatable, uncontrolled steam release, which causes a non-uniform core cooldown (typical of an open safety valve) during the period immediately following a reactor trip which inserts all but the most reactive rod cluster control assembly (RCCA). The resulting reactivity excursion may be large enough to overcome the shutdown margin and return the core to critical, especially when there is little or no decay heat (with power peaking in the region of the stuck RCCA). The credible steam line break is analyzed in Mode 2, and the results are presented in SSAR subsection 15.1.4. The assumptions used in the analysis lead to a more severe, post-trip transient than will result from a load increase initiated in Mode 1.

In Mode 1, prior to reactor trip, the transient characteristics of an inadvertent opening of a steam generator safety or relief valve are similar to the excessive load increase. A reactor trip signal, if needed, may result from overpower ΔT logic. After the reactor trip, the concern becomes a possible return to criticality with the most reactive RCCA stuck in the fully withdrawn position, leading to high local power levels. However, a post-trip return to criticality is less likely when this event occurs in Mode 1 than in Mode 2 because there will be more decay heat present, which tends to retard the cooldown.

In Mode 3, results are expected to be better than the Mode 2 case because pressure, temperature, and flow conditions will be less limiting. An occurrence in Mode 4 will be less severe than in Modes 2 or 3 due to the lower initial RCS temperature, and an effective decoupling of the secondary system from the primary system as the reactor coolant pumps (RCPs) are removed from service and the RNS is started. Automatic safeguards actuation signals are available through Mode 3, until the RCS is borated and the automatic safeguards signals are blocked (see excessive load increase discussion). Both CMTs continue to be available for automatic actuation on low-2 pressurizer level or manual actuation through Mode 4 with the RCS not being cooled by the RNS (see Technical Specification LCO 3.5.2) (Reference 4.2-2). In Mode 4 with the RNS in operation and in Mode 5 with the RCS pressure boundary intact, one CMT is available for activation if needed.

Any cooldown in Modes 5 and 6 caused by depressurization of the secondary system is meaningless because the RCS is already cold, and the RNS system effectively decouples the steam generators from the core.

The steam line rupture is a Condition IV event, producing a greater uncontrolled steam release than the spurious opening of a steam generator safety valve (described above), but the relative effects in the various modes and requirements for protection equipment are the same. This is the most severe cooldown event.

4.2.4 Inadvertent PRHR HX Operation

Inadvertent actuation of the PRHR HX causes an injection of relatively cold water into the RCS. This produces a reactivity insertion in the presence of a negative moderator temperature coefficient. Because the PRHR HX is connected to only one RCS loop, the cooldown resulting from its actuation is asymmetric with respect to the core. Inadvertent actuation of the PRHR HX could lead to an asymmetric power increase and a reduction in margin-to-core design limits.

A limiting analyses of an inadvertent actuation of the PRHR HX heat exchanger is presented in section 15.1.6 of the AP600 SSAR. The analysis in the SSAR is initiated in Mode 1 from hot full-power conditions. This is the most limiting case.

The PRHR HX heat transfer rate is a function of the inlet temperature to the heat exchanger and the flow rate through the heat exchanger. PRHR HX heat transfer rate is higher with high flow rates and high inlet temperatures. Therefore, the maximum heat removal rate will occur when the plant is at full-power condition with forced RCS flow and a high hot leg temperature. At plant full-power conditions, the PRHR HX heat removal rate is approximately 10 percent of full power. At hot zero power (HZP) conditions with natural circulation, heat removal by the PRHR HX is approximately 1.5 percent to 2 percent of full power.

The heat sink for the PRHR HX is the in-containment refueling water storage tank (IRWST), in which the heat exchanger is submerged. Prior to actuation of the PRHR HX, the fluid within the heat exchanger is in thermal equilibrium with the fluid in the IRWST. Thus, the PRHR HX is initially filled with relatively cold fluid which is at containment ambient temperature. When the PRHR HX is actuated, the initial fluid outsurge is fluid at containment ambient temperature. Once the original fluid in the PRHR HX is purged, the out-flow temperature trend of the heat exchanger is set by the temperature entering the heat exchanger from the RCS hot leg minus the temperature drop through the heat exchanger. Thus, the outlet fluid temperature is limited by the cooling capacity of the PRHR HX.

If the reactor is at power (Mode 1 or 2) when the PRHR HX is inadvertently actuated, a cooldown induced increase in core power will occur. The transient response will have two parts. As the cold fluid from the PRHR HX, which is initially at the ambient IRWST temperature, enters the RCS, a large core power increase will occur. The magnitude of the power increase is proportional to the volume of the cold fluid in the PRHR HX. Once the original fluid is purged from the PRHR HX, the fluid temperature exiting the PRHR HX increases to a value limited by the cooling capacity of the PRHR HX. Core power will then decrease to a value higher than the initial core power, but in equilibrium with the heat removal capability of the steam generators plus the PRHR HX.

With the assumptions of a protection system channel out of service as allowed by the Technical Specifications, a failure of an additional protection system channel, and maximum instrument uncertainties, the asymmetric core power transient may not result in actuating any overpower reactor trips, such as high nuclear flux or overpower Δt. In this case, the core power transient is controlled only by the initial volume of cold water in the PRHR HX and the heat removal capability of the heat exchanger.

Higher initial core power will result in the largest achievable core power and in more severe consequences. Therefore, if the reactor is at-power, the full-power case produces the worst results.

In Mode 3, because the reactor is subcritical, inadvertent actuation of the PRHR HX produces a less severe power excursion than if the reactor is at power or at HZP with the reactor just critical. If in Mode 3 below no-load temperature, the cooldown caused by the actuation of the PRHR HX results in the cold leg temperature dropping below the low T_{cold} safeguards signal setpoint. This function actuates a reactor trip, initiates boration by the CMTs, and most importantly, trips all the RCPs. When the RCPs trip, natural circulation flow begins in the RCS and the PRHR HX loop. When natural circulation flow is initiated, the heat removal capability of the PRHR HX decreases to approximately 1.5 percent of full power and the severity of the transient is minimized. With the RCS in natural circulation, the cooldown rate of the RCS is also slowed. If criticality is obtained, boration by the CMTs will bring the core subcritical again.

The low T_{cold} safeguards signal may be blocked by the operator in Mode 3 to allow plant depressurization and cooldown to lower modes. However, prior to blocking the low T_{cold} safeguards signal, the RCS is borated to the shutdown margin requirements at cold shutdown (200°F). Therefore, in Mode 3 with safeguards signals blocked or in Mode 4, cooldown of the RCS by inadvertent actuation of the PRHR HX will not result in a reactivity excursion, which produces a power increase.

In Modes 5 and 6, the RCS will be borated such that a cooldown-induced power excursion could not be postulated. The RCS will be at 200°F or less, and with initial RCS temperatures this low, no significant cooling of the RCS by inadvertent actuation of the PRHR HX could be postulated.

4.2.5 References

4.2-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.2-2 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

4.3 DECREASE IN HEAT REMOVAL BY THE SECONDARY SYSTEM

4.3.1 Loss of Load and Turbine Trip

Discussions and analyses of the consequences of loss of load, turbine trip, inadvertent closure of main steam isolation valves (MSIVs), or loss of condenser vacuum are presented in SSAR subsections 15.2.2 through 15.2.5 (Reference 4.3-1). These events are characterized by a rapid reduction in steam flow from the steam generators. This results in an increase in steam pressure and a heatup of the primary side if the reactor power is not reduced. The effects of the primary to secondary power mismatch during these events are mitigated by tripping the reactor and opening secondary and primary side safety valves. The severity of these events is increased if the primary to secondary power mismatch is increased. Therefore, the most severe results occur if the plant is initially operating in Mode 1 at maximum-rated plant power conditions rather than lower power conditions. The turbine is off-line below Mode 1 and transients related to turbine-related faults cannot occur.

In Modes 2, 3, or 4, the plant may be removing decay heat by dumping steam to the condenser. In Mode 4 when the RCS is below 350°F, decay heat is removed using the RNS. In Modes 2, 3, or 4, the transient response to a loss of condenser vacuum or inadvertent MSIV closure is bounded by the turbine trip analysis from full power because the power mismatch is low. Decay heat removal can still be accomplished by the steam generators through atmospheric steam relief through power-operated relief valves (PORVs) if available or through steam generator safety valves, which are available through Mode 4 (see Technical Specification LCO 3.7.1 [Reference 4.3-2]). Additionally, decay heat can be removed with the PRHR HX, which is available through Mode 5 with the RCS intact (see Technical Specifications LCO 3.5.4 and 3.5.5).

4.3.2 Loss of ac Power

A discussion and an analysis of a loss of ac power event is provided in SSAR subsection 15.2.6. The loss of ac power results in the loss of forced primary coolant flow and the loss of main feedwater flow. This results in a heatup and pressurization of the RCS. If the reactor is at power, the event is mitigated by tripping the reactor. The reactor may be automatically tripped on low RCP speed, low RCS flow, low steam generator level, or several other primary side heatup signals. Also reactor trip may occur due to the loss of power to the control rod drive mechanisms.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for loss of ac power would be if the plant were at full rated power. This will result in the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. In Modes 4 or 5 with the RNS in operation, the plant response to a loss of ac power is the same at the loss of RNS cooling as discussed in subsection 4.8.5 of this report.

4.3.3 Loss of Normal Feedwater

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used, and therefore, loss of feedwater events are irrelevant.

A discussion and an analysis of a loss of normal feedwater event from rated full-power conditions are provided in SSAR subsection 15.2.7. The loss of normal feedwater flow results in a heatup and pressurization of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a loss of normal feedwater is with the plant initially at full rated power. This case will have the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. The SSAR analysis initiated from full power bounds cases initiated from the shutdown modes.

4.3.4 Feedwater System Pipe Break

Depending upon the size of the break and plant operating conditions, the break could cause either an RCS heatup or an RCS cooldown. The cooldown aspects are less severe than a steam line break, which is discussed in subsection 4.2.3 of this report and is not considered in the following discussion.

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used, and therefore, a loss of feedwater caused by a feedwater system pipe break will not cause a heatup of the RCS.

A discussion and an analysis of feedwater system pipe break from rated full-power conditions are provided in SSAR subsection 15.2.8. A rupture of a feedwater system pipe results in a loss of feedwater flow causing a heatup and pressurization of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a feedline break occurs with the plant at full rated power. This case will have the highest decay heat levels and the highest stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized.

4.3.5 References

4.3-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.3-2 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

4.4 DECREASE IN REACTOR COOLANT FLOW RATE

4.4.1 Partial and Complete Loss of Forced RCS Flow

A partial loss of forced RCS flow may be caused by a mechanical or an electrical failure in an RCP or from a fault in the power supply to the pumps. An RCP failure will result in only the loss of a single RCP. A fault in the power supplies for the RCPs could result only in the loss of one, two, or all four RCPs. There is no credible failure that could result in the loss of three RCPs.

The loss of one or more RCPs reduces the heat removal rate from the primary to the secondary coolant system and thereby causes a heatup in the RCS. The heatup of the RCS results in an increase in RCS pressure and a decrease in margin-to-core design limits (that is, departure from nucleate boiling [DNB]). An occurrence at full power will produce a greater and more rapid heatup than at part-power conditions or low-power conditions in Mode 2. Therefore, for evaluating the maximum RCS pressure or the minimum DNB ratio, analyses are performed at full-power conditions. Analyses for partial loss of forced RCS flow transients are presented in subsection 15.3.1 of the AP600 SSAR (Reference 4.4-1). Analyses for a complete loss of flow are presented in SSAR subsection 15.3.2. These analyses bound loss of flow events initiated in other modes.

Protection for loss of forced RCS flow events is provided by tripping the reactor. This reduces reactor power and preserves margin-to-DNB limits. The AP600 PMS includes a reactor trip on low RCS flow in any cold leg and a reactor trip on low RCP speed in any two of four RCPs. These two reactor trips are used to detect all possible partial and complete loss of RCS flow transients. Opening of the pressurizer safety valves in conjunction with the reactor trip prevents overpressurization of the RCS.

Below Mode 2, when the core is subcritical, forced RCS flow is not needed because margin-to-DNB is not an issue. It is common to have one or more RCPs out of service below Mode 2 because full RCS flow is no longer needed. In Modes 3 through 5, LCO 3.4.5 of the Technical Specifications (Reference 4.4-2) requires that only three RCPs need to be operating if the reactor trip breakers are closed, to ensure that DNB limits are not exceeded, in the event RCCAs are inadvertently withdrawn. If the trip breakers are open and RCCA withdrawal is precluded, no RCPs are required to be operating in Modes 3 through 5.

Following reactor trip in loss of forced RCS flow events, decay heat removal is required. The PRHR HX or the steam generators can be used for decay heat removal. In the event of a complete loss of forced RCS flow, RCS natural circulation is adequate to remove core decay heat. This is demonstrated by the loss of ac power analysis presented in SSAR subsection 15.2.6.

4.4.2 Reactor Coolant Pump Shaft Seizure or Break

An RCP shaft seizure or break results in a partial loss of forced RCS flow. The results are similar to partial loss of flow events discussed in subsection 4.4.2 of this report except that the rate of flow reduction is much more rapid if an RCP shaft breaks or seizes. Like the partial loss of flow, a locked or broken RCP shaft reduces the heat removal rate from the primary to secondary coolant system and thereby causes a heatup of the RCS. An occurrence at full power produces the most severe heatup transient. The discussion for the partial loss of flow with respect to limiting modes and protection is applicable to the RCP shaft seizures or breaks.

Analyses and evaluation of RCP shaft seizures and breaks for Mode 1, from full-power conditions, are provided in SSAR subsections 15.3.3 and 15.3.4. The analyses bound events initiated from the shutdown modes.

4.4.3 References

4.4-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.4-2 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

4.5 REACTIVITY AND POWER DISTRIBUTION ANOMALIES

4.5.1 Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition

An uncontrolled RCCA bank withdrawal from a subcritical condition could cause a reactivity excursion, which if not terminated by a reactor trip, could result in DNB. SSAR subsection 15.4.2 (Reference 4.5-1) presents an analysis for the uncontrolled RCCA bank withdrawal from a subcritical condition in Mode 2. Assumptions are used that make the analysis bound an occurrence in Modes 2, 3, 4, or 5. Specific conservative assumptions are made for the number of RCPs operating, the reactor trip functions credited, initial RCS temperature, and the magnitude of the reactivity excursion.

A single failure in the rod control system could cause the withdrawal of only one bank, and its withdrawal rate would be expected to be slower than the maximum rod speed possible when in automatic rod control. The analysis assumes the simultaneous withdrawal of the combination of two sequential RCCA banks having the greatest combined worth at the maximum possible speed.

LCO 3.3.1 of the AP600 Technical Specifications (Reference 4.5-2) gives the operational requirements for reactor trips. The source-range high neutron flux trip must be in operation in Modes 3, 4, and 5 if the reactor trip breakers are closed. If the reactor trip breakers are open, then an RCCA withdrawal is precluded from occurring. The source-range high neutron flux trip is available in Mode 2 if power is below the P-6 interlock. In these instances, the source-range high neutron flux trip would be available to terminate the event, by tripping any withdrawn and withdrawing rods, before any significant power level could be attained. Therefore, DNB would be precluded. The intermediate-range high neutron flux reactor trip is also available in Mode 2. The AP600 SSAR analysis assumes that reactor trip does not occur until the power-range (low setting) high neutron flux setpoint is reached. No credit is assumed in the analysis for the source-range high neutron flux reactor trip or the intermediate-range high neutron flux reactor trip.

LCOs 3.4.4 and 3.4.5 of the AP600 Technical Specifications give the operation requirements for RCPs. LCO 3.4.4 specifies that in Modes 1 and 2, all four RCPs must be operating. LCO 3.4.5 specifies that in Modes 3, 4, and 5, at least three RCPs must be operating whenever the reactor trip breakers are closed. For minimizing the DNB margin, the AP600 analysis assumed only three RCPs are operating to bound operation in Modes 2, 3, 4, or 5.

The RCS temperature is assumed to be at the HZP value in the analysis. This is more limiting than that of a lower initial system temperature for DNB and core kinetics feedback calculations.

These conservative assumptions result in the core returning to critical and generating power before reactor trip occurs. The analysis presented in the SSAR bounds the inadvertent RCCA bank withdrawal from a subcritical condition transient in Modes 2 through 5.

4.5.2 Uncontrolled RCCA Bank Withdrawal at Power

This transient is defined only in Mode 1.

4.5.3 RCCA Misalignment

RCCA misalignment events are analyzed in SSAR subsection 15.4.3. RCCA misalignment events include the following:

- One or more dropped RCCAs
- Statically misaligned RCCA
- Withdrawal of a single RCCA

This group of events may result in core radial power distribution perturbations, which may cause allowable design power peaking factors and DNB design limits to be exceeded. Therefore, these events are a concern only in the at-power modes, and the severity will be increased at high power. If the reactor is subcritical, DNB will not be a concern.

Following the dropping of one or more RCCAs while at-power, core power will immediately be reduced. The reduced core power and the continued steam demand to the turbine causes a reactor coolant temperature decrease. If the reactor is in manual control, the core power rises due to moderator feedback to the initial power level at a reduced core inlet temperature. If the reactor is in automatic control, the control system detects the drop in power and initiates withdrawal of a control bank. Power overshoot above the initial power level may occur as the control system withdraws a bank. Following dropping of one or more RCCAs, the most severe results occur when the control system overshoots the initial power level in conjunction with a perturbation in the radial power distribution. This is the most limiting case for this event, and the results are presented in the SSAR. If the reactor is in any of the subcritical modes, dropping RCCAs will not result in any power transient.

As in the case of dropped RCCAs, statically misaligned RCCAs have no effect in the absence of a critical neutron flux and are not a concern below Mode 2. The most limiting case, and analysis, is for Mode 1 which also bounds Mode 2 operation.

The most limiting case for the withdrawal of a single RCCA is an occurrence while in Mode 1. An occurrence in any of the subcritical modes will have no effect. The shutdown margin requirements are specified in LCO 3.1.1 of the AP600 Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, no single RCCA withdrawal initiated from the subcritical modes will insert enough reactivity to attain criticality.

4.5.4 Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature

Starting an idle RCP without bringing the inactive pump cold leg temperature closer to the core inlet temperature results in the injection of cold water into the core, which causes a reactivity insertion and subsequent power increase. The consequences of this event are directly related to the temperature difference between the cold leg temperature in the loop with the inactive RCP and the core inlet. The most severe consequences are included when the plant is operating at maximum permissible power level.

Startup of an inactive RCP while in any of the subcritical modes will have relatively little effect upon core temperature because there will be little or no temperature difference between loops. Safety analyses for the inadvertent starting of an RCP are presented in SSAR subsection 15.4.4. A conservative analysis is performed for Mode 1 operation with the plant initially at 70-percent power. LCO 3.4.4 of the AP600 Technical Specifications requires all RCPs to be operating in Modes 1 and 2. At-power condition is chosen in the analyses to maximize the inlet temperature differences. This analysis bounds operation in Mode 2 and the subcritical modes.

4.5.5 Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant

Boron dilution analyses and evaluations for Modes 1 through 5 are provided in SSAR subsection 15.4.6. In Mode 6, administrative controls isolate the RCS from potential sources of unborated water by locking closed specified valves in the chemical and volume control system (CVS) and thereby precludes an uncontrolled boron dilution transient. Makeup needed during refueling is supplied from the boric acid tank which contains borated water.

4.5.6 Inadvertent Loading of a Fuel Assembly in an Improper Position

Fuel loading errors – such as inadvertent loading of one or more fuel assemblies into improper positions, having a fuel rod with one or more pellets of the wrong enrichment, or having a fuel assembly with pellets of the wrong enrichment – may result in power shapes in excess of design values. SSAR subsection 15.4.7 presents Mode 1 results for this event. The SSAR results bound the results for operation in Mode 2. This event is meaningful only if the reactor is at-power and, therefore, not applicable in the subcritical Modes of 3 through 6.

4.5.7 RCCA Ejection

Analyses for RCCA ejections in Mode 1 and Mode 2 are presented in SSAR subsection 15.4.8. The cases analyzed in the SSAR are the most limiting cases. The shutdown margin requirements are specified in LCO 3.1.1 of the AP600 Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, the ejection of a single RCCA initiated from the subcritical modes would not insert enough reactivity to attain criticality.

4.5.8 References

4.5-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.5-2 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

4.6 INCREASE IN REACTOR COOLANT INVENTORY

An increase in RCS inventory could be caused by inadvertent actuation of the CMTs or by malfunctions in the CVS system. Analyses of events that increase the RCS inventory are provided in SSAR section 15.5 (Reference 4.6-1). SSAR subsection 15.5.1 presents the analysis results for inadvertent actuation of the CMT. SSAR subsection 15.5.2 contains results from the analysis of a CVS malfunction which increases RCS inventory. These events do not present a challenge to core design limits. If unchecked, these events could lead to an overfill of the pressurizer and possible loss of reactor coolant from the system. The increase in pressurizer water volume is slow during these events and is controlled by the injection rate, core decay heat produced, and heat removal rate from the RCS. While the pressurizer safety valves may open, the steam relief from the pressurizer safety valves is low and no serious challenge to the RCS pressure boundary occurs (if the pressurizer does not fill).

The SSAR analyses for these events are performed with the plant initially in Mode 1 at full-power conditions. This results in the maximum amount of stored energy in the plant and in the maximum core decay heat. If the plant was assumed to be at part power, or in the subcritical modes, the amount of stored energy and decay heat will be significantly reduced.

If a spurious "S" signal occurs causing the CMTs to be actuated, the reactor is also tripped and the PRHR HX is also actuated. The CMTs will begin injecting cold, borated fluid into the RCS. The injected fluid expands as it is heated in the RCS by decay heat. The expansion is counteracted by decay heat removal through the PRHR HX. The severity of the expansion is increased with higher decay heat levels.

Malfunctions in the CVS, which add excess inventory to the RCS, are protected against by the inclusion of automatic CVS isolation functions in the PMS. If a safeguards signal has occurred (which also would activate the CMTs), the CVS is automatically isolated if the pressurizer level exceeds the high-1 pressurizer level setpoint. Above the high-1 pressurizer level setpoint, there is a high-2 pressurizer level setpoint, which also isolates the CVS. The high-2 pressurizer level function is not interlocked with the safeguards signal. The high-2 function protects in situations where the reactor is at-power or a safeguards signal has not occurred. The high-2 pressurizer level function is available in Modes 1 through Mode 3 and in Mode 4 when the RNS is not operating. These functions effectively prevent overfilling of the pressurizer when the CVS acts alone or where CVS interacts to also cause the CMTs to be actuated.

Isolation of CVS on high-2 pressurizer level is available in Modes 1 through 4 until the plant is operating on RNS. There are applications where the RCS may be filled water-solid when the RNS is in operation. In Modes 4, 5, and 6 when the RNS is in operation, low-temperature overpressure protection (LTOP) of the RCS pressure boundary is provided by the RNS relief valve. A discussion of this is provided in subsection 4.10.1 of this report.

4.6.1 References

4.6-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.7 DECREASE IN REACTOR COOLANT INVENTORY

4.7.1 Inadvertent Opening of a Pressurizer Safety Valve or Inadvertent Operation of the Automatic Depressurization System

SSAR subsection 15.6.1 (Reference 4.7-1) includes analyses and evaluations of the inadvertent opening of a pressurizer safety valve or the inadvertent operation of the automatic depressurization system (ADS). The analyses discussed here and in SSAR subsection 15.6.1 evaluate the RCS depressurization aspect following these events. Loss of RCS inventory aspects of these events is covered in subsection 4.8.2 of this report.

When analyzed as depressurization events, inadvertent opening of primary side relief valves, if the reactor is at-power, could result in exceeding core design limits, specifically DNB criteria. Violation of DNB criteria is not a realistic concern if the reactor is in any of the subcritical modes. Therefore, these events are analyzed in Mode 1 at the maximum rated power and the analysis performed bounds cases initiated from Mode 2.

4.7.2 Failure of Small Lines Carrying Primary Coolant Outside Containment

This event is reported in SSAR subsection 15.6.2 as the rupture of a primary coolant sample line; the radiological consequences of this event are analyzed during Mode 1 because the coolant temperature and iodine concentrations bound those that would exist in the other modes. Concerning shutdown risk, the consequences of a sample line break during Modes 2, 3, 4, or 5 are no more severe than if the accident occurs during Mode 1 operation.

4.7.3 Steam Generator Tube Rupture in Lower Modes

The steam generator tube rupture (SGTR) analysis presented in the SSAR is the limiting case with respect to offsite doses. The SSAR analysis was performed at full power because this results in the maximum offsite dose. The key inputs from the thermal-hydraulic SGTR analysis performed with the LOFTTR2 computer code to the offsite dose analysis are the amount of flashed primary to secondary break flow and the steam released from the faulted steam generator. Both of these will be significantly reduced at lower power levels and in lower modes of operation.

Margin to overfill analyses are not presented in the SSAR. The SSAR does indicate that an analysis was performed to demonstrate margin to steam generator overfill with no operator actions modeled. This is necessary because the dose analysis does not include consideration of water relief from the ruptured steam generator PORV/MSSV. This margin to steam generator overfill analysis was supported by the assertion that an analysis with operator actions modeled will also demonstrate margin to overfill. The overfill analysis with no operator actions discussed in the SSAR was initiated at full power. WCAP-10698-P-A (Reference 4.7-2) indicates that margin to overfill is reduced when the SGTR is initiated at zero power because of the higher initial steam generator secondary liquid inventory. WCAP-10698-P-A concludes that zero power and lower mode SGTR overfill analyses are not limiting, based primarily on more rapid operator responses expected in those conditions. This is discussed further in the Appendices to WCAP-10698-P-A, which include responses to NRC questions regarding this conclusion. When operator actions are credited for AP600 SGTR mitigation, the plant behaves in a manner comparable to a standard Westinghouse PWR and the conclusions of WCAP-10698-P-A apply.

When operator actions are not relied upon and only the AP600 automatic RCS cooling and depressurization are credited, margin to overfill would still be maintained for SGTR events initiated at lower power levels despite the increased initial steam generator secondary side inventory corresponding to the lower initial power assumption. This is because the automatic protection system actions that prevent overfill are independent of the operator actions. For operating plants, there is a set period of time from the start of the event until the operator can reverse the trend toward filling the steam generator. Therefore, the initial margin to overfill directly impacts the final margin. For the AP600, the primary cooldown and depressurization occur automatically when the PRHR HX is actuated on a low pressurizer pressure "S" signal or low pressurizer level CMT actuation signal. The primary pressure may still be held up by the CVS, until it is isolated on a high steam generator level signal. For the AP600, a higher initial steam generator water level results in the CVS flow being terminated earlier.

In lower modes, the PRHR HX actuation is provided only by the low pressurizer level signal. Although this results in delayed cooling and depressurization, margin to steam generator overfill is still maintained. The increase in mass in the secondary side of the ruptured steam generator is directly related to the reduction in pressurizer water level, because (once the CVS is isolated on high steam generator water level) there is no source of makeup to the RCS. The steam generator secondary side can accommodate the amount of fluid initially contained in the pressurizer and still retain a significant amount of margin to steam generator overfill. The PRHR HX will, therefore, be actuated on low pressurizer water level in sufficient time for the PRHR HX to cool and depressurize the primary and terminate break flow before steam generator overfill will occur.

4.7.4 References

4.7-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.7-2 Lewis, R. N., Huang, P., Behnke, D. H., Fittante, R. L., and Gelman, A., WCAP-10698-P-A, *SGTR Analysis Methodology to Determine the Margin to Steam Generator Overfill*, August 1987.

4.8 LOSS-OF-COOLANT ACCIDENT EVENTS IN SHUTDOWN MODES

The AP600 SSAR presents a spectrum of break sizes of the postulated LOCAs at the full-power operating condition. Other things being equal, the reduction in power to decay heat levels associated with shutdown mode operations will make all LOCA events less limiting than those analyzed at full power and reported in SSAR subsection 15.6.5 (Reference 4.8-1). However, as the plant proceeds through shutdown modes of operation, various PXS equipment are removed from service at identified points in time. One particularly significant action in the course of taking the AP600 to cold shutdown in the elimination of PXS equipment is the isolation of the accumulators at 1000 psig. This procedural action reduces the capability of the PXS to mitigate LOCAs. For assessing the adequacy of the remaining PXS components to mitigate postulated LOCA events, three events are analyzed, assuming they occur immediately after the isolation of the accumulators: a double-ended cold leg guillotine (DECLG) break, a double-ended rupture of the direct vessel injection (DVI) line, and an inadvertent actuation of the ADS by a spurious signal. Only safety-related systems are modeled in the analysis of these events, which occur during Mode 3.

For these analyses, the plant was assumed to be shut down in Mode 3 at steady-state conditions of 1000 psig and 425°F with the accumulators isolated. An initial pressure of 1000 psig is assumed because this is the highest pressure with the accumulators isolated and a hot leg temperature of 425°F is the highest expected temperature when the pressure is 1000 psig. The decay heat level is determined at 2.78 hours after reactor shutdown based on the time estimate to cool down the plant from full-power operation to 425°F at a cooldown rate of 50°F per hour. The low pressurizer pressure safeguards signal is also assumed to be disabled because the initial pressure is below the setpoint.

The matrix presented in this SDER, section 4.1, details the relationship between the SSAR analysis and LOCA-related accidents during the shutdown modes of operation. Other postulated events involving a decrease in reactor coolant inventory during shutdown presume the loss of RNS cooling during Mode 4 and Mode 5. SDER subsection 4.8.5.1 presents loss of RCS cooling with the RCS intact; the analysis with the RCS open is presented in SDER subsection 4.8.5.2. As discussed in SDER subsection 4.8.4, among the LOCA-related events that may be postulated to occur in lower modes, these cases may be considered bounding. It is extremely conservative to presume that a DECLG break could occur under the reduced pressure and temperature conditions associated with Mode 3 plant operation. The DECLG break exhibits the limiting calculated peak cladding temperature (PCT) value among the SSAR cases.

The NOTRUMP computer code (Reference 4.8-2), used in the SSAR analysis, was used in the small-break LOCA cases. The NOTRUMP input was set for the shutdown analyses to comply with AP600 Westinghouse Small-Break LOCA Evaluation Model methodology (WCAP-14601) (Reference 4.8-3) to obtain suitable representation of the AP600.

In the SSAR analysis, the actuation of ADS depressurizes the RCS to accumulator actuation pressure to thereby increase safety injection flow. Therefore, the limiting single active failure for the double-ended direct vessel injection (DEDVI) line break at full power is taken as failure of a set of one first-stage and one third-stage ADS valves to open on demand. For the Mode 3 shutdown LOCA case, reducing the initial venting capability of the RCS to delay accumulator injection does not apply. Thus, for both DEDVI and inadvertent ADS cases, failure of one of the four fourth stage ADS valves to open on demand is postulated.

4.8.1 Double-ended Cold Leg Guillotine

The DECLG break is analyzed using the WCOBRA/TRAC computer code and the AP600-specific noding presented in WCAP-14171, Revision 1 (Reference 4.8-4). Table 4.8-1 summarizes the results.

This case models the double-ended rupture of one of the two cold legs in the RCS loop without the PRHR HX at a pressure of 1000 psig just after the accumulators are isolated. Only the core makeup tanks (CMTs) and IRWST are available to deliver PXS flow. This break evaluates the ability of the plant to withstand a large LOCA during shutdown with its conditions and equipment availability. The limiting discharge coefficient (0.8) is modeled. The analysis is performed with 10 CFR 50, Appendix K (Reference 4.8-5), required decay heat, and Technical Specification/Core Operating Limits Report maximum peaking factors.

The break is assumed to open instantaneously at 0.0 seconds. The subcooled discharge from the broken cold leg (Figure 4.8-1) causes a rapid RCS depressurization (Figure 4.8-2). In Figure 4.8-1, the positive flow direction is the normal operation direction. The reversal of flow entering the vessel to flow out of the break is shown. Due to high-1 containment pressure, an "S" signal is generated at 1.8 seconds, and following a 1.2-second delay, the isolation valves on the CMT and PRHR HX outlet lines begin to open. The signals also trip the RCPs after a 16.2-second delay. The limiting discharge coefficient of 0.8 identified in full-power LOCA analyses is assumed.

Within a few seconds, the collapsed liquid level drops within the upper plenum due to voiding (Figure 4.8-3). The downcomer collapsed liquid level (Figure 4.8-4) quickly falls below the elevation of the cold legs; the elevation of the top of the core is 18.8 feet. Because the RCS fluid enthalpy is lower than the full-power value, the RCS depressurization rate is decreased from the SSAR cases and more of the initial inventory is retained in the reactor vessel.

Table 4.8-1
Double-ended Cold Leg Guillotine Break

Event	Time (seconds)
Break Open	0.0
"S" Signal Receipt	3
RCPs Start to Coast Down	18
CMT Draindown Begins	30
Lower Plenum Refilled	208

CMT injection from both tanks replenishes the RCS mass inventory (Figure 4.8-5). Injection from the CMTs as the RCS pressure declines terminates the peak cladding temperature (PCT) transient because the stable injection of water from the CMTs exceeds the break flow. The core collapsed level refills are as shown in Figure 4.8-6. The pressure is low enough that the IRWST injection will begin once the CMTs drain to the low-2 level actuation setpoint. The maximum PCT value is approximately 1200°F for this bounding break size, and all the 10 CFR 50.46 (Reference 4.8-6) acceptance criteria are met.

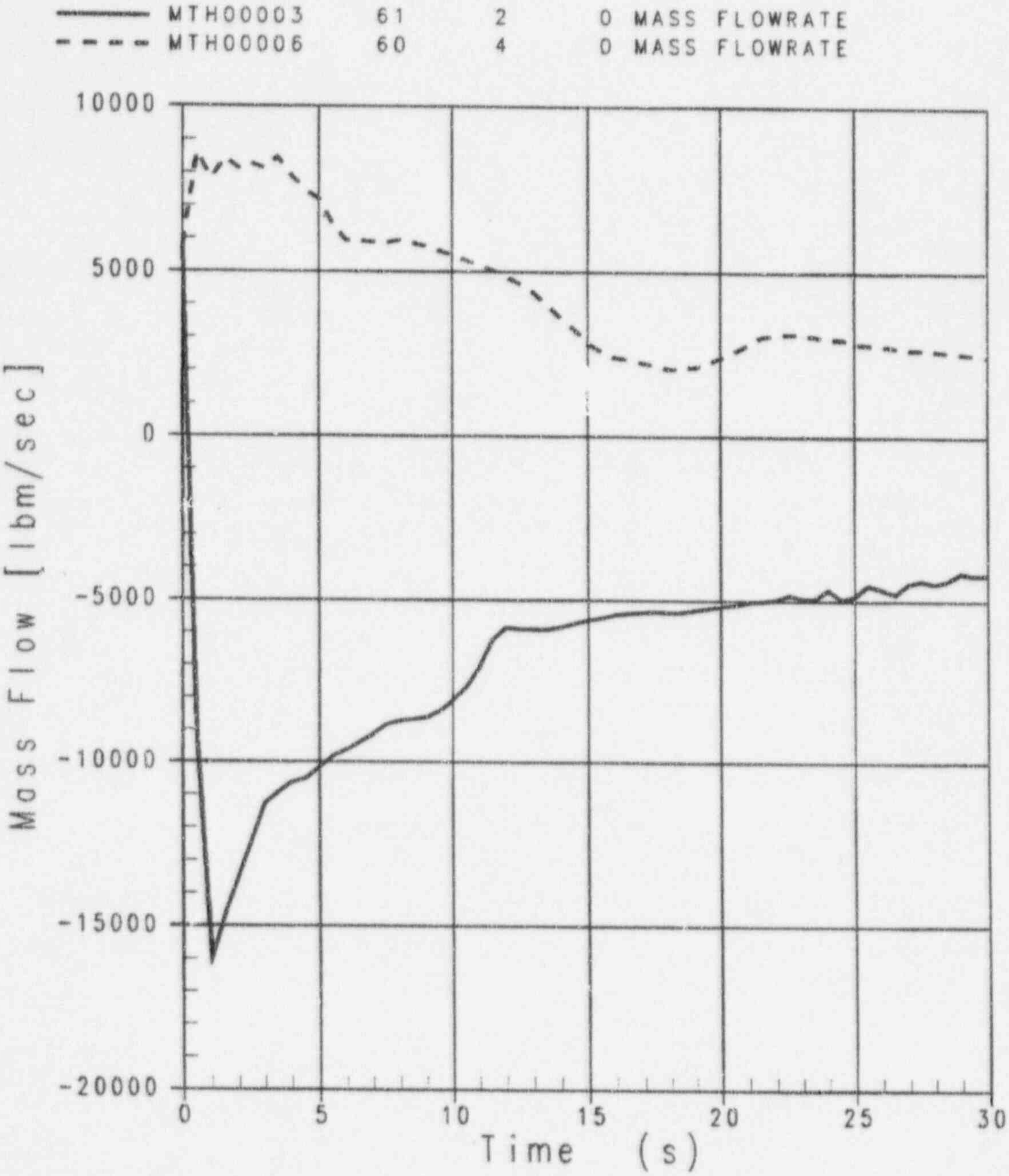


Figure 4.8-1 Mode 3 C_D = 0.8 DECLG Break, Break Flow Rates, Vessel and RCP Sides

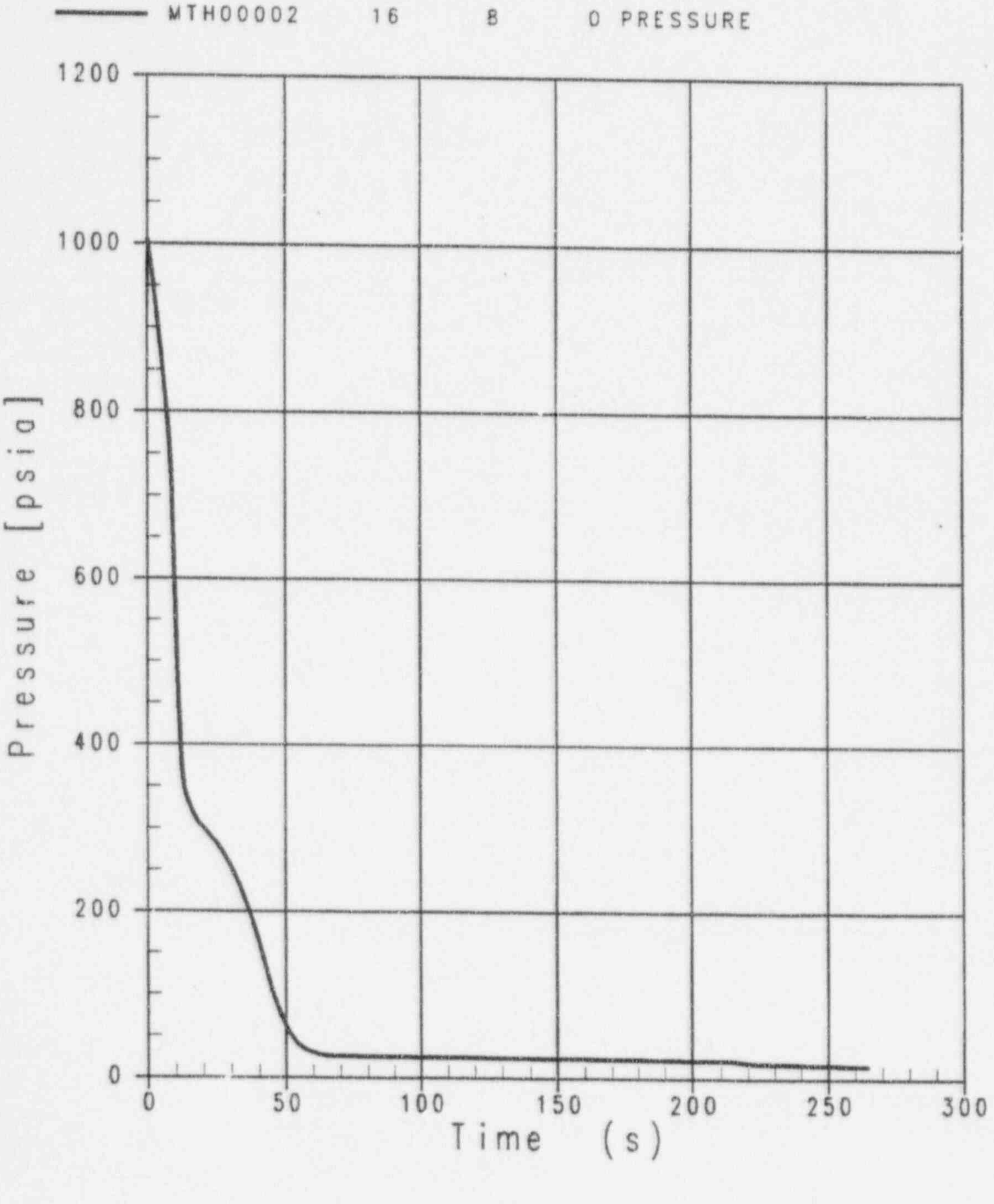


Figure 4.8-2 Mode 3 C_D = 0.8 DECLG Break, Pressurizer Pressure

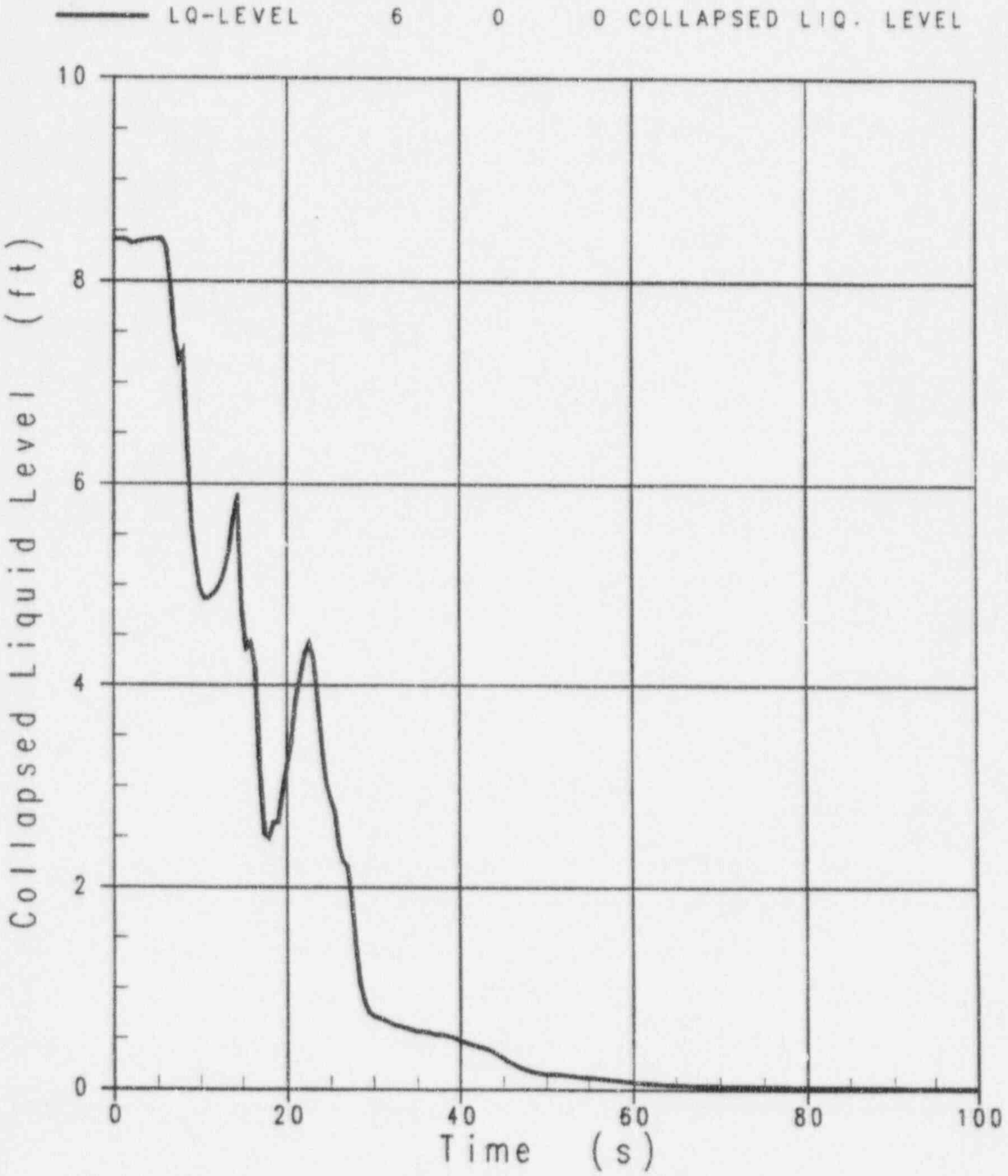


Figure 4.8-3 Mode 3 C_D = 0.8 DECLG Break, Upper Plenum Collapsed Liquid Level

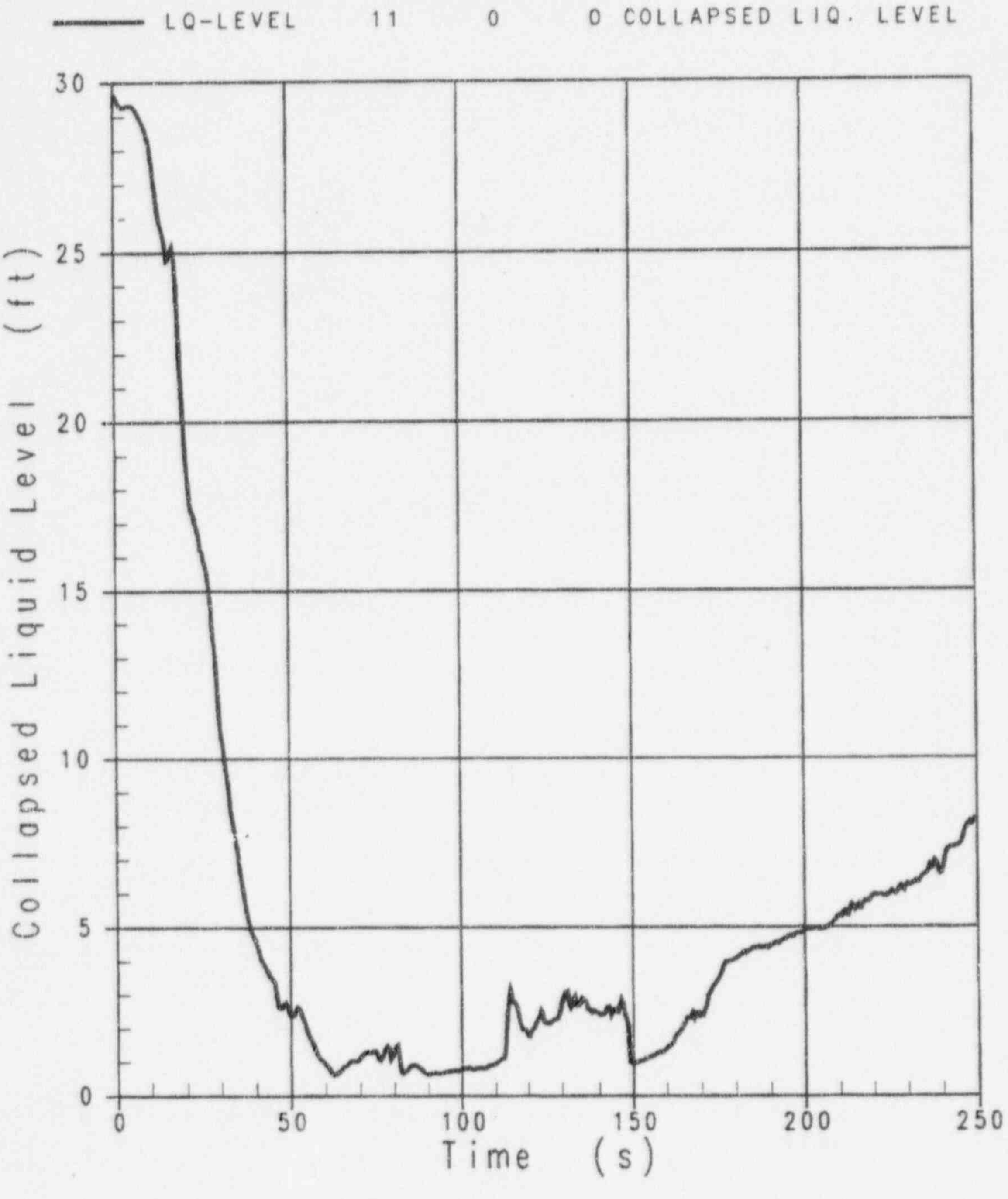


Figure 4.8-4 Mode 3 C_D = 0.8 DECLG Break, Downcomer Collapsed Liquid Level

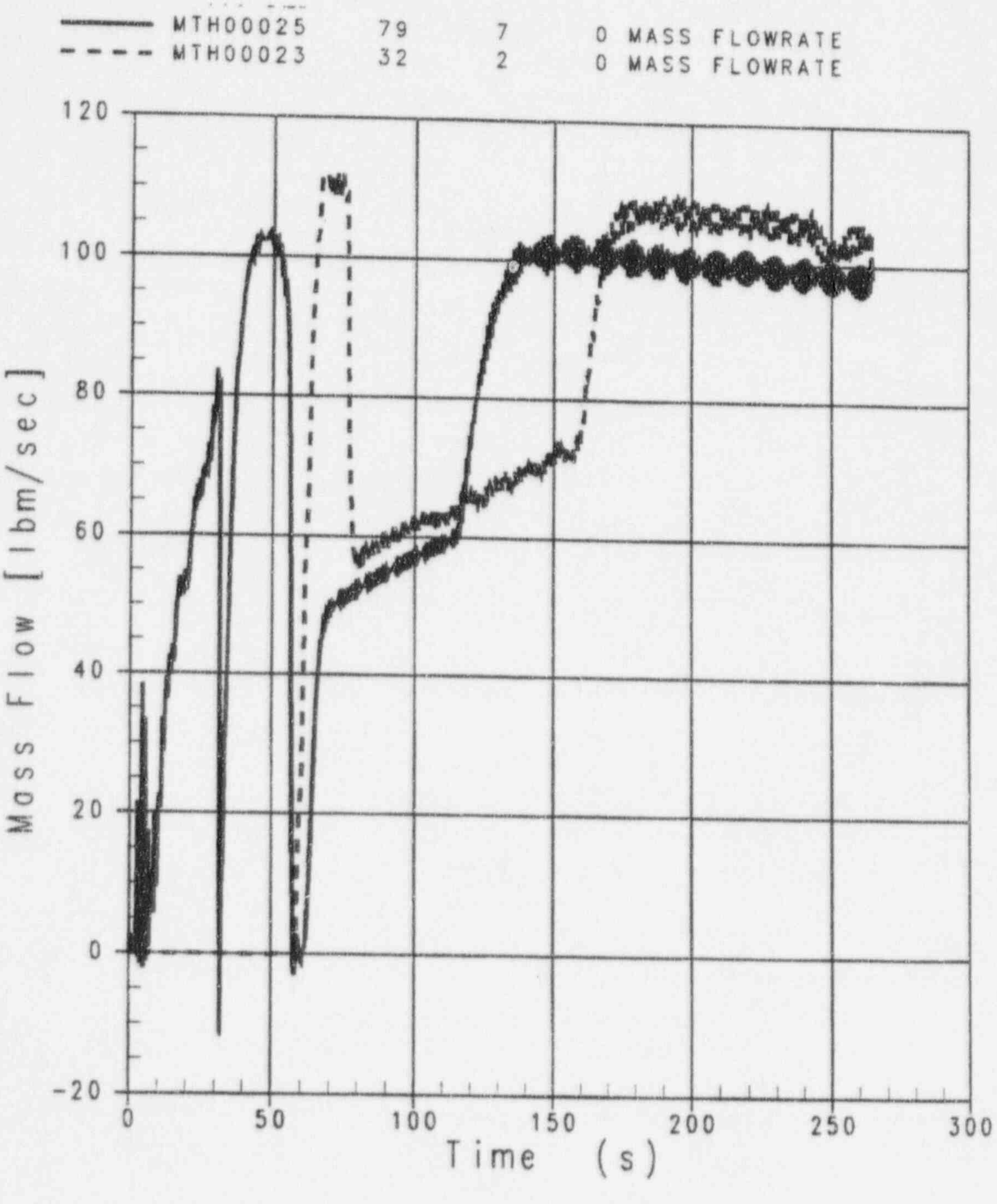


Figure 4.8-5 Mode 3 C_D = 0.8 DECLG Break, CMT Flow Rates

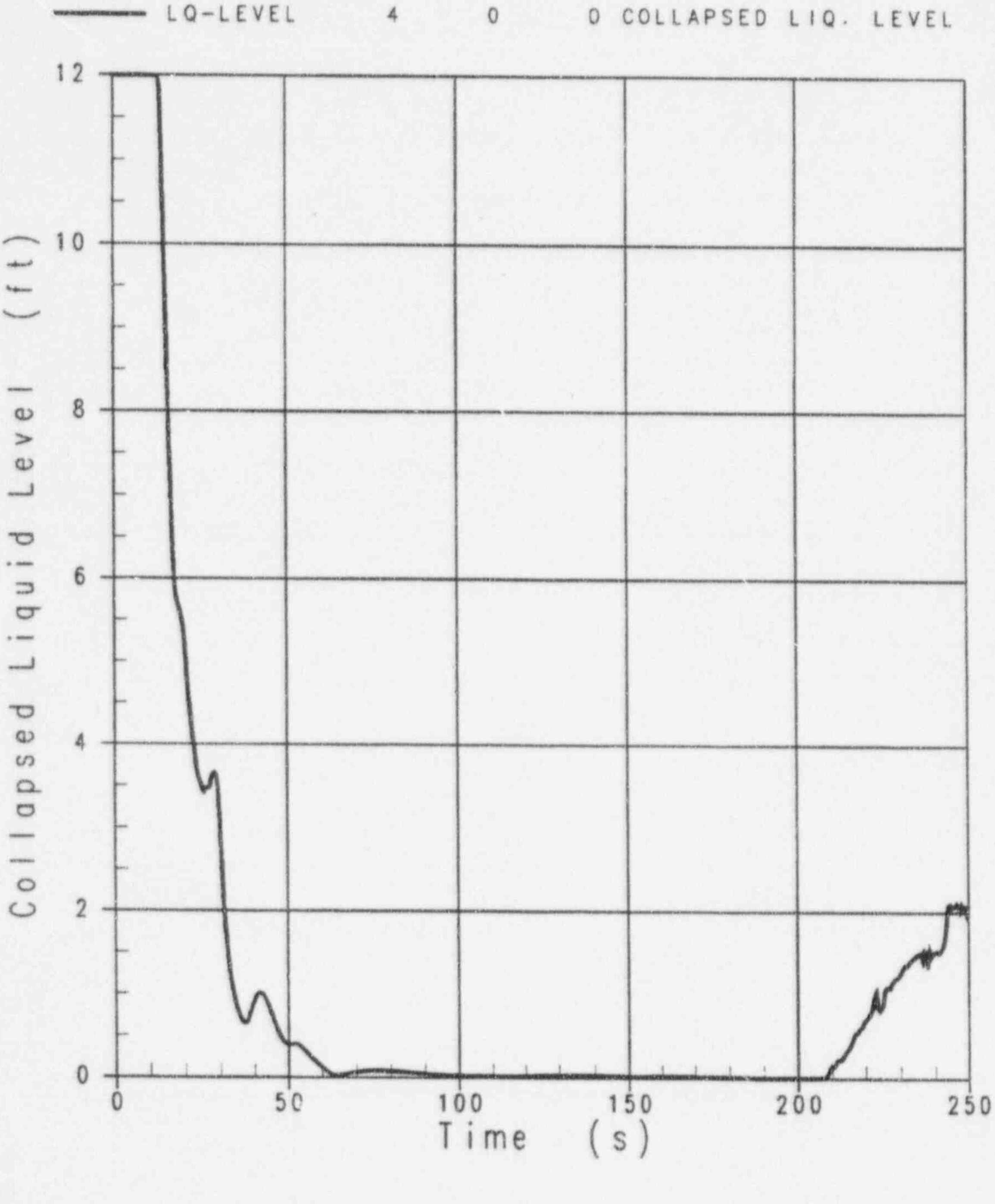


Figure 4.8-6 Mode 3 C_D = 0.8 DECLG Break, Core Collapsed Liquid Level

4.8.2 Inadvertent Actuation of Automatic Depressurization System Results

An inadvertent ADS signal is spuriously generated, and the first-stage ADS valves open. The plant, which is shut down at 1000 psig, is depressurized via the ADS alone. Only safety-related systems that are in service are assumed to operate in this analysis. The second- and third-stage ADS valves actuate based on the design time delays. At the 20-percent tank level, the fourth-stage ADS valves, which are on the hot legs, receive signals to open. Three of the four fourth-stage ADS paths are assumed to open; one of the paths fails to open as the assumed single active failure.

The scenario analyzed is the same inadvertent ADS actuation considered in the SSAR. The sequence of events for the transient is given in Table 4.8-2.

The transient is initiated by the opening of the two first-stage ADS paths. The total throat area of the valves is 9.2 in^2. The opening of the ADS valves causes the primary pressure to fall rapidly (Figure 4.8-7). The accumulators are isolated and thus accumulator injection does not occur. Flow of fluid toward the open ADS path causes the pressurizer to fill by about 100 seconds (Figure 4.8-8), and the ADS flow becomes two-phase. A level begins to form in the upper plenum at about 110 seconds and drops to the hot leg elevation (Figure 4.8-9). Although a safeguards signal is not obtained on low-pressurizer pressure, the ADS opening results in a CMT actuation signal, which opens the valves isolating the CMTs, and injection of cold water begins (Figure 4.8-10); the PRHR HX is also actuated by the CMT actuation signal.

Table 4.8-2
Inadvertent ADS Actuation

Case	Time (seconds)
ADS Stage 1 Flow Starts	0.0
CMT Actuation Signal	0.0
PRHR HX Actuation	0.0
RCPs Start to Coast Down	16.2
ADS Stage 2 Flow Starts	70
ADS Stage 3 Flow Starts	190
ADS Stage 4 Flow Starts	1497
CMT Empty	1820
IRWST Injection Starts	2030

The mixture level in the CMTs is constant until about 350 seconds, then the tanks begin to drain. The RCPs begin to coast down due to an automatic trip signal following a 16.2-second delay. The second-stage ADS actuation at 70 seconds accelerates the depressurization transient slightly. At about 220 seconds following the ADS actuation, enough mass has been discharged that a mixture level forms in the downcomer (Figure 4.8-11). CMT injection flow increases at approximately 350 seconds and the mixture level in the CMT falls steadily after that time.

The levels in the CMTs eventually reach the fourth-stage ADS setpoint. Vent paths, opened from the hot legs, begin discharging fluid. The increased depressurization reduces the flow from ADS stages 1, 2, and 3. The single active failure assumed is that one of the four fourth-stage ADS valves fails to open, maximizing the resistance to depressurizing the RCS to achieve IRWST injection.

The reduced flow through ADS stages 1 through 3 allows the pressurizer level to fall, and these stages begin to discharge only steam after 1645 seconds. By 1820 seconds, the CMTs are empty and delivery ceases. At 2030 seconds, the RCS pressure has fallen enough to allow gravity drain from the IRWST to begin (Figure 4.8-12). The calculation was stopped with a quasi-steady-state condition existing in the RCS with the IRWST delivery exceeding the ADS flows (which are removing the decay heat) and the RCS inventory slowly rising. Core uncovery does not occur; the upper plenum mixture level remains well above the top of the core elevation (18.8 feet) throughout the transient (Figure 4.8-9).

The minimum RCS mass inventory for this case is approximately 146,000 pounds (Figure 4.8-13), which is above the SSAR case minimum inventory. Thus, the consequences of inadvertent ADS actuation during shutdown without the accumulators is bounded by the full-power analysis in the SSAR.

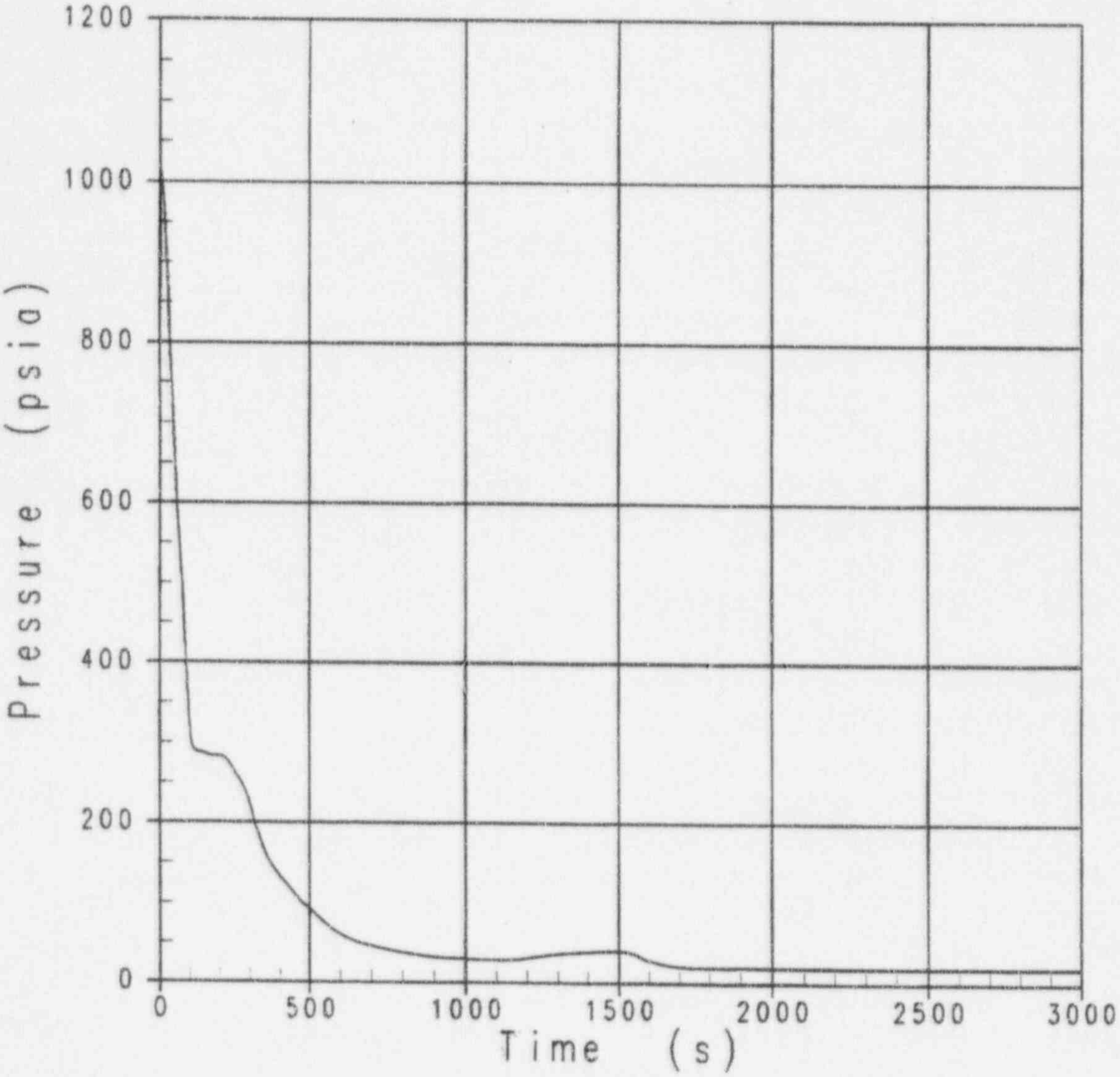


Figure 4.8-7 Pressurizer Pressure, Inadvertent ADS Actuation

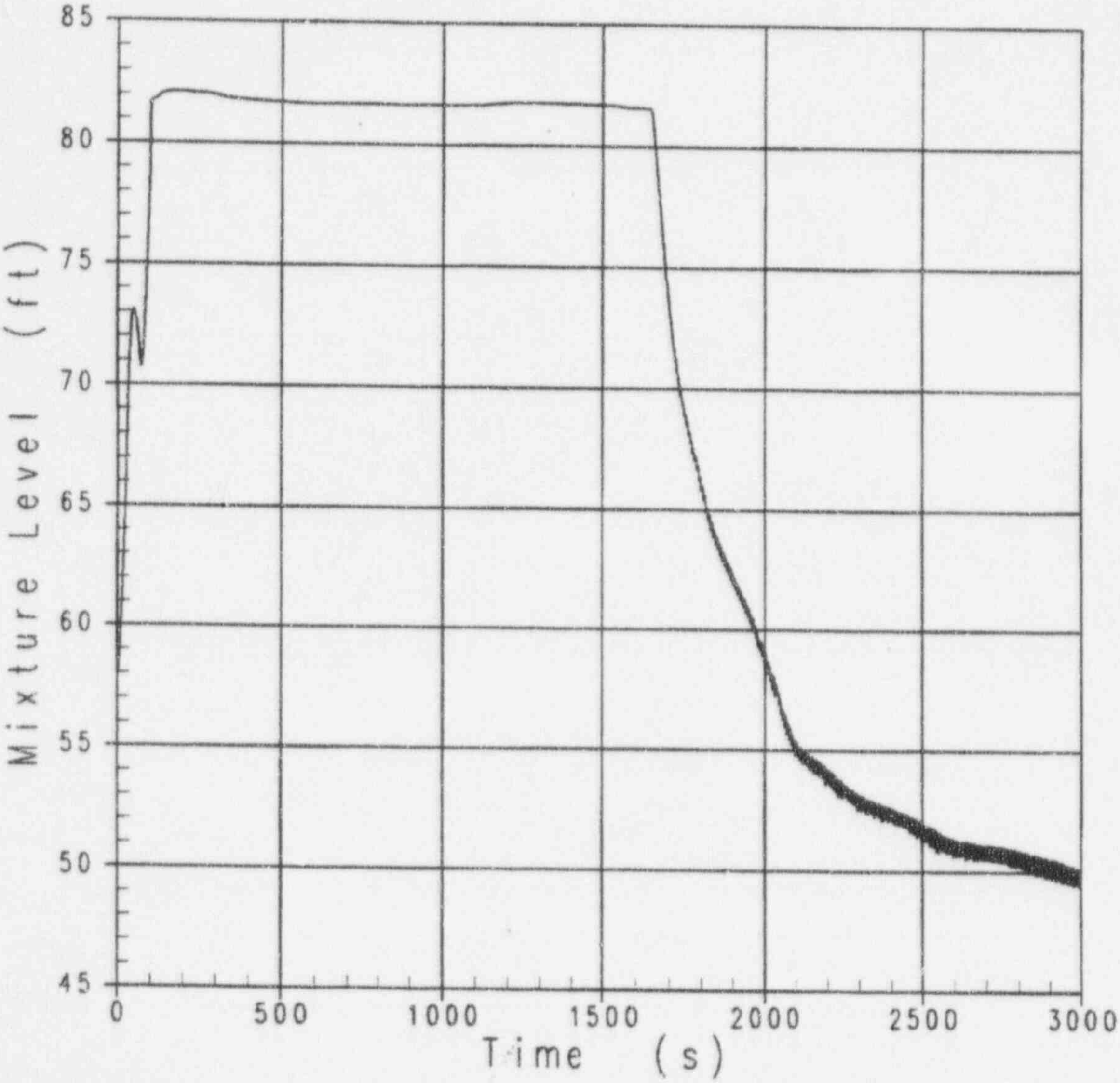


Figure 4.8-8 Pressurizer Level, Inadvertent ADS Actuation

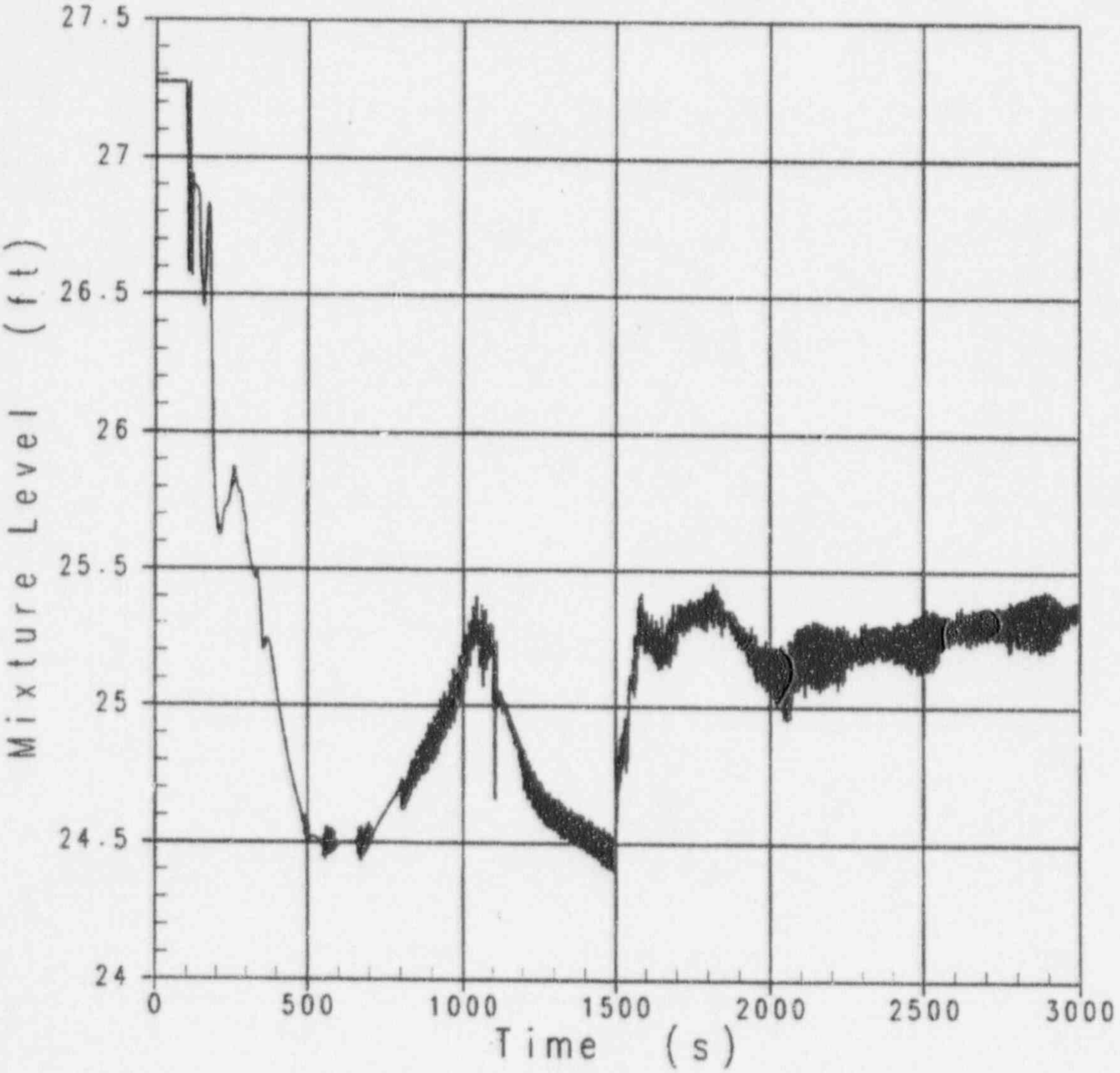


Figure 4.8-9 Core Stack Mixture Level, Inadvertent ADS Actuation

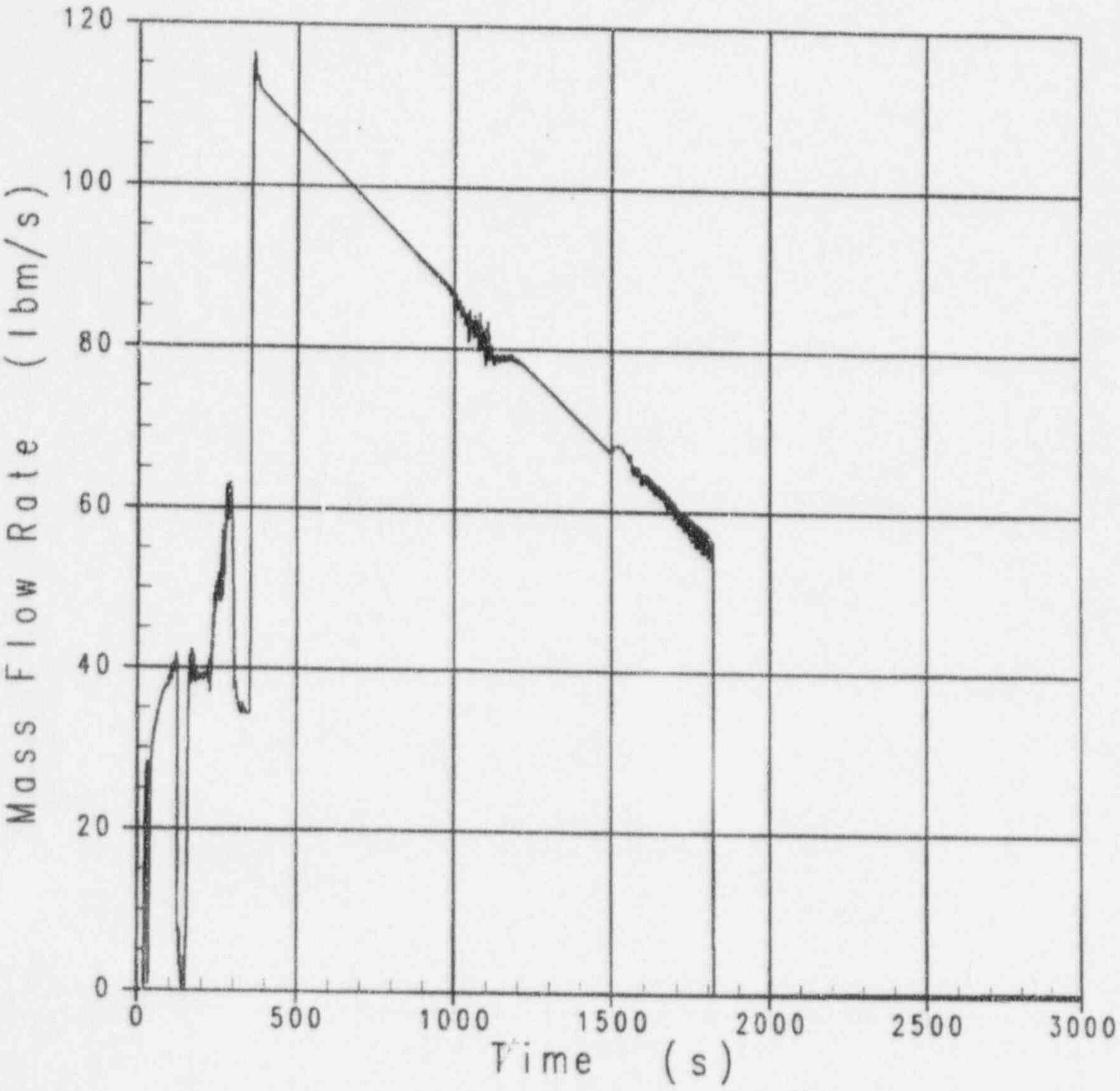


Figure 4.8-10 Loop 1 CMT to DVI Flow, Inadvertent ADS Actuation

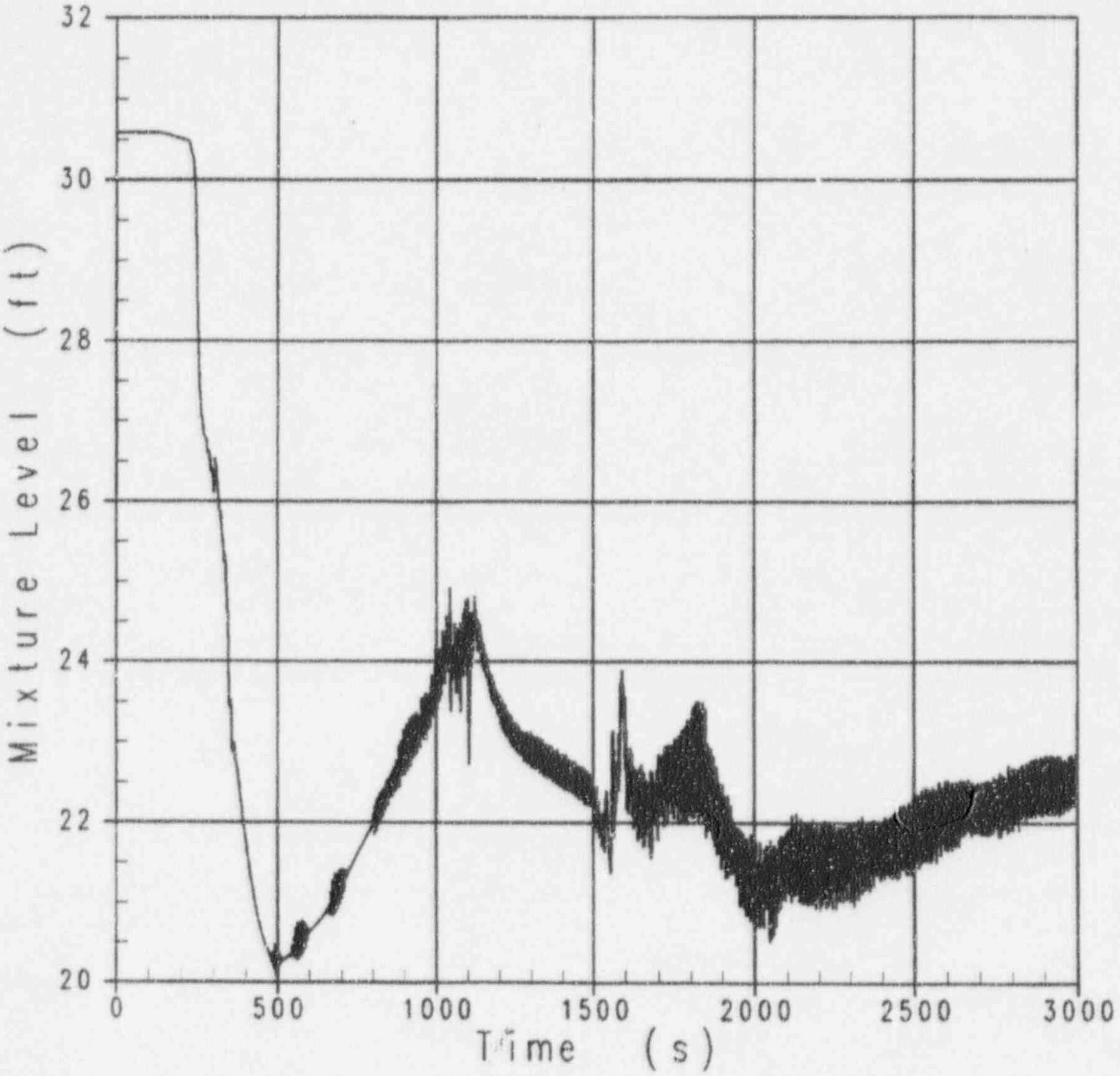


Figure 4.8-11 Downcomer Mixture Level, Inadvertent ADS Actuation

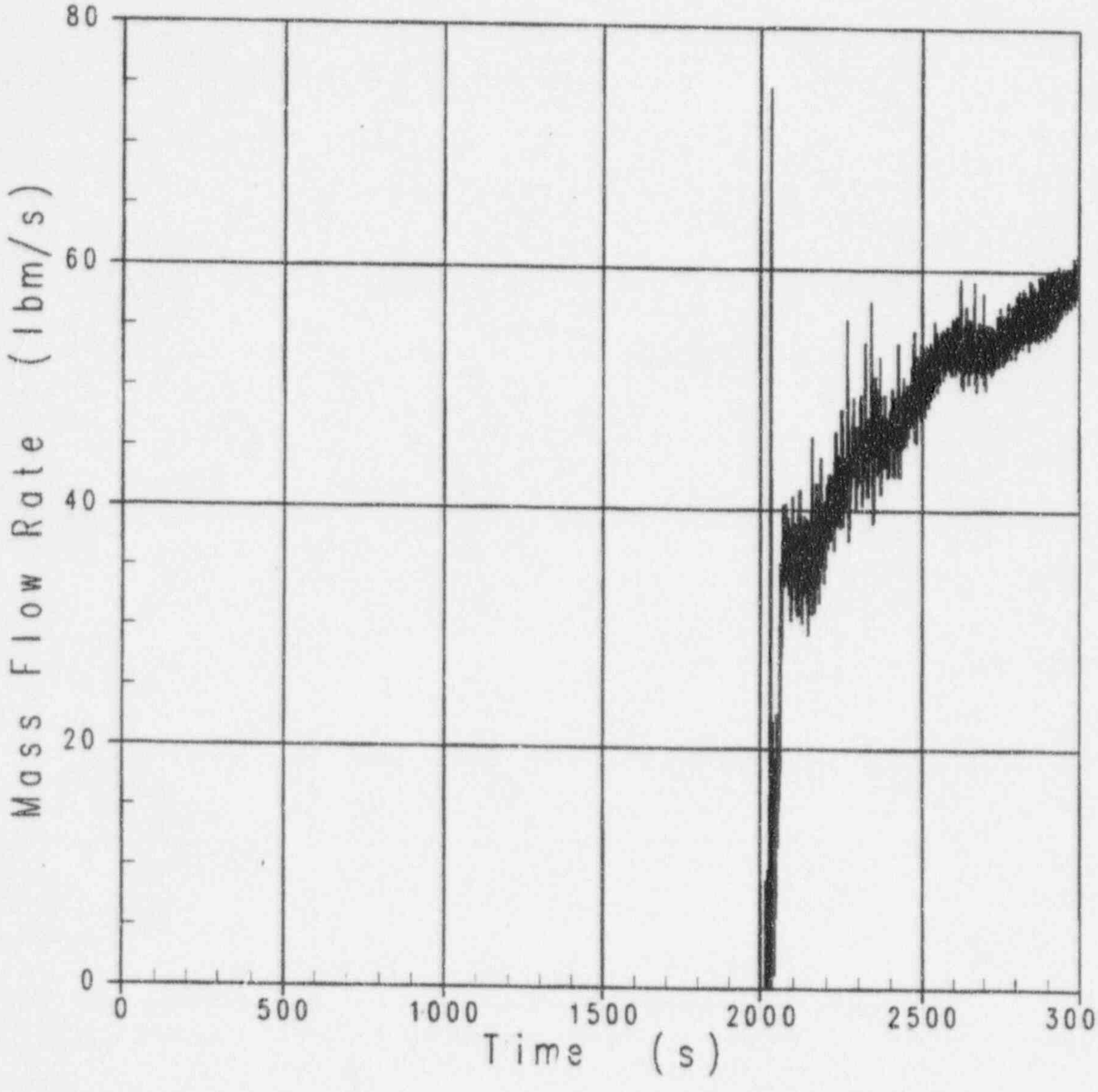


Figure 4.8-12 Loop 1 IRWST Injection Flow, Inadvertent ADS Actuation

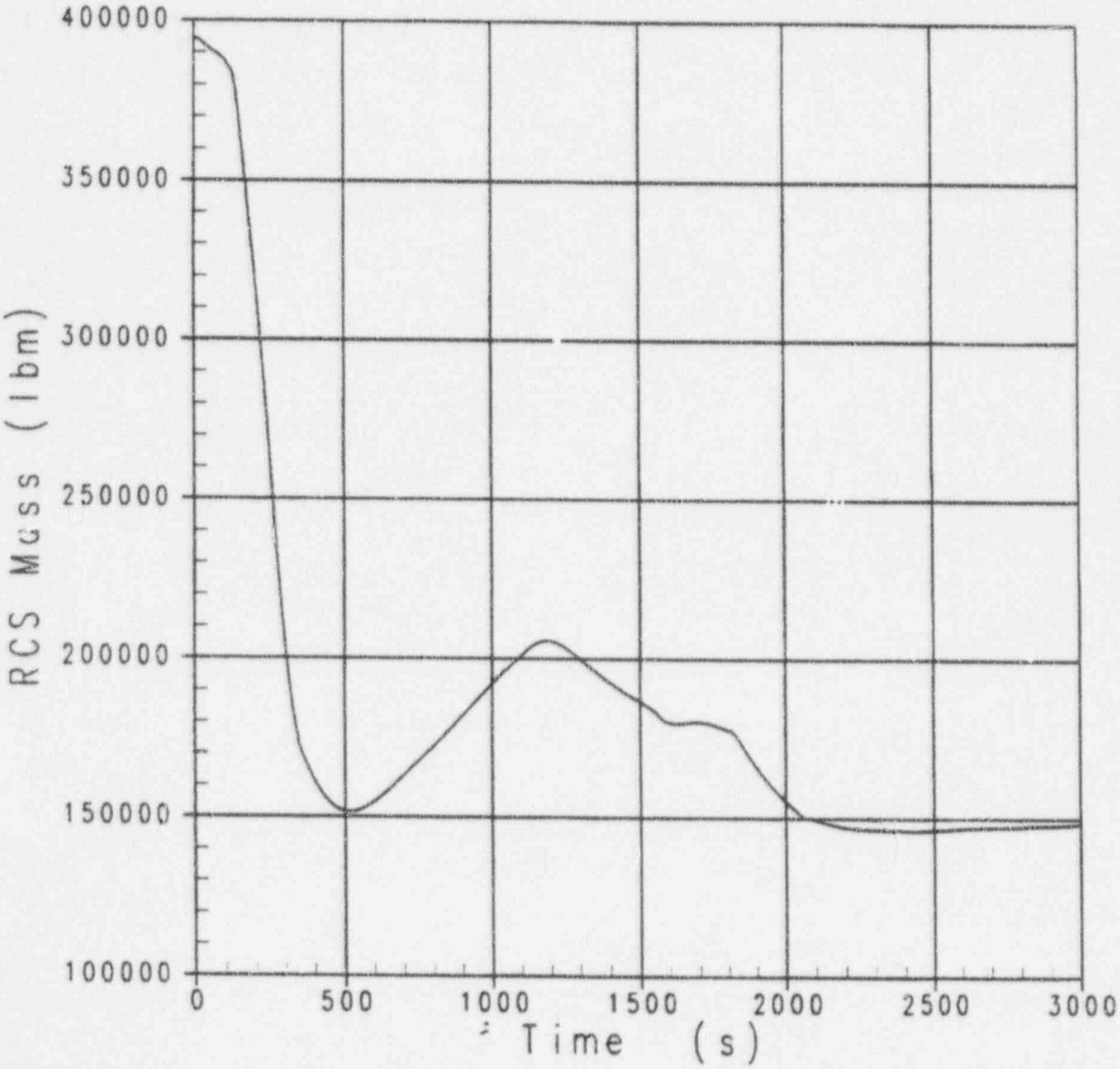


Figure 4.8-13 Primary Mass Inventory, Inadvertent ADS Actuation

4.8.3 Double-ended Direct Vessel Injection Line Break Results

This case models the double-ended rupture of the DVI line at the nozzle into the downcomer. The broken loop injection system (consisting of a CMT and an IRWST delivery line) is modeled to spill completely out of the break. The accumulators are isolated, and thus accumulator injection does not occur. The injection line break evaluates the ability of the plant to recover from a moderately large break with only half of the total available emergency core cooling system (ECCS) capacity available. The venturi installed in the AP600 DVI nozzles provides a 4-inch-diameter flow restriction, which has been modeled in NOTRUMP. The accident analyzed is the same as the DVI line break considered in the SSAR. The sequence of events for this analysis is presented in Table 4.8-3 and a discussion of the results follows.

The break is assumed to open instantaneously at 0 seconds. The subcooled discharge from the downcomer nozzle (Figure 4.8-14) through a 4-inch-diameter venturi causes a rapid RCS depressurization (Figure 4.8-15). Although an "S" signal does not occur on low pressurizer pressure, a CMT actuation signal is generated on low pressurizer level at approximately 18 seconds and following a 1.2-second delay, the isolation valves on the CMT tank delivery and cold leg balance lines begin to open. The opening of the PRHR HX isolation valve on a CMT actuation signal starts the flow through the heat exchanger. The broken loop CMT discharges directly to the containment (Figure 4.8-16), and a small circulation flow provides some injection from the intact loop CMT (Figure 4.8-17).

Table 4.8-3
DEDVI Break Sequence of Events Table

Case	Time (seconds)
Break Open	0.0
CMT Actuation Signal	18
RCPs Start to Coast Down	34.2
ADS Stage 1 Flow Starts	342
ADS Stage 2 Flow Starts	412
ADS Stage 3 Flow Starts	532
ADS Stage 4 Flow Starts	652
IRWST Injection Starts	820

As the pressure falls, the RCS fluid saturates, and at about 50 seconds, a mixture level forms in the upper plenum and then falls to the hot leg elevation (Figure 4.8-18). The upper parts of the RCS start to drain, and a mixture level begins to form in the downcomer at about 100 seconds (Figure 4.8-19) and falls to the elevation of the break at about 300 seconds. Two-phase discharge then occurs from the downcomer side of the break.

At about 110 seconds, the fluid at the top of the broken loop CMT saturates and a level forms and starts to fall. The first-stage ADS setpoint is reached, and after an appropriate delay, the two first-stage paths are opened at 342 seconds. The ensuing steam discharge from the top of the pressurizer increases the RCS depressurization rate.

At about 350 seconds, the fluid at the top of the intact loop CMT saturates and the mixture level in the tank starts to fall slowly. CMT injection after 350 seconds slows the rate of decrease in the downcomer mixture level and eventually causes the level to rise (Figure 4.8-19). The level in the upper plenum also decreases to about the break elevation and then the level begins to increase (Figure 4.8-18). The two second-stage ADS valves begin to open at 412 seconds, following the timer delay between the actuation of the first two stages of the ADS. The third-stage ADS valves open at 532 seconds because of the time delay of 120 seconds for the actuation of this stage of the ADS. At 388 seconds, the broken loop CMT level reaches the fourth-stage ADS setpoint, but the fourth-stage ADS valves do not open until 652 seconds because the minimum time delay is 120 seconds between the actuation of the final two stages of the ADS. Three of the four fourth-stage ADS paths are assumed to open; one of the paths fails to open as the assumed single active failure. Two-phase discharge ensues through the fourth-stage path. By 458 seconds, the broken loop CMT empties.

After the broken loop CMT empties, injection continues from the intact loop CMT as the RCS pressure declines slowly. At 820 seconds, the intact loop CMT has not yet emptied, yet the RCS pressure has fallen to the point that IRWST injection begins. Injection from the IRWST increases as the primary pressure decreases, and the CMT flow rate decreases as the CMT empties. The CMT and IRWST injection causes the mixture level in the upper plenum to increase and level off at the hot leg elevation. The downcomer level also increases and stabilizes at about the break elevation. After the intact loop CMT empties at 2020 seconds, the IRWST injection flow eventually becomes greater than the break and ADS flows, resulting in a slow rise in RCS inventory (Figure 4.8-20). The minimum RCS mass inventory of 119,000 pounds is greater than the corresponding SSAR DEDVI break value. Thus, the consequences of a DEDVI break during shutdown without accumulators is bounded by the full-power analysis in the SSAR.

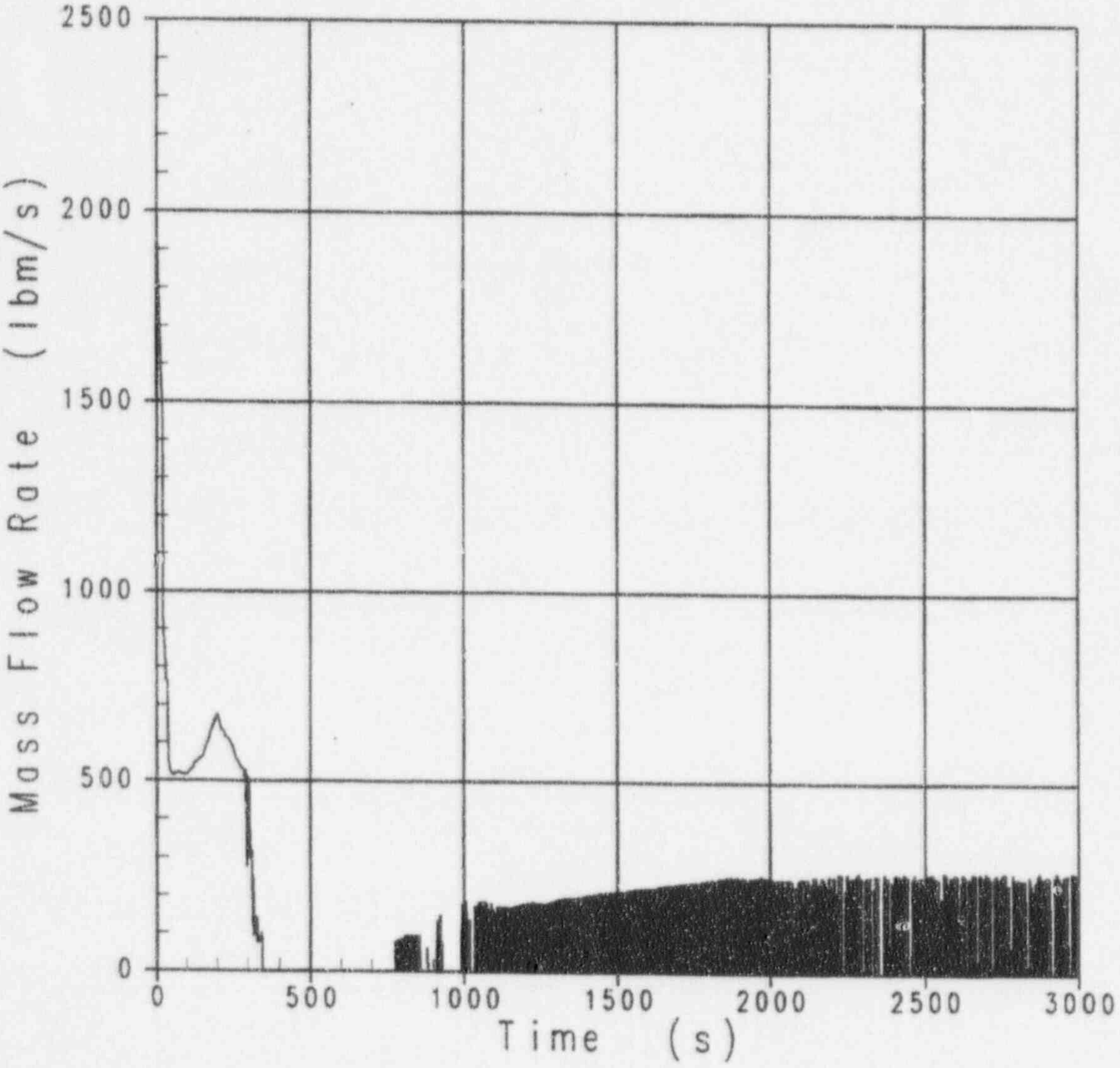


Figure 4.8-14 Break Liquid Flow, DEDVI Break

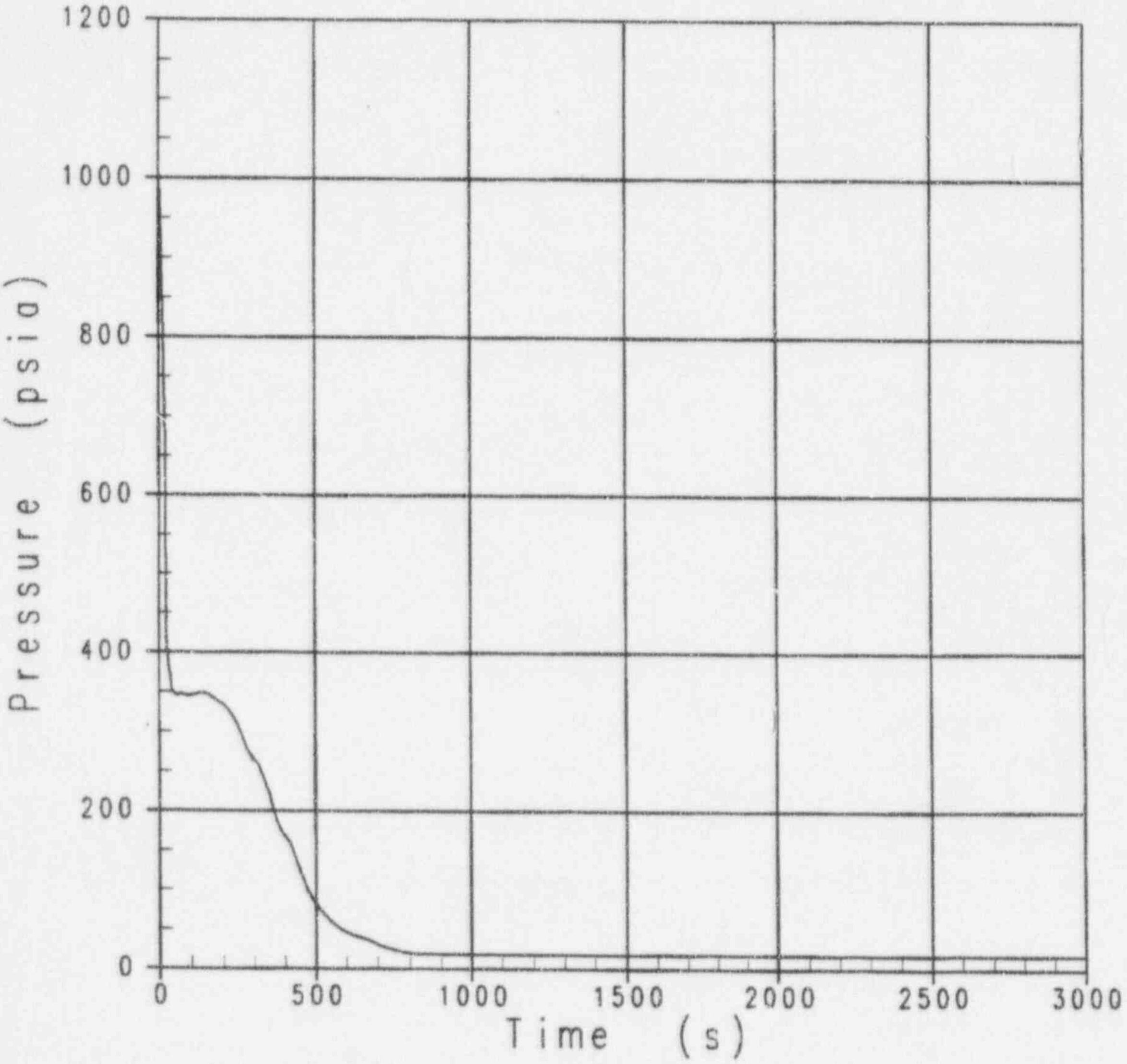


Figure 4.8-15 Pressurizer Pressure, DEDVI Break

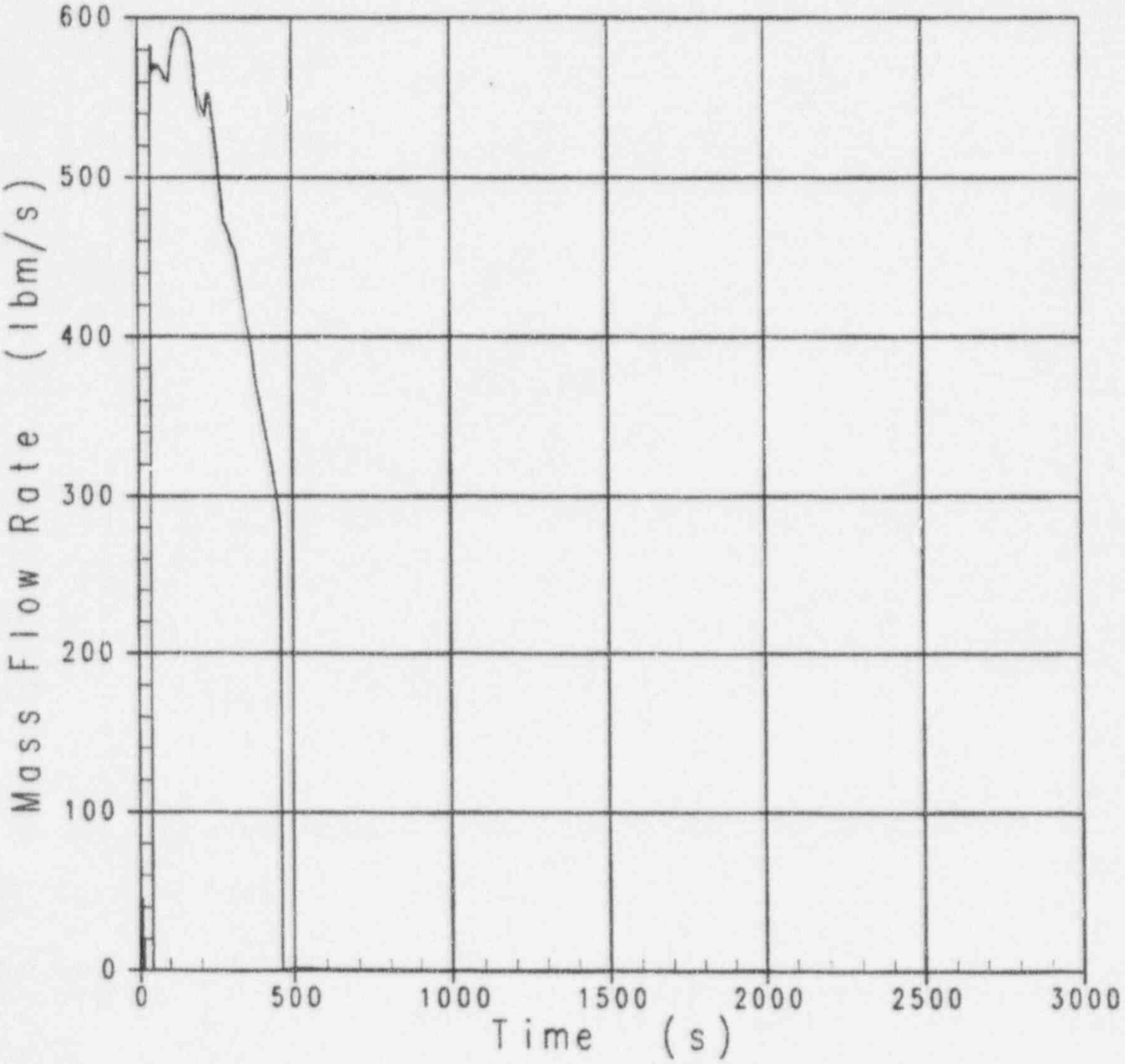


Figure 4.8-16 Loop 1, CMT to DVI Flow, DEDVI Break

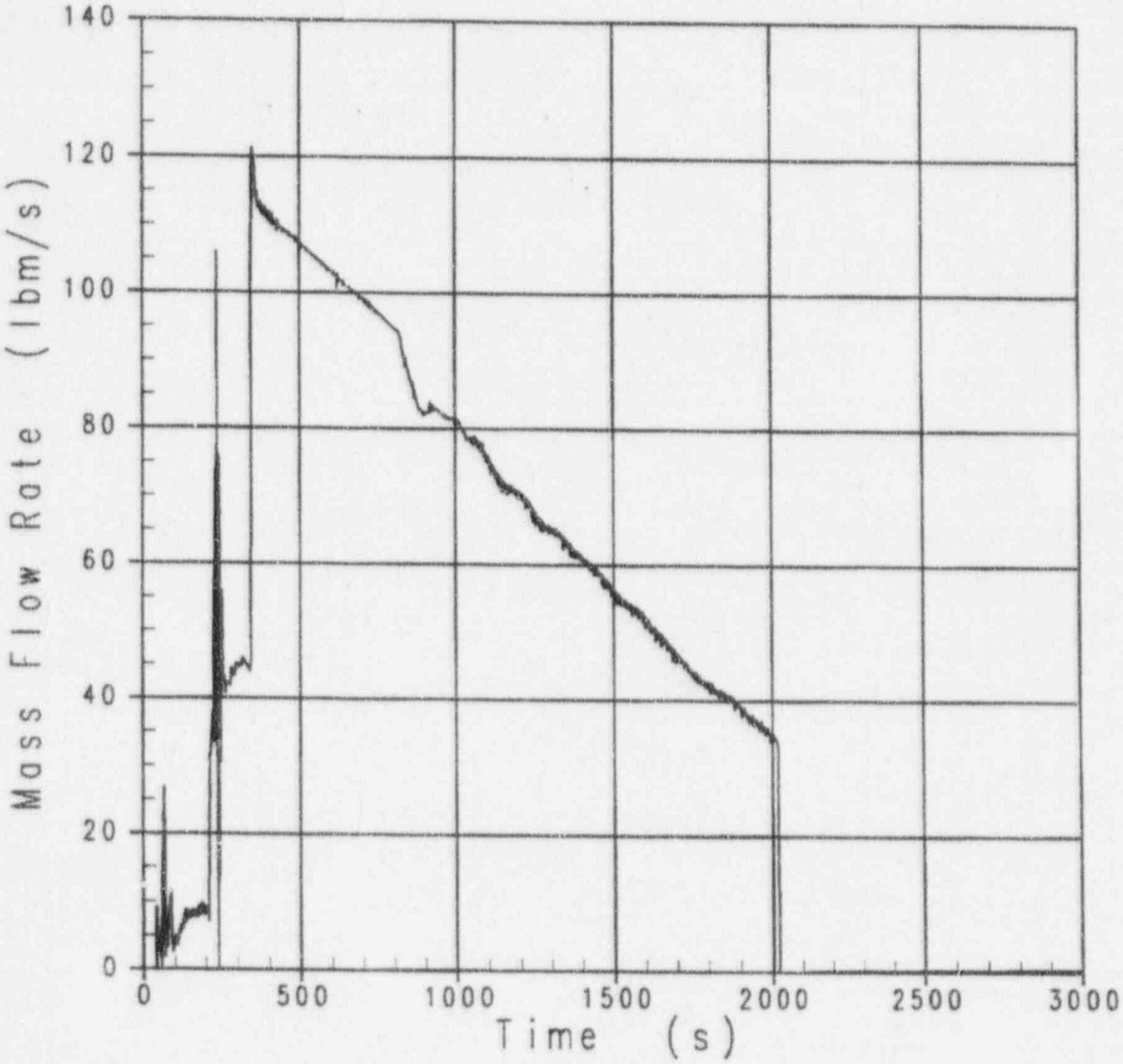


Figure 4.8-17 Loop 2, CMT to DVI Flow, DEDVI Break

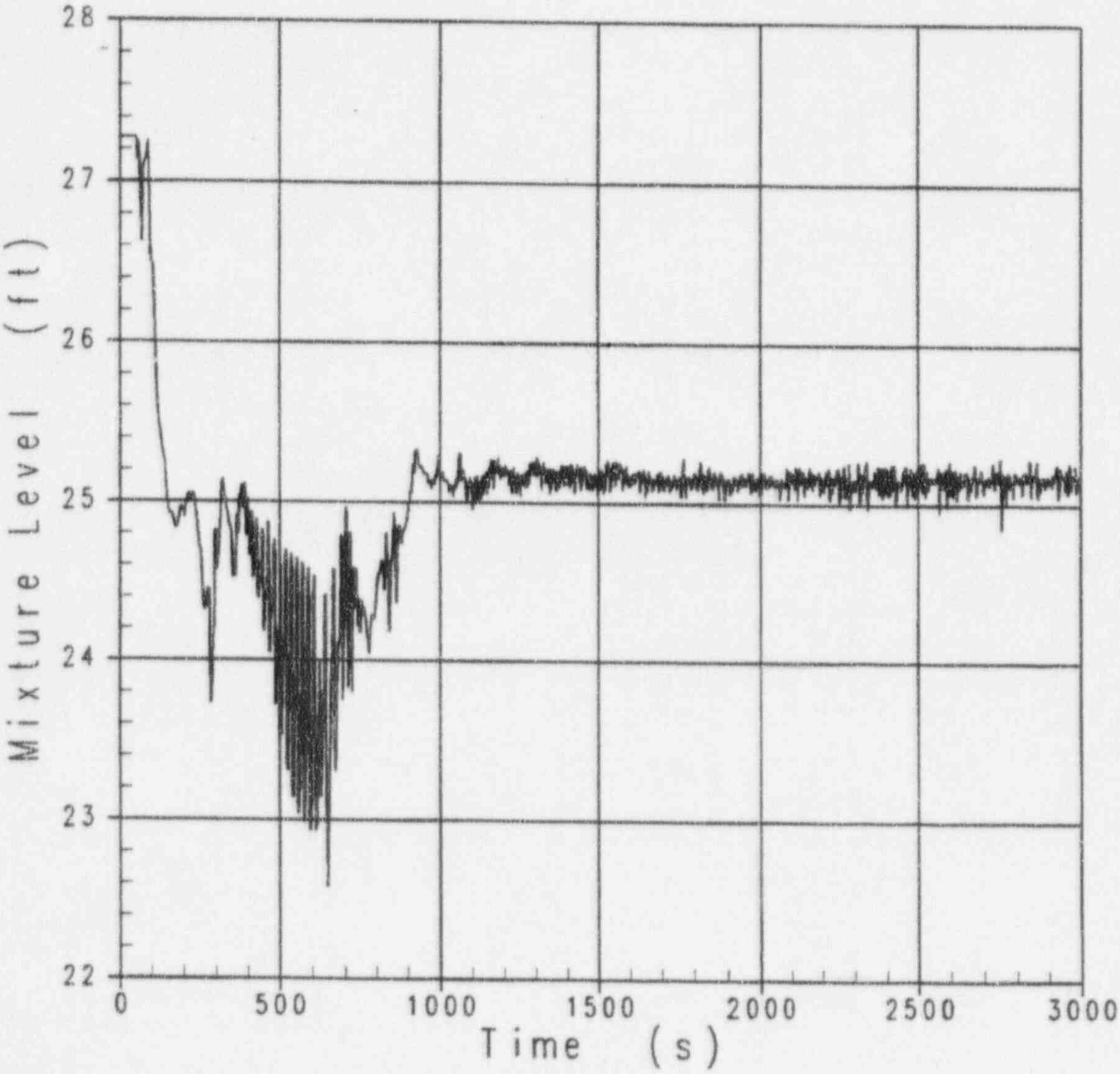


Figure 4.8-18 Core Stack Mixture Level, DEDVI Break

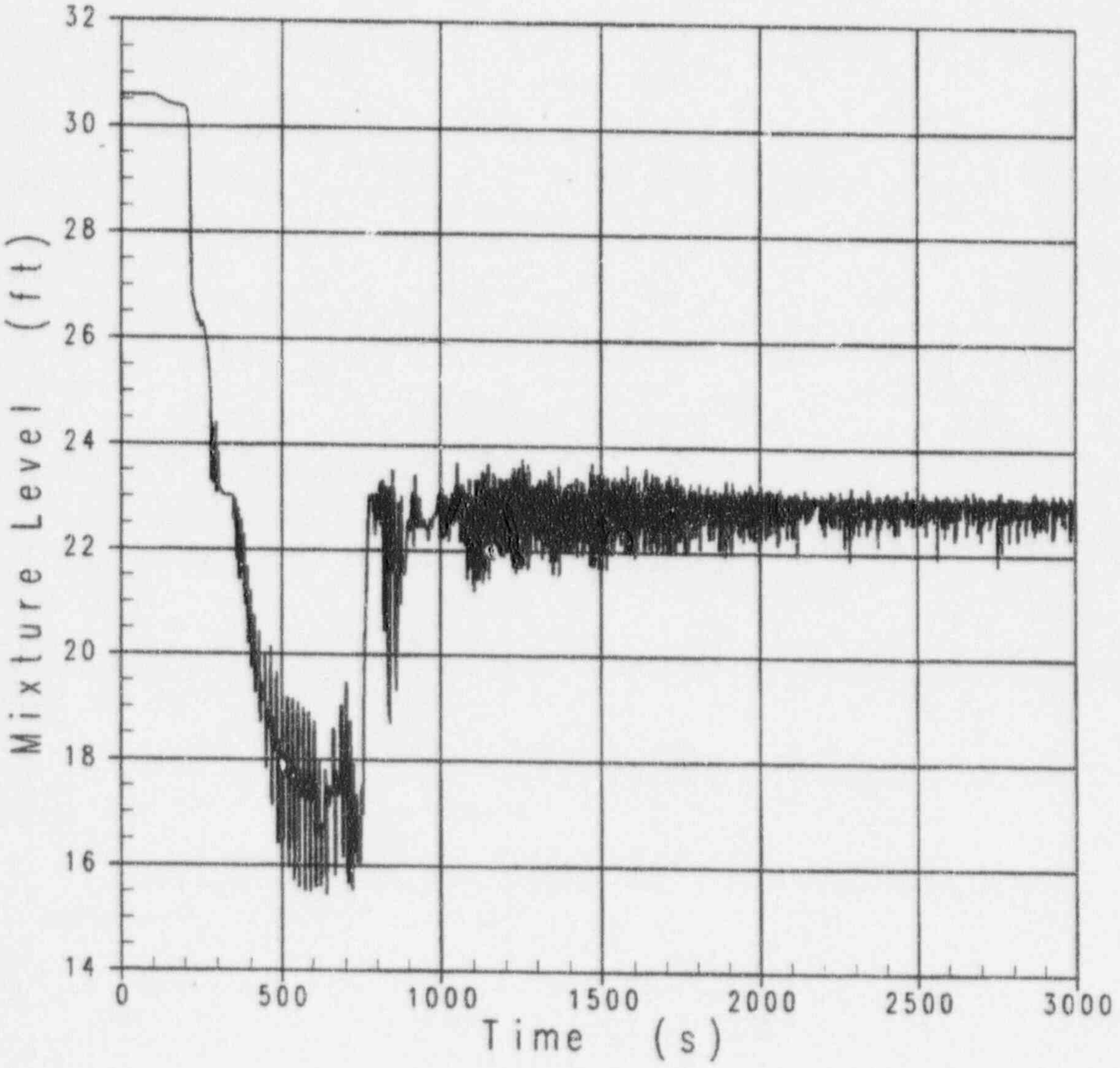


Figure 4.8-19 Downcomer Mixture Level, DEDVI Break

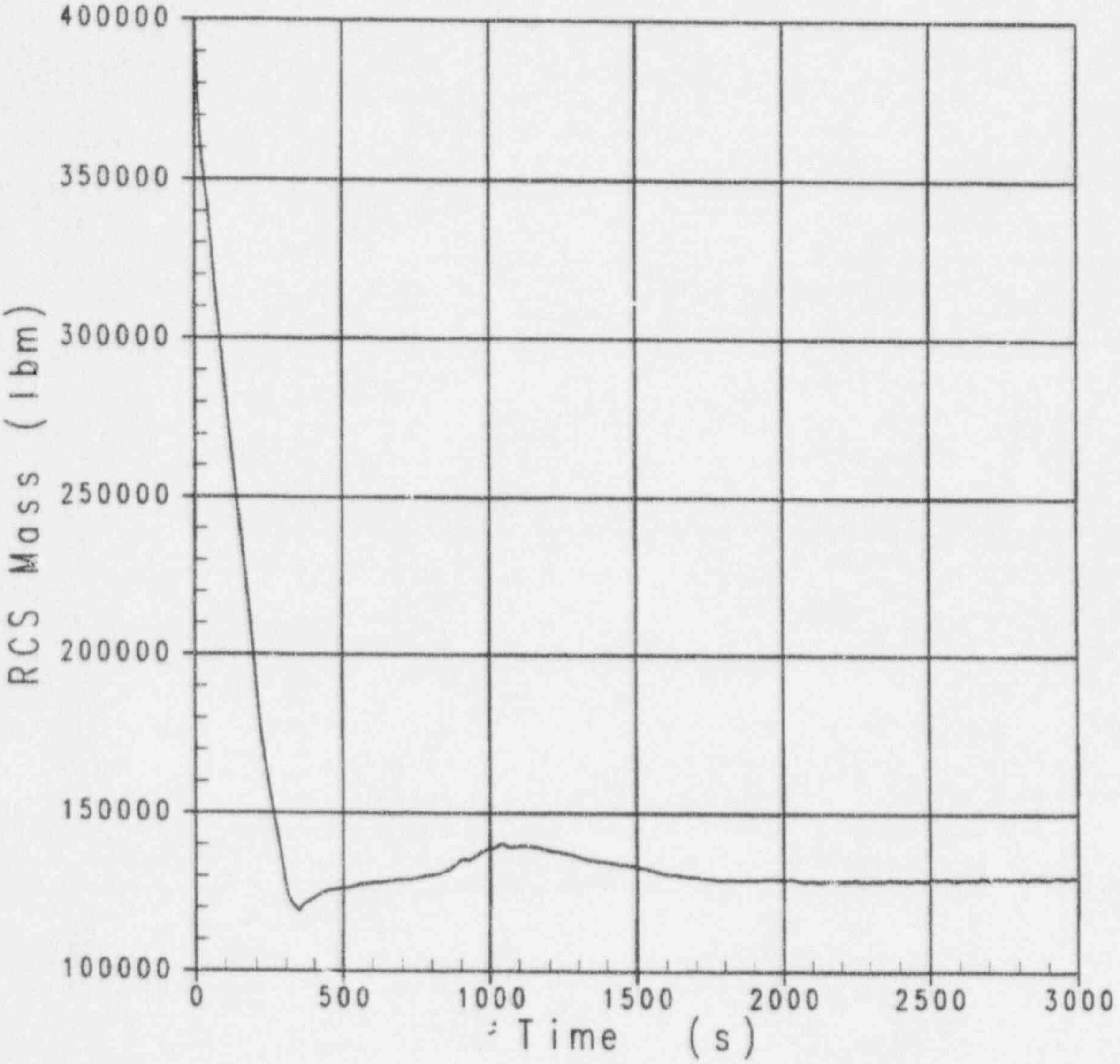


Figure 4.8-20 Primary Mass Inventory, DEDVI Break

4.8.4 Spectrum of Small-Break LOCAs

The small-break LOCA analyses in the SSAR included an analysis of a no-break case due to the inadvertent opening of the 4-inch stage 1 ADS valves due to a spurious signal, as well as analyses for a spectrum of small-break LOCAs. The breaks analyzed included a DEDVI, a 2-inch break in a cold leg with CMT balance line connections, a double-ended rupture of a CMT balance line, and a 2-inch break in the RCS loop with the PRHR HX. The SSAR analyses demonstrated that the DEDVI and inadvertent ADS cases represent limiting small-break LOCAs with respect to providing safety injection delivery to limit core uncovery and ADS depressurization capability to achieve IRWST injection, respectively. Therefore, analyses were performed for these two limiting cases under shutdown conditions. The analyses for the DEDVI break and inadvertent ADS actuation cases under shutdown conditions with the accumulators isolated have demonstrated that the results are bounded by the respective full-power analyses in the SSAR. On this basis, it is considered that analyses for the remaining spectrum of small-break LOCAs for shutdown conditions are not required and that it can be concluded that the full-power small-break LOCA analyses in the SSAR are bounding for the respective cases during shutdown operations.

4.8.5 Loss of RNS Cooling

The RNS is used to reduce the temperature of the RCS during the second phase of plant cooldown, following the first cooldown phase, which is accomplished using the main steam system (MSS). Following initial cooldown, the RNS is used to remove heat from the core and RCS during the plant shutdown. The RNS is designed for the initiation of operation at 4 hours following reactor shutdown, after the first phase of cooldown by the MSS has reduced the RCS to less than or equal to 350°F and 450 psig. The RNS is capable of reducing the temperature of the RCS from 350°F to 120°F within 96 hours after shutdown and maintaining the reactor coolant temperature at or below 120°F for the plant shutdown.

Analyses have been performed to determine the plant response to a loss of RNS cooling in Mode 4 with the RCS intact and in Mode 5 with the RCS open, and the results are discussed in the following subsections. These analyses were performed using the NOTRUMP computer code (Reference 4.8-2), and the NOTRUMP input used for the analyses complies with the AP600 Westinghouse Small-Break LOCA Evaluation Model methodology (WCAP-14601) (Reference 4.8-3) to obtain a suitable representation of the AP600.

4.8.5.1 Loss of RNS Cooling in Mode 4 with RCS Intact

For this analysis, it is assumed that the RNS has just been placed in operation at 4 hours after reactor shutdown with the RCS at 350°F and 450 psig (464.7 psia). It is assumed that a loss of offsite power occurs, resulting in a loss of flow through the RNS, and thus in a loss of

RNS cooling. The MSS is assumed to be unavailable for heat removal, although the steam generator secondary side is assumed to be at saturated conditions for 350°F with the normal water level. Because the Mode 4 plant conditions assumed for the analysis are more limiting than Mode 5 conditions, this analysis is also applicable for a loss of RNS cooling in Mode 5 when the RCS is intact.

It is assumed that only one CMT is available for injection because the Technical Specifications permit one CMT to be taken out of service in Mode 4. Although all of the fourth-stage ADS valves are available in Mode 4, the Technical Specifications permit one of the fourth-stage ADS valves to be out of service in Mode 5 when the RCS is intact. Thus, it was assumed that only three of the fourth-stage ADS valves are available for operation in order to bound the equipment availability in Mode 5. However, one of the three available fourth-stage ADS valves is assumed to fail to open on demand as the single failure, consistent with the single failure assumption used for the small-break LOCA analyses for shutdown conditions.

The accident analyzed is a loss of RNS cooling, which is assumed to result in a complete loss of heat removal for the RCS. The sequence of events for this analysis is presented in Table 4.8-4.

Following the loss of RNS cooling, there is no mechanism for heat removal from the RCS, and the core decay heat generation causes the reactor coolant temperature and pressure to increase. Although the MSS is assumed to be unavailable for heat removal, the steam

Table 4.8-4
Loss of RNS Cooling in Mode 4 with RCS Intact
Sequence of Events

Event	Time (seconds)
Loss of RNS Cooling	0
RNS Relief Valve Flow Starts	1400
CMT Actuated	9500
RNS Relief Valve Flow Terminated	9700
ADS Stage 1 Flow Starts	10,075
ADS Stage 2 Flow Starts	10,145
ADS Stage 3 Flow Starts	10,265
ADS Stage 4 Flow Starts	10,895
IRWST Injection Starts	11,845

generators represent a heat sink which slows the rate of heatup of the reactor coolant. The fluid temperature at the core outlet for the transient is shown in Figure 4.8-21. The reactor oolant heatup causes the system pressure to increase as shown in Figure 4.8-22 until the pressure reaches the RNS relief valve setpoint of 563 psig (577.7 psia) at approximately 1400 seconds. The normal relieving capacity of the RNS relief valve is 555 gpm, and the pressure is maintained at the relief valve setpoint as the temperature continues to increase and reactor coolant is discharged from the relief valve. The expansion of the water due to the coolant temperature increase also causes the pressurizer level to increase slightly as shown in Figure 4.8-23.

The loss of reactor coolant through the relief valve is not sufficient to remove the core decay heat, and the reactor coolant temperature continues to increase until the core outlet temperature reaches saturation at the relief valve setpoint at approximately 5500 seconds. The generation of steam in the core causes the system pressure to increase above the RNS relief valve setpoint and the pressurizer level to continue to increase. A mixture level begins to form in the upper plenum at approximately 5670 seconds and drops to the top of the hot leg elevation as shown in Figure 4.8-24. At about 6250 seconds, enough mass has been discharged such that a mixture level also forms in the downcomer (Figure 4.8-25), and the downcomer two-phase level begins to decrease. As the boiling front moves lower and lower into the core, more steam generation occurs and the pressure continues to increase. Once the entire core length is boiling, the upper plenum mixture level is within the hot leg perimeter. At approximately 7980 seconds, when steam begins to flow through the relief valve along with liquid, the pressure begins to decrease. The pressurizer level also begins to decrease as water drains from the pressurizer into the reactor coolant system hot leg. However, the voiding in the RCS increases as the pressure decreases, and flashing begins to occur in the pressurizer at approximately 8660 seconds. This additional steam generation causes the pressure to begin to increase, and the relief valve flow becomes solely liquid again. The steam voiding in the pressurizer not only causes the pressure increase, but also facilitates draining, and the pressurizer level continues to decrease.

As the pressurizer level decreases, a CMT actuation signal is generated automatically on low pressurizer level, and following a 1.2-second delay, the isolation valves on the available CMT tank delivery lines open and CMT injection flow is initiated at approximately 9500 seconds as shown in Figure 4.8-26. The opening of the PRHR HX isolation valve on a CMT actuation signal starts the flow through the heat exchanger. The CMT injection causes the reactor coolant pressure to decrease below the RNS relief valve setpoint, and the loss of reactor coolant is terminated at approximately 9700 seconds. As the CMT level decreases (Figure 4.8-27), the first-stage ADS setpoint at 67.5 percent is reached at 10,075 seconds. The second-stage and third-stage ADS valves also open following the timer delays for the actuation of the second- and third-stage ADS valves. The vapor and liquid flow through the ADS valves (Figures 4.8-28 and 4.8-29) results in a rapid depressurization of the reactor coolant system. The CMT reaches the fourth-stage ADS setpoint of 20 percent, and two of the four fourth-stage paths open at 10,895 seconds. As noted previously, it is assumed that one of the fourth-stage paths is out of service, and one path is assumed to fail as the single active failure. The vapor and liquid flow through the fourth stage ADS paths (Figures 4.8-30 and 4.8-31) further reduces the pressure to the point where IRWST injection begins at approximately 11,845 seconds (Figure 4.8-32).

The CMT and IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 4.8-24 and 4.8-25, respectively. As shown in Figure 4.8-24, the core stack mixture level is maintained well above the elevation of the top of the core active fuel (18.8 feet) throughout the transient. At the end of the transient, the core stack mixture level has been restored to within the hot leg perimeter and the downcomer mixture level has been restored to the DVI nozzle elevation. The fluid temperature at the core outlet has also been reduced and is being maintained at less than 250°F. As shown in Figure 4.8-33, the reactor coolant mass inventory twice reaches a minimum of approximately 120,000 pounds, when the CMT and IRWST injection then increase the inventory. The reactor coolant mass inventory is greater than 150,000 pounds and is slowly increasing at the end of the transient. Thus, it is concluded that the consequences of a loss of RNS in Modes 4 and 5 with the RCS intact are acceptable.

4.8.5.2 Loss of RNS Cooling in Mode 5 with RCS Open

For this analysis, it is assumed that the RNS is in operation in Mode 5 at 24 hours after reactor shutdown with the ADS Stage 1, 2, and 3 valves open and the RCS vented to the IRWST. The reactor coolant temperature is assumed to be at 160°F, and the pressurizer pressure is assumed to be at atmospheric pressure plus the elevation head in the IRWST, or 18.2 psia. The steam generator secondary side is assumed to be drained, and thus, there is no secondary heat sink for this case. It is assumed that the CMTs and the PRHR are not available because the Technical Specifications permit them to be taken out of service when the RCS is open in Mode 5. It is also assumed that only two of the fourth-stage ADS valves are available for potential use by the operators because the Technical Specifications permit two of the fourth-stage ADS valves to be out of service in Mode 5 when the RCS is open. In addition, one of the two available fourth-stage ADS valves is assumed to fail to open on demand as the single failure. The Technical Specifications also permit one of the two IRWST injection paths to be out of service in Mode 5 with the RCS open, and thus, only one of the IRWST injection paths is assumed to be available.

It is assumed that a loss of offsite power occurs, resulting in a loss of RNS flow, and thus a loss of RNS cooling. The sequence of events for this analysis is presented in Table 4.8-5.

Following the loss of RNS cooling, there is no mechanism for heat removal from the RCS and the core decay heat generation results in an increase in the reactor coolant temperature. The fluid temperature at the core outlet for the transient is shown in Figure 4.8-34. The core

Table 4.8-5
Loss of RNS Cooling in Mode 5 with RCS Open
Sequence of Events

Event	Time (seconds)
Loss of RNS Cooling	0
Hot Leg Empty	7200
ADS Stage 4 Flow Initiated	7290
IRWST Injection Starts	7400

outlet fluid temperature increases steadily until approximately 3000 seconds when saturation temperature is reached and voiding is initiated in the core. Because the RCS is vented to the IRWST via ADS Stages 1, 2, and 3, the pressure initially remains constant until approximately 3800 seconds as shown in Figure 4.8-35. As the void generation in the system increases, the vapor flow through ADS Stages 1, 2, and 3 is not sufficient to maintain the pressure, and the pressure increases to approximately 30.6 psia and then begins to decrease. As shown in Figure 4.8-36, the pressurizer level also increases as the reactor coolant temperature increases, and the level subsequently reaches the top of the pressurizer as a result of the steam generation in the system. As shown in Figures 4.8-37 and 4.8-38, a mixture of steam and water is discharged via ADS Stages 1, 2, and 3 after the pressurizer fills.

The continued loss of reactor coolant through ADS Stages 1, 2, and 3 causes the pressure to begin to decrease after approximately 5200 seconds. The core outlet temperature is at saturation and also begins to decrease as the pressure decreases. A mixture level begins to form in the upper plenum at approximately 4090 seconds, and the level begins to decrease as shown in Figure 4.8-39, as the voiding continues in the system. At about 5100 seconds, enough mass has been discharged that a mixture level forms in the downcomer (Figure 4.8-40) and the downcomer level also begins to decrease. The pressurizer level does not decrease significantly due an increasing void fraction in the pressurizer.

As the voiding in the core continues, the core stack mixture level continues to decrease as shown in Figure 4.8-39. The void fraction in the hot legs also increases, and the mixture level in the hot leg begins to decrease after 4000 seconds. The hot leg is empty at approximately 7200 seconds as shown in Figure 4.8-41. This is the normal signal for opening the fourth-stage ADS valves and to initiate IRWST injection when the systems are aligned for automatic actuation. Thus, it is assumed that the operator will initiate manual action at 7200 seconds to open the fourth-stage ADS valves and to open the IRWST flow path to permit IRWST injection when the downcomer pressure is sufficiently low. Thus, discharge through one of the fourth-stage ADS valves is initiated at 7290 seconds as shown in Figures 4.8-42 and

4.8-43. As noted previously, one of the two available fourth-stage ADS paths is assumed to fail to open as the single active failure. The flow through the fourth-stage ADS path results in a further reduction in the pressurizer pressure and a rapid decrease in the pressurizer level. The downcomer pressure is also reduced to the point where IRWST injection is initiated at approximately 7400 seconds (Figure 4.8-44). However, the pressurizer level increases due to subsequent additional void formation at the lower pressure, and the downcomer pressure increases slightly, temporarily terminating the IRWST flow. The downcomer pressure then drops slowly, resulting in sustained IRWST injection at approximately 8204 seconds.

The IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 4.8-40 and 4.8-41, respectively. As shown in Figure 4.8-40, the core stack mixture level is maintained well above the elevation of the top of the core active fuel (18.8 feet) throughout the transient. At the end of the transient, the core stack mixture level has been restored to above the middle of the hot leg elevation and the downcomer mixture level is above the DVI nozzle elevation. The fluid temperature at the core outlet has also been reduced to approximately 250°F. As shown in Figure 4.8-45, the reactor coolant mass inventory reaches a minimum of approximately 170,000 pounds and then begins to increase as a result of the IRWST injection. Thus, it is concluded that when the appropriate operator action is performed, one ADS Stage 4 valve is effective in reducing system pressure so that the consequences of a loss of RNS in Mode 5 with the RCS vented are acceptable.

The analysis presented here is a conservative analysis of a loss of RNS cooling during reduced inventory conditions. During Mode 5, prior to draining to mid-loop conditions, the operator manually opens the ADS Stages 1 through 3 paths to the IRWST. With the RCS "open," the operator then proceeds to slowly drain the RCS to "mid-loop" conditions, for the purpose of performing steam generator maintenance or other maintenance that requires a reduced RCS water level. At this moment, it is postulated that a loss of decay heat removal via the nonsafety-related RNS occurs. A loss of RNS cooling at this time is selected because it is the earliest time the RCS could be placed into a reduced inventory (that is, RCS open) condition. In addition, the backpressure on the reactor vessel, due to the presence of water in the pressurizer, is higher at this time. This presents the most challenging condition for the ADS to depressurize the RCS to IRWST cut-in pressure. This transient represents the most limiting "surge line flooding" scenario, a term commonly used for operating plants to refer to the phenomenon associated with water in the pressurizer and surge line causing a high backpressure in the RCS, which potentially challenges the ability of the low head safety injection systems to inject properly. In addition, this scenario can potentially challenge the design pressure of temporary nozzle dams placed in the steam generators to facilitate maintenance of the RCS during refueling.

For a loss of the RNS during mid-loop operations, calculations have been performed to determine the time until core uncovery would occur. The results of these calculations are presented in Table 2.3-2 of this report. The progression of events following a loss of RNS cooling during mid-loop would result in a heatup of the RCS to saturation, followed by a boiling off of the coolant to the IRWST via the ADS Stages 1, 2, and 3 valves. Eventually, the operator would actuate the IRWST upon a loss of RCS subcooling, followed by the loss of RCS inventory. The conditions in the RCS following IRWST and fourth-stage ADS actuation would be similar to those in this evaluation. As shown in Table 2.3-2, the operator would have at least 100 minutes from the loss of RNS cooling until the onset of core uncovery to manually actuate the IRWST and ADS Stage 4. In general, the results of a loss of RNS during mid-loop conditions would be similar but slightly less severe to those presented in this evaluation, due to the lower levels of decay heat and to the absence of the initial water inventory in the pressurizer, which will serve to reduce the surge line flooding phenomenon that degrades the depressurization capability of the ADS Stages 1 through 3 vent paths.

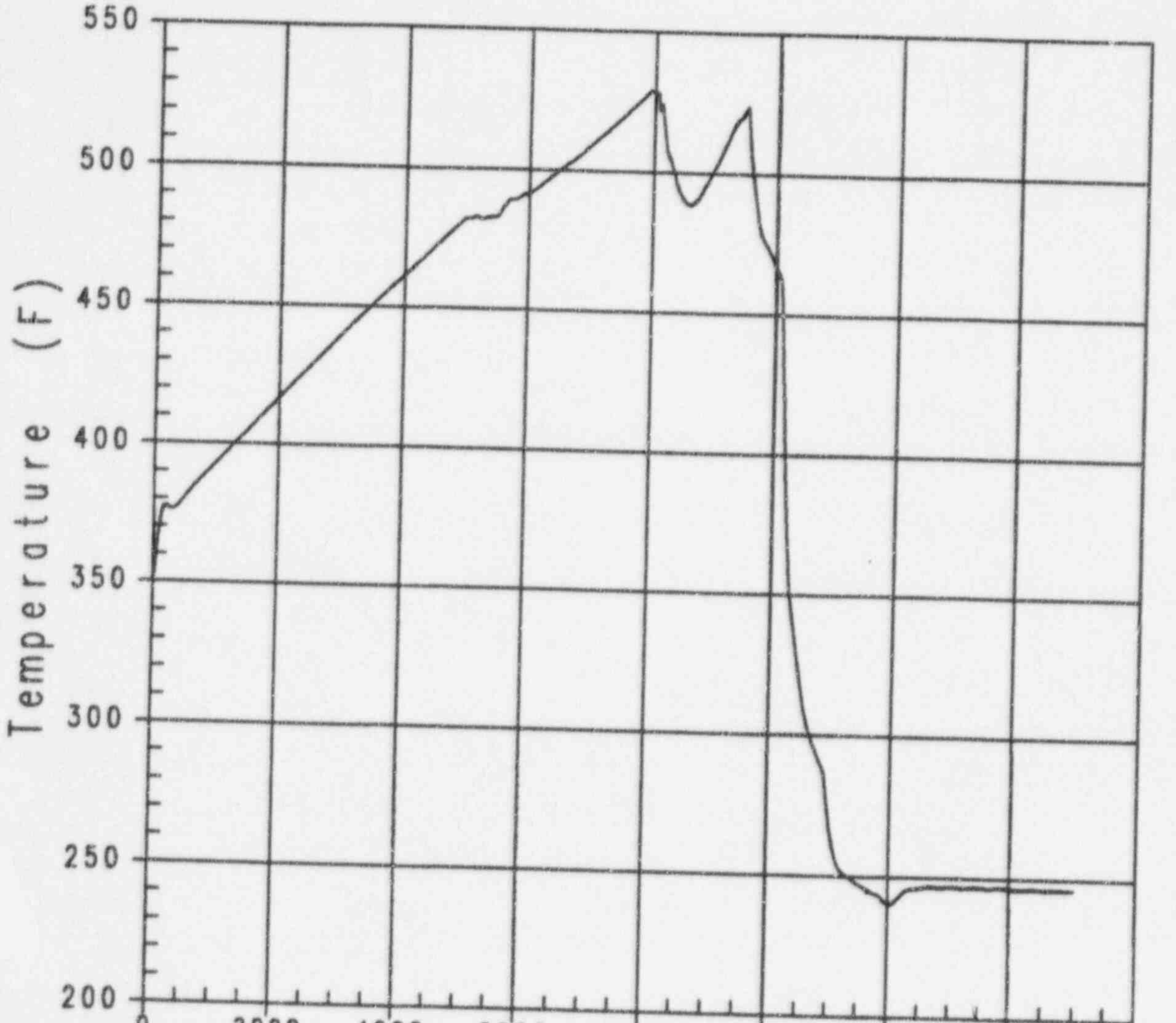


Figure 4.8-21 Core Outlet Fluid Temperature, Loss of RNS in Mode 4 with RCS Intact

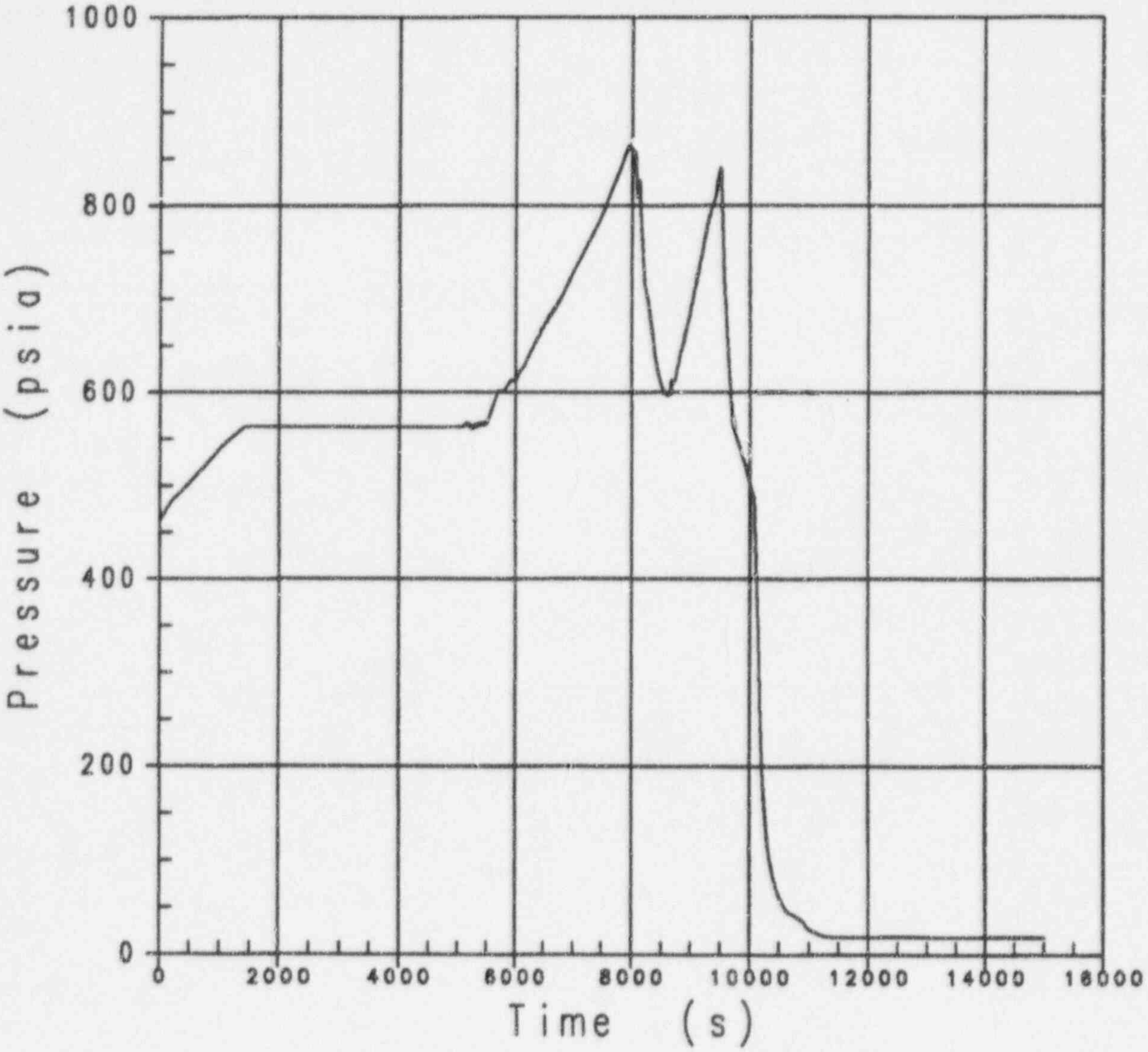


Figure 4.8-22 Pressurizer Pressure, Loss of RNS in Mode 4 with RCS Intact

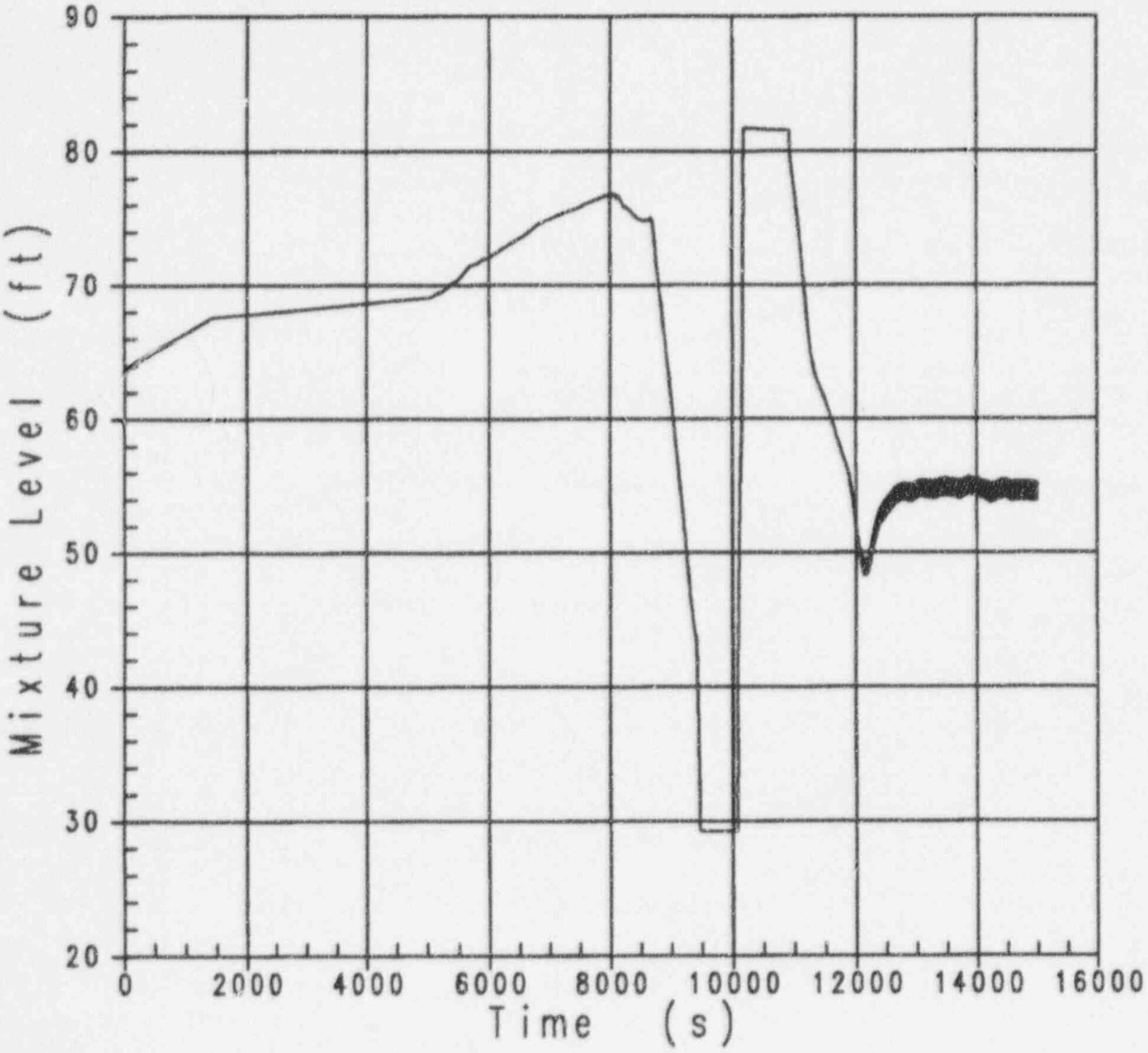


Figure 4.8-23 Pressurizer Mixture Level, Loss of F.NS in Mode 4 with RCS Intact

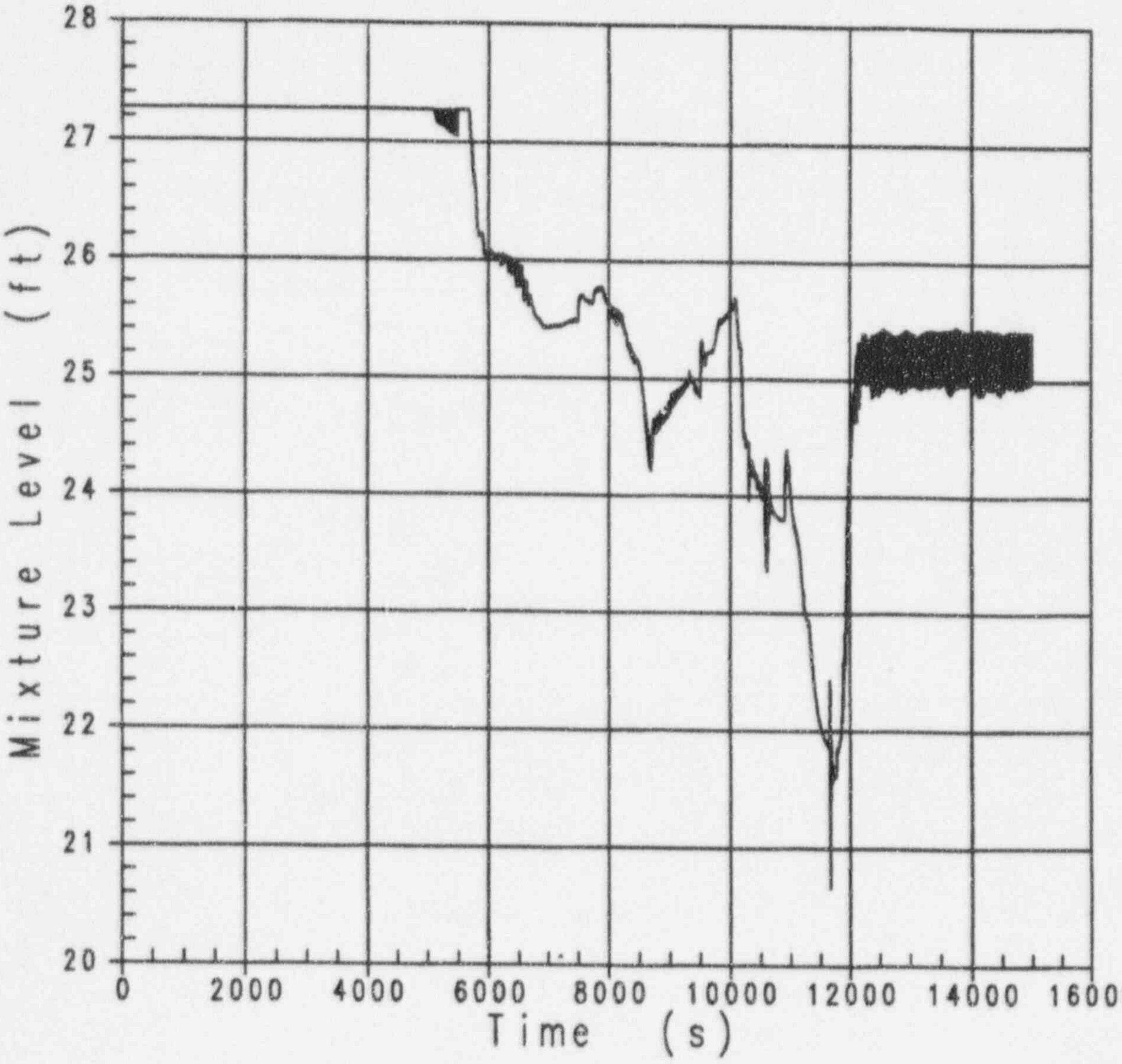


Figure 4.8-24 Core Stack Mixture Level, Loss of RNS in Mode 4 with RCS Intact

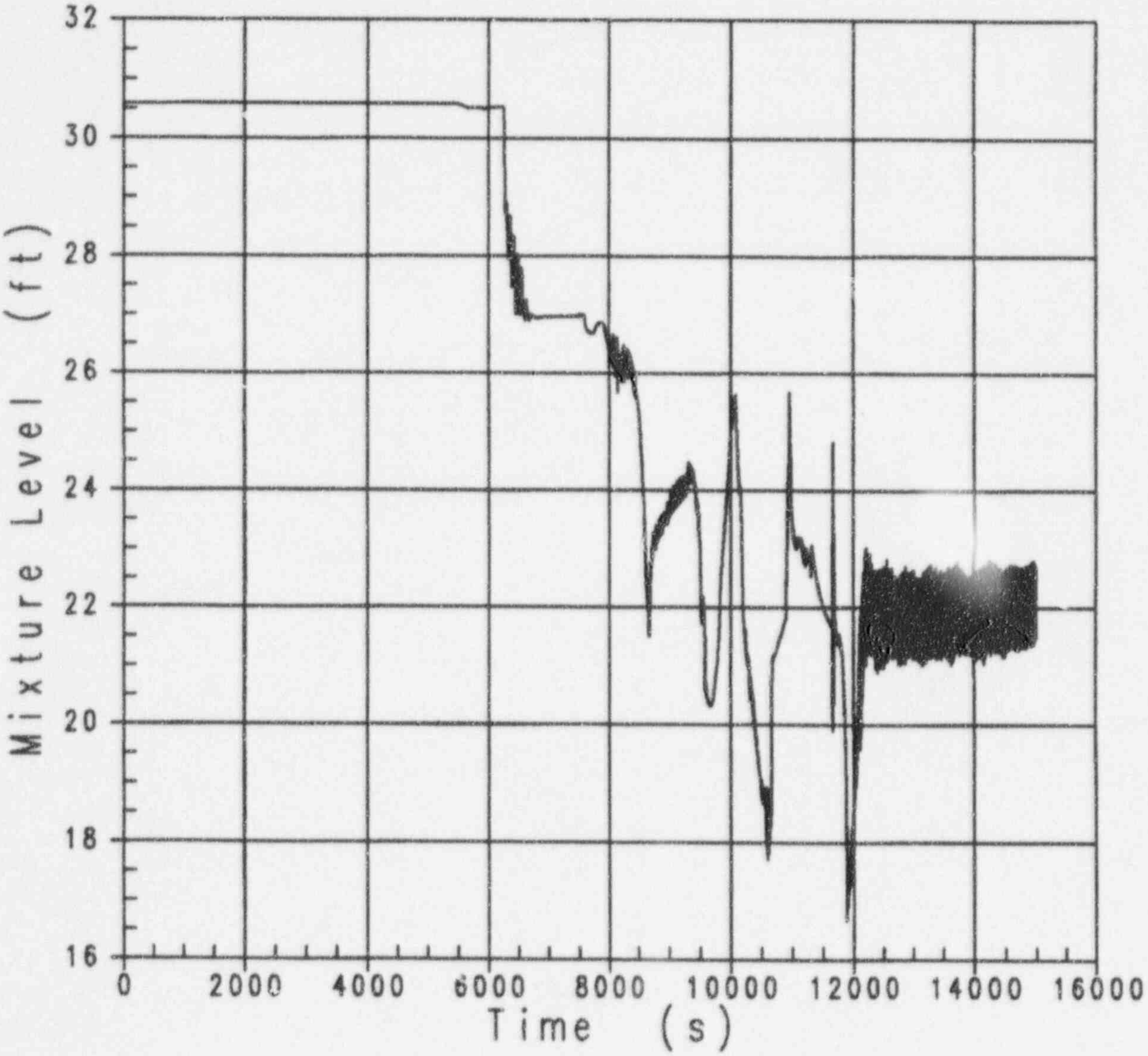


Figure 4.8-25 Downcomer Mixture Level, Loss of RNS in Mode 4 with RCS Intact

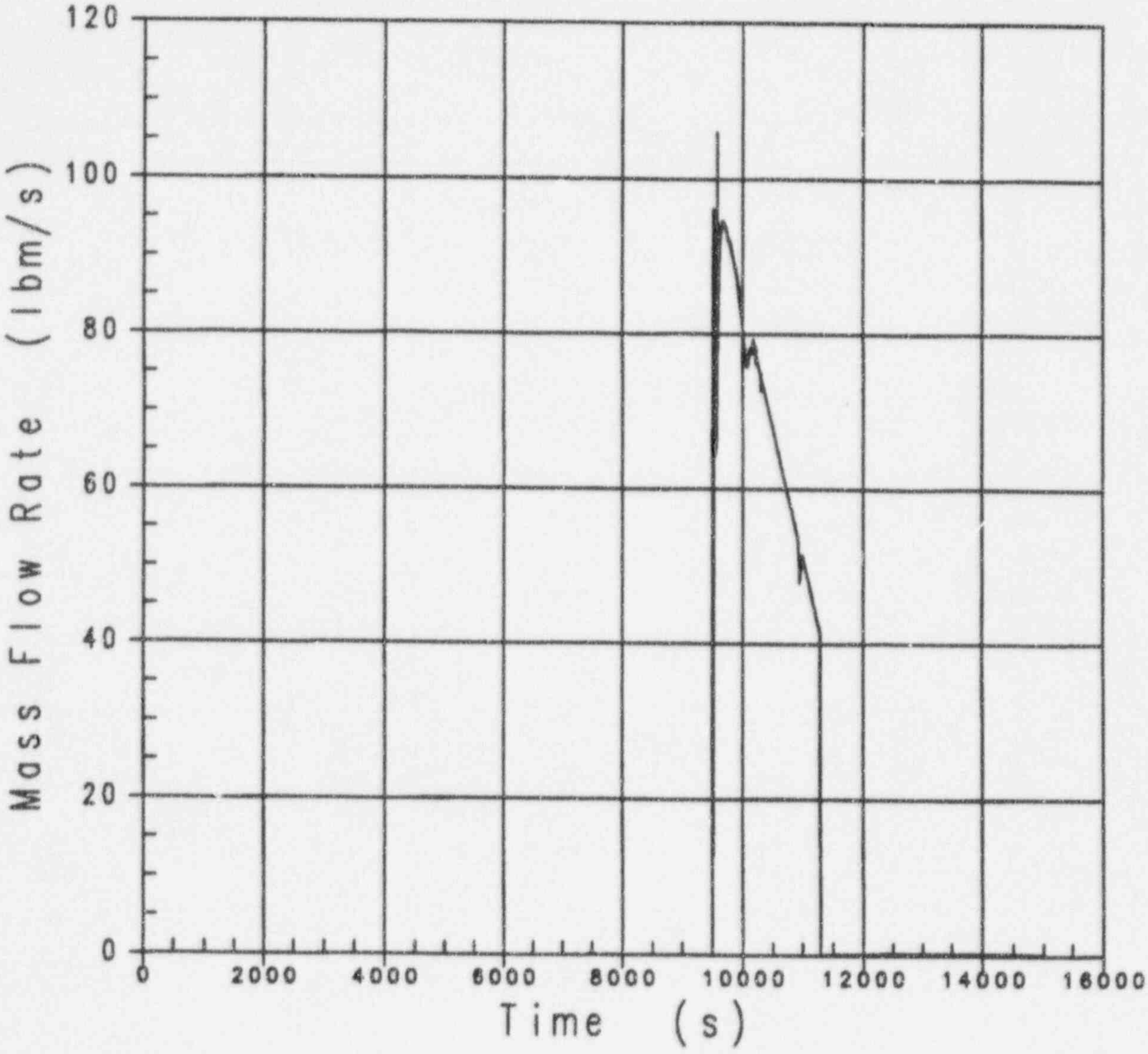


Figure 4.8-26 CMT to DVI Flow, Loss of RNS in Mode 4 with RCS Intact

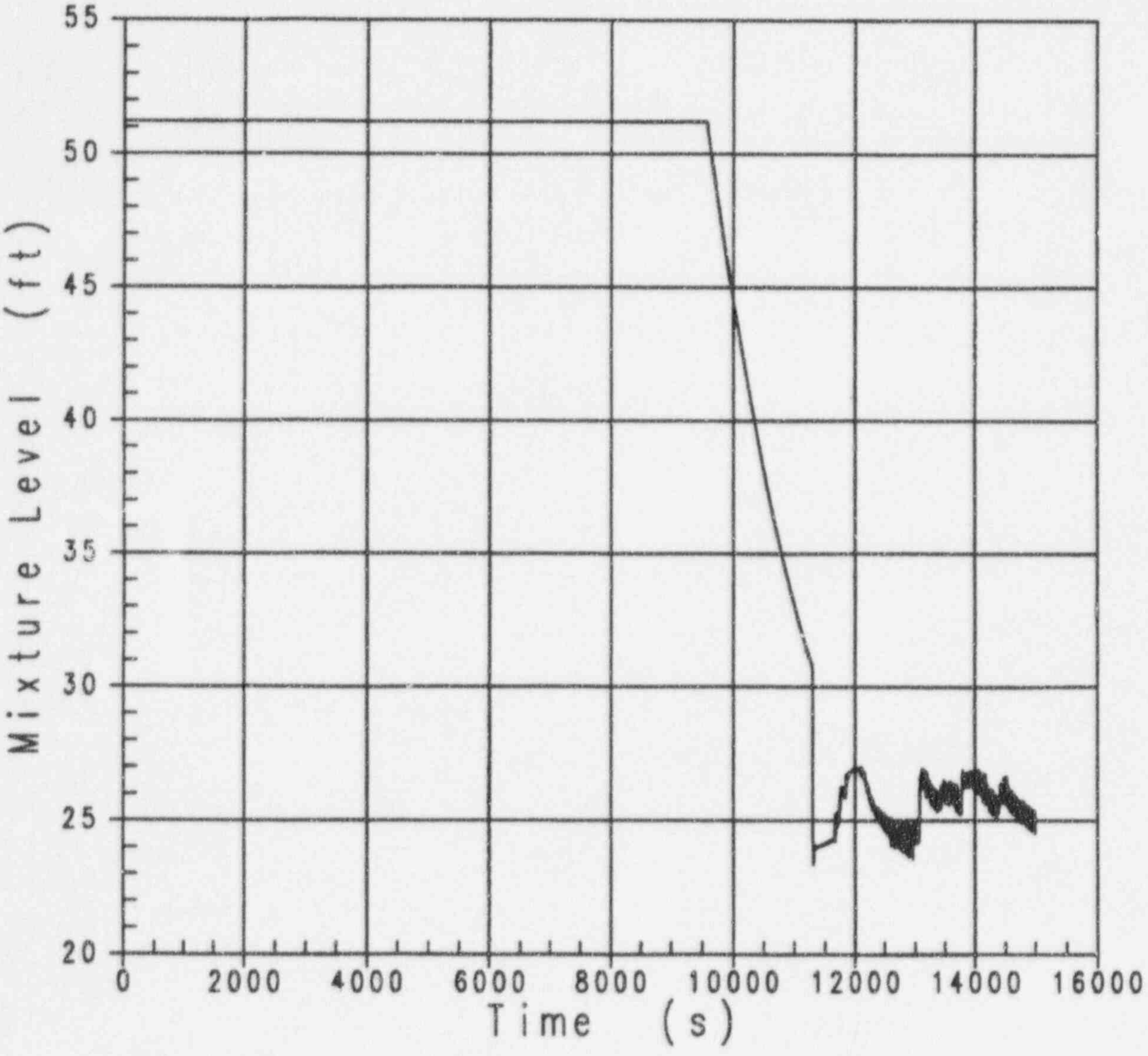


Figure 4.8-27 CMT Mixture Level, Loss of RNS in Mode 4 with RCS Intact

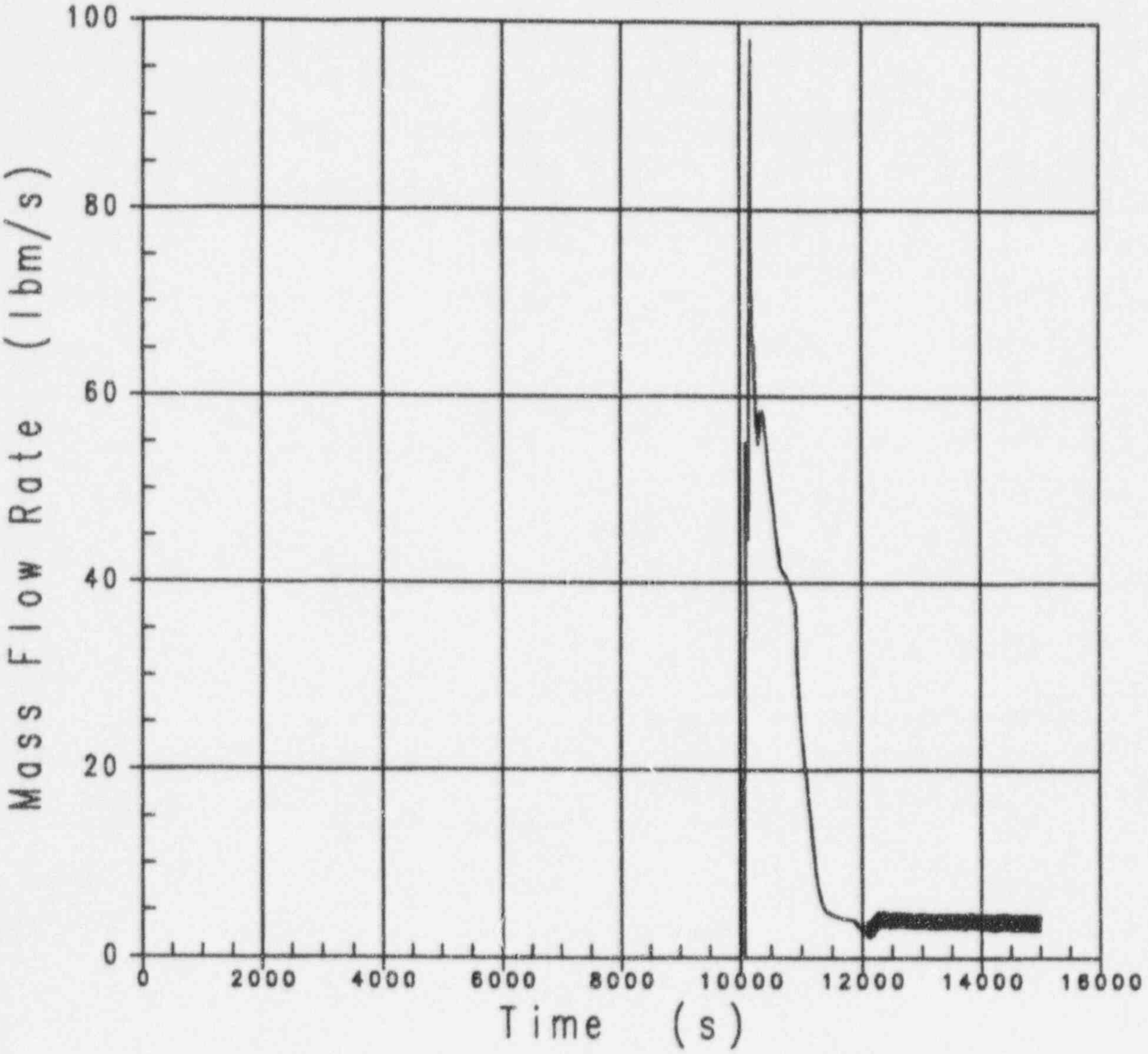


Figure 4.8-28 ADS Stages 1-3 Vapor Flow, Loss of RNS in Mode 4 with RCS Intact

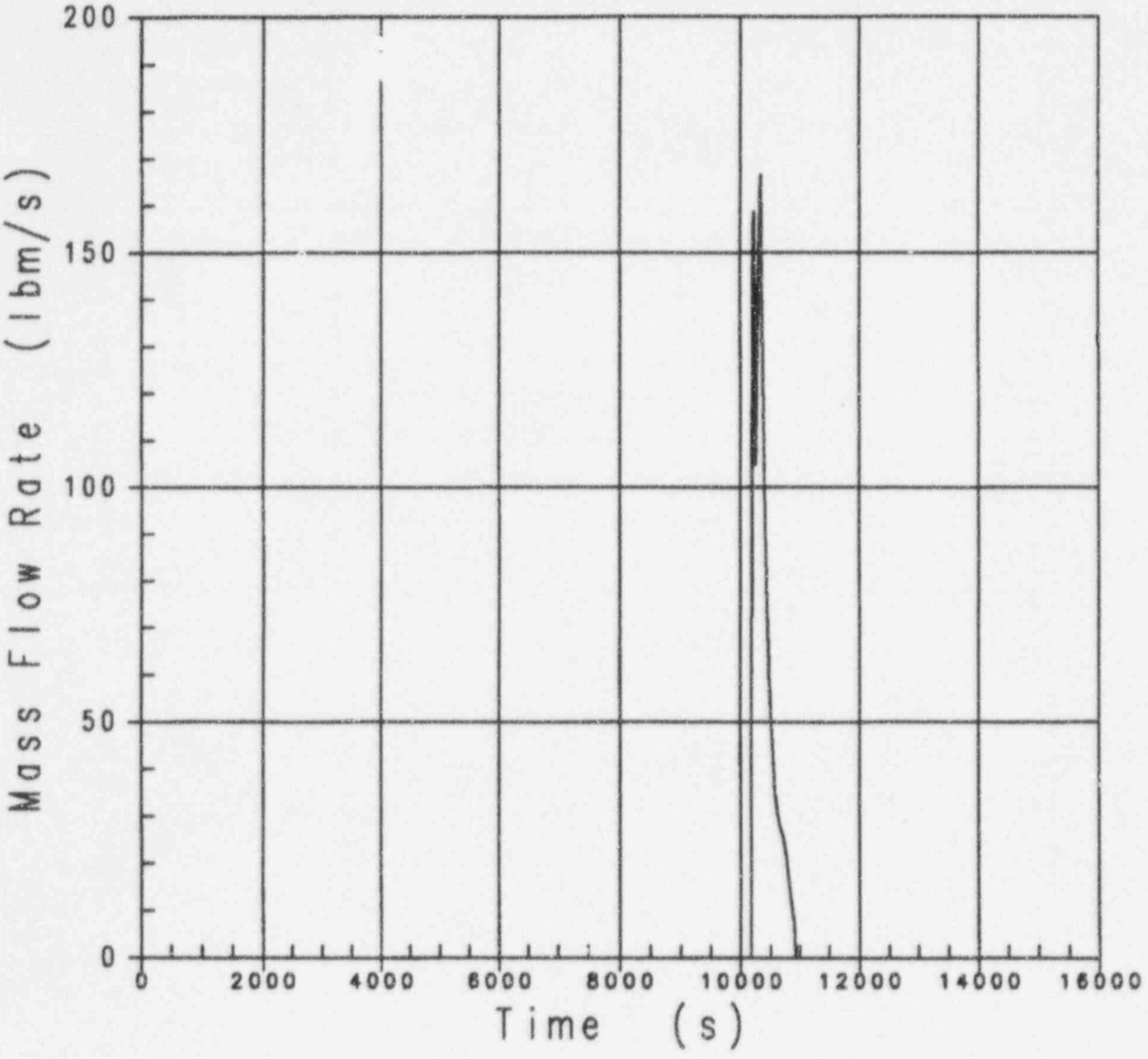


Figure 4.8-29 ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

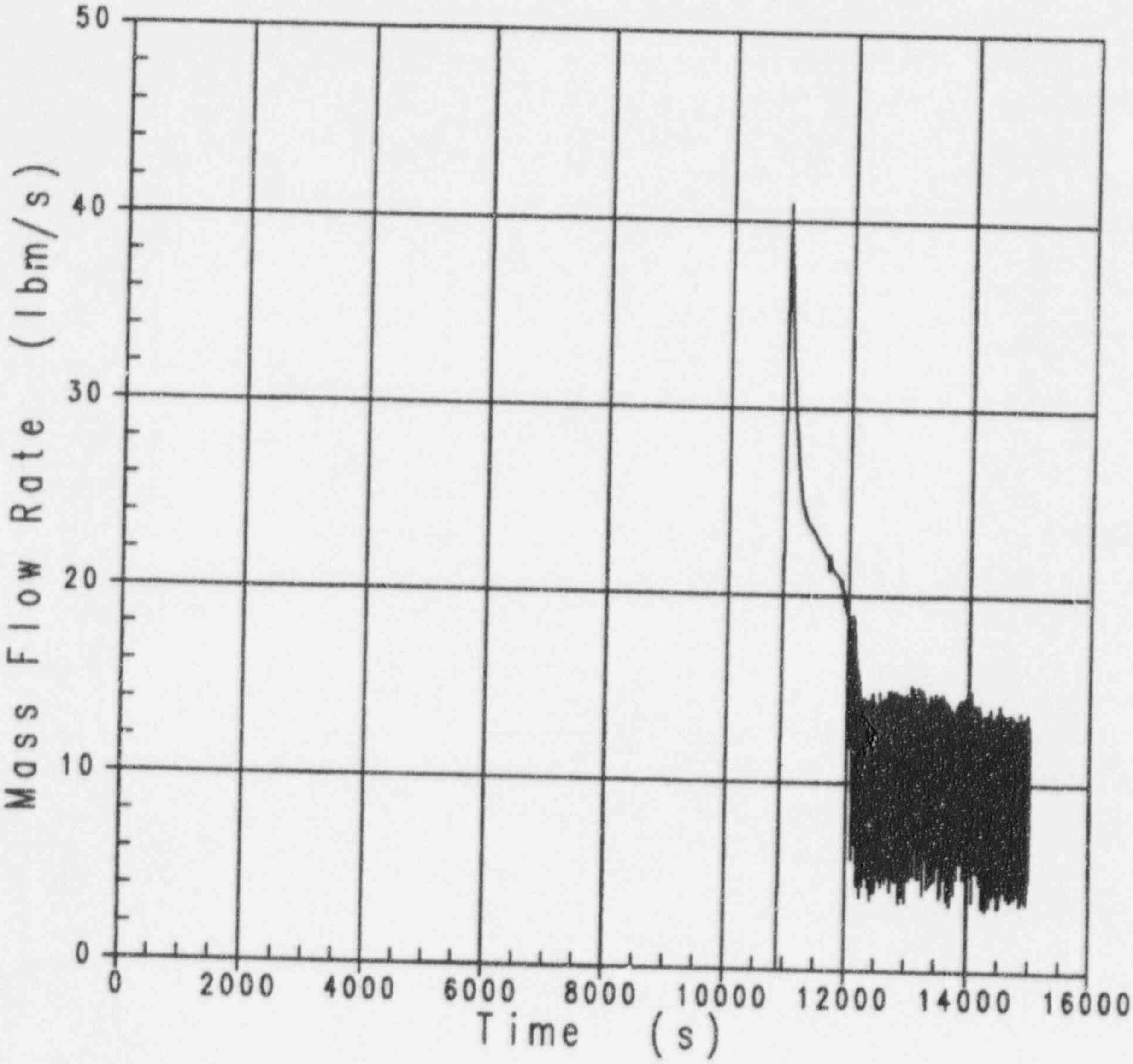


Figure 4.8-30 ADS Stage 4 Vapor Flow, Loss of RNS in Mode 4 with RCS Intact

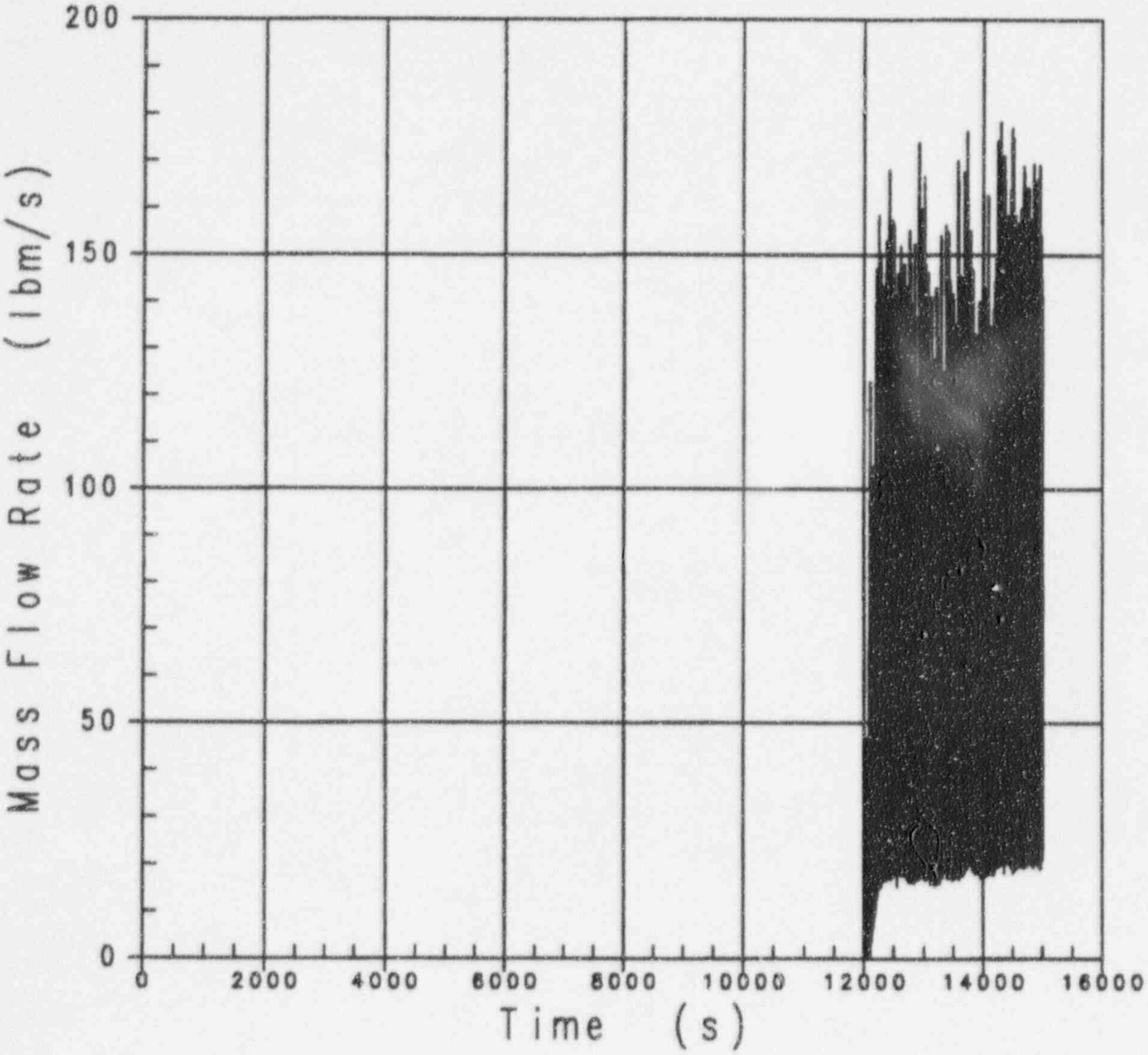


Figure 4.8-31 ADS Stage 4 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

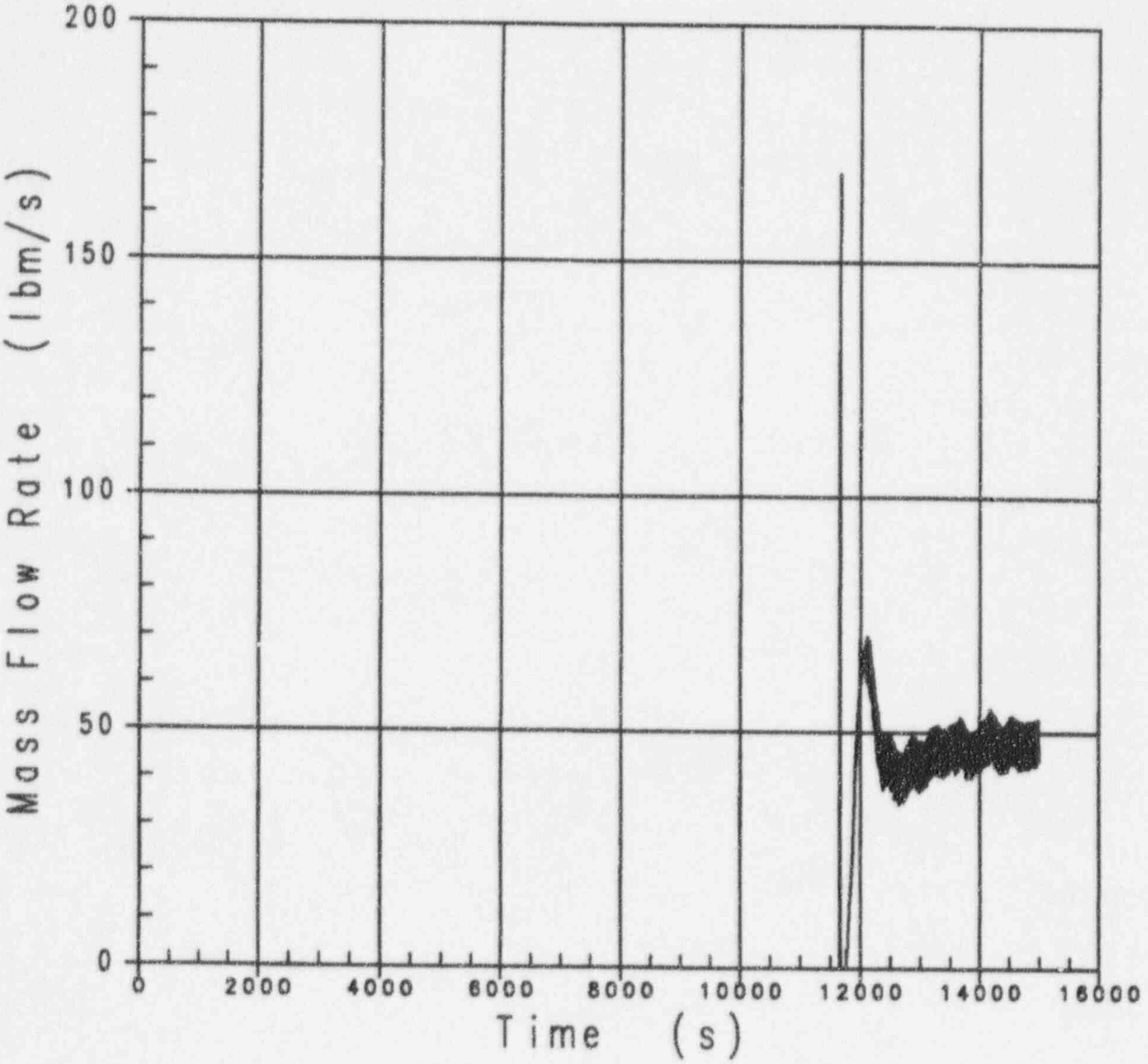


Figure 4.8-32 Loop 1 IRWST Injection Flow, Loss of RNS in Mode 4 with RCS Intact

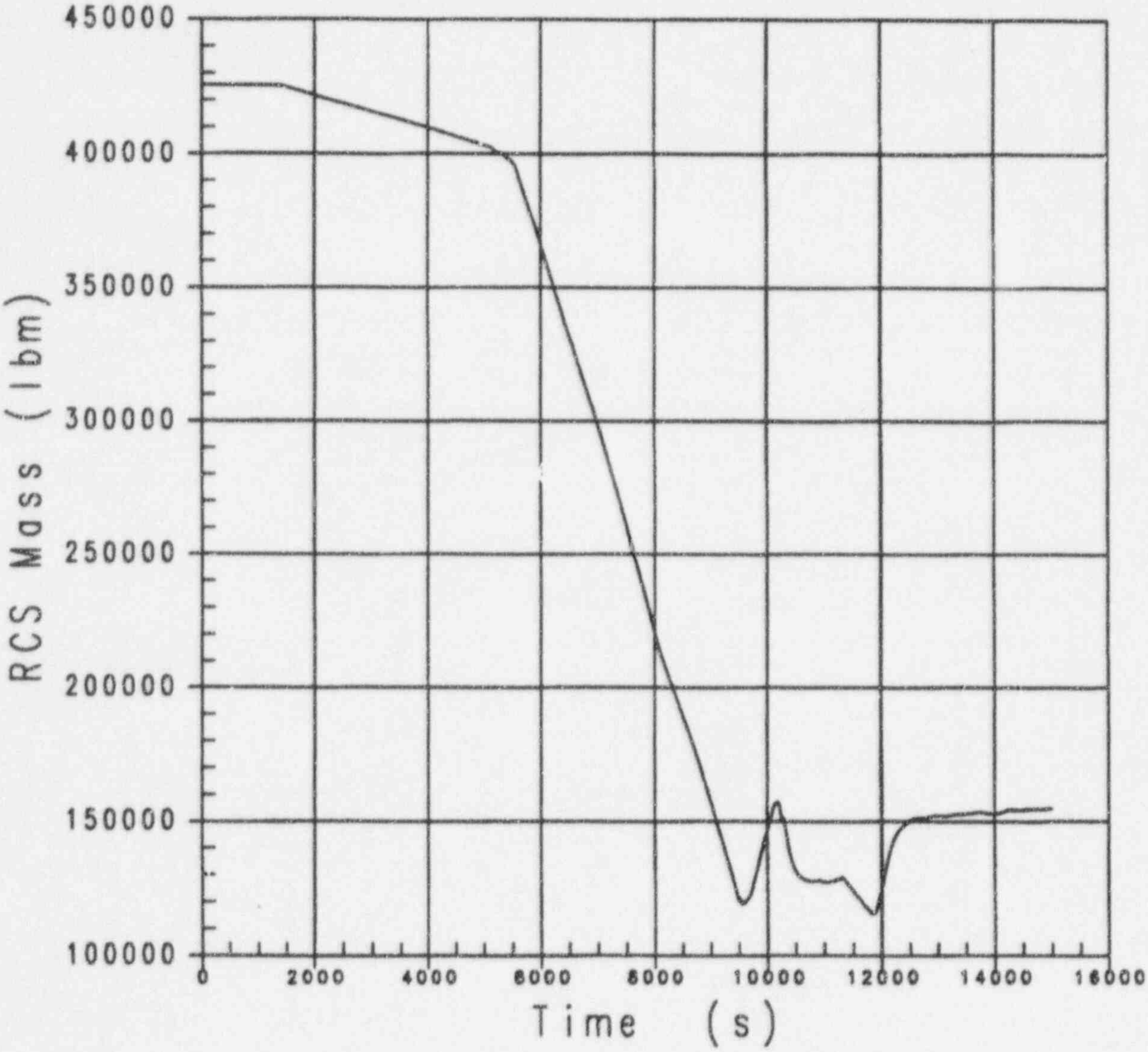


Figure 4.8-33 Primary Mass Inventory, Loss of RNS in Mode 4 with RCS Intact

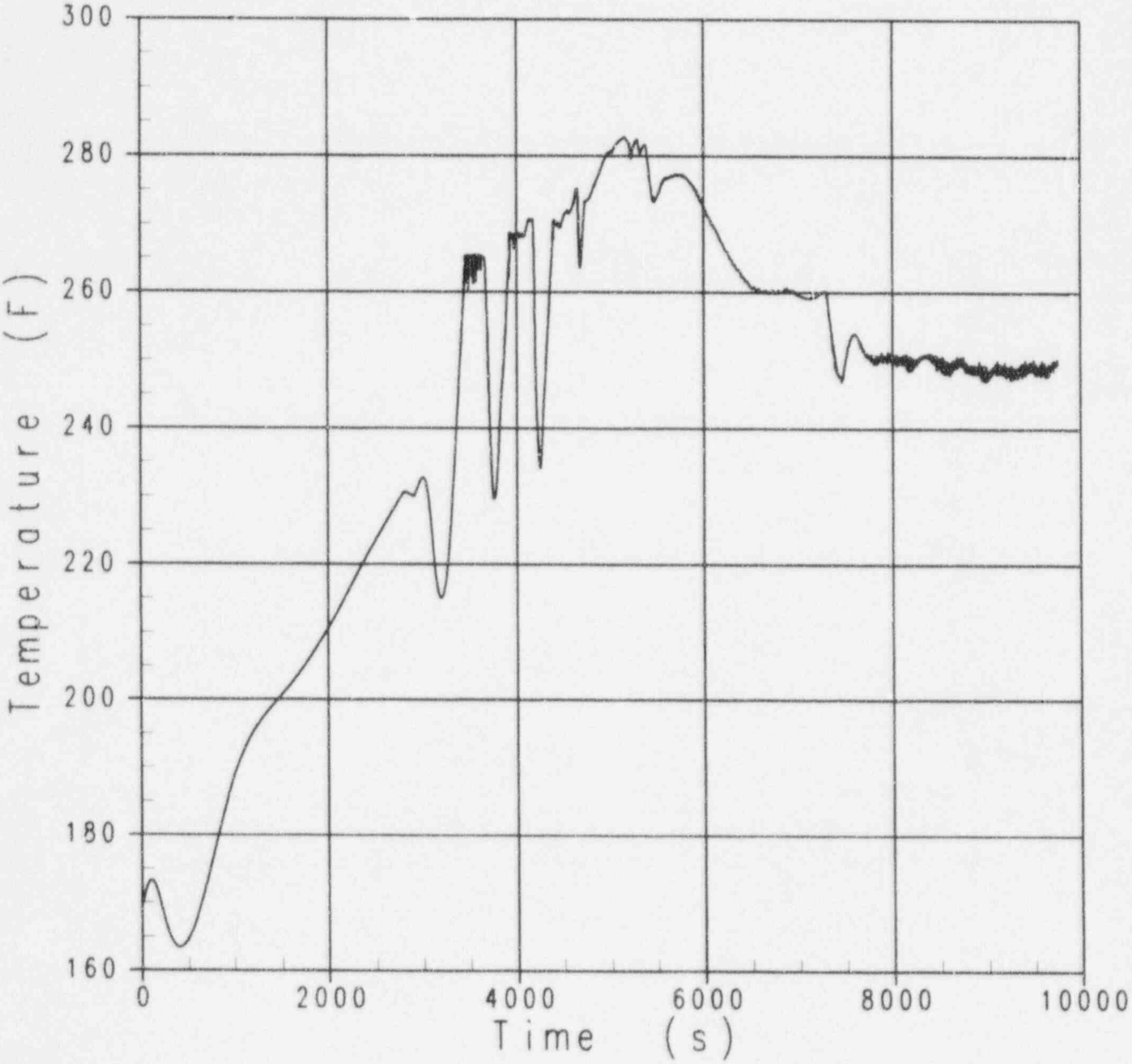


Figure 4.8-34 Core Outlet Fluid Temperature, Loss of RNS in Mode 5 with RCS Open

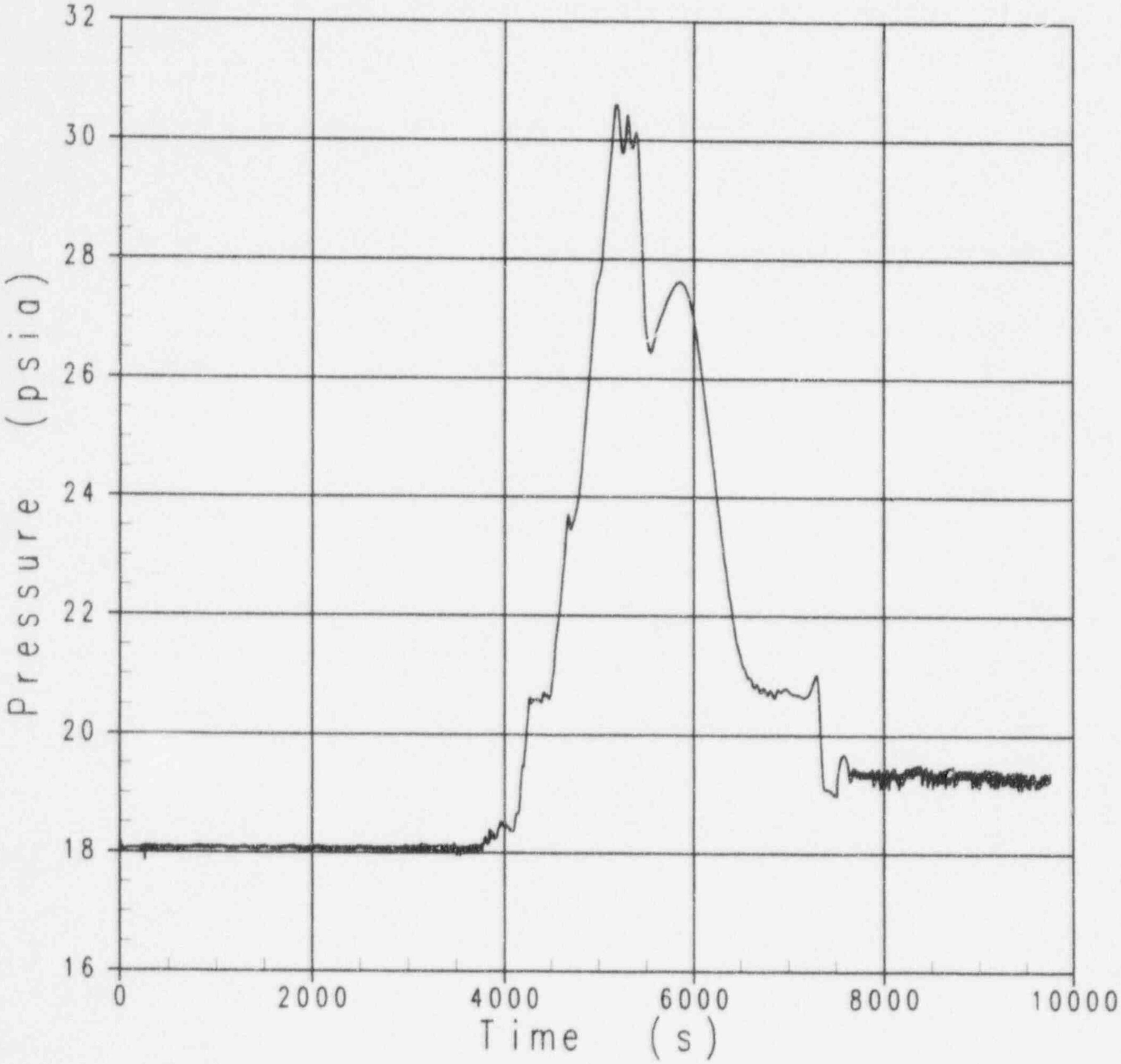


Figure 4.8-35 Pressurizer Pressure, Loss of RNS in Mode 5 with RCS Open

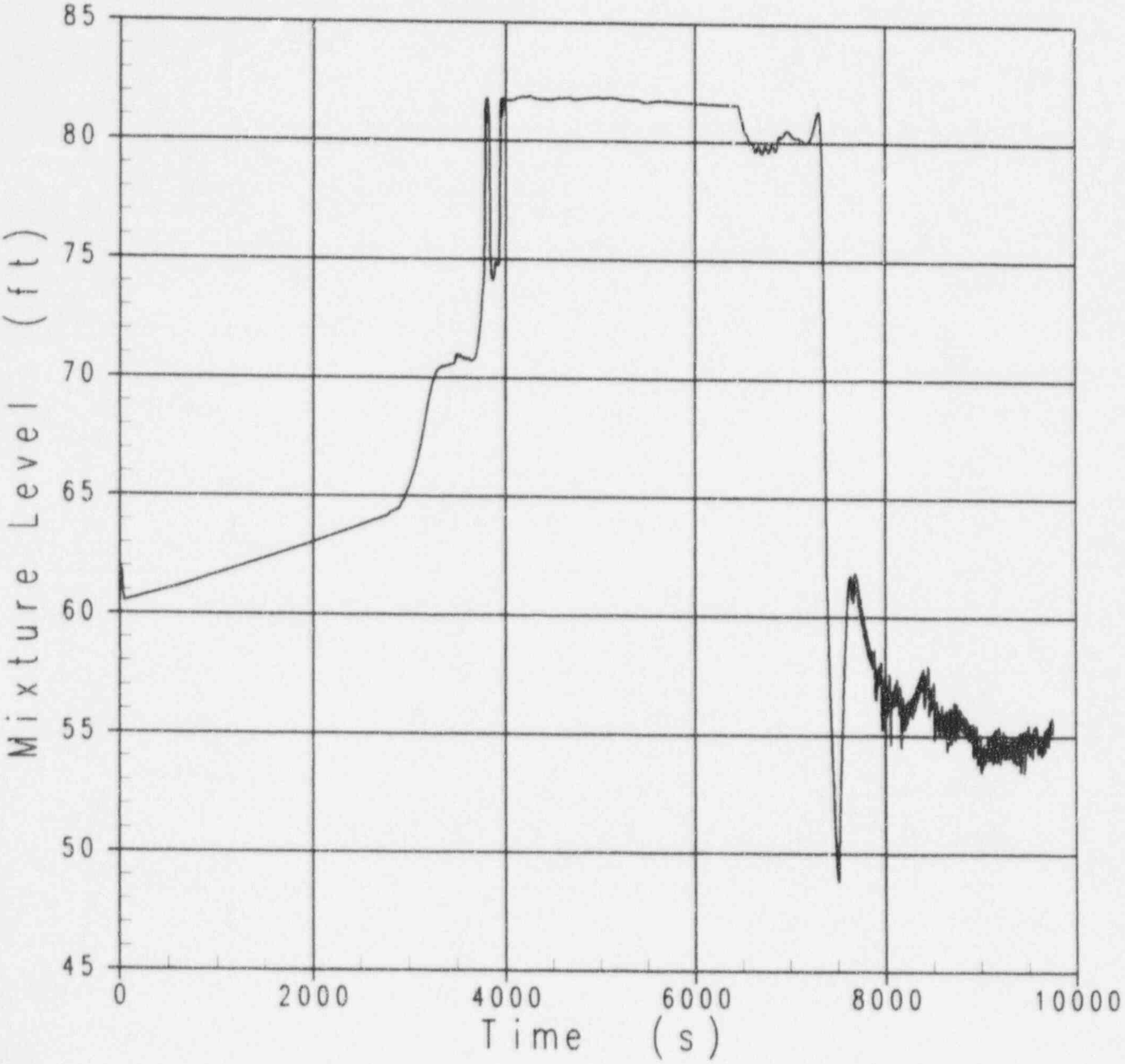


Figure 4.8-36 Pressurizer Mixture Level, Loss of RNS in Mode 5 with RCS Open

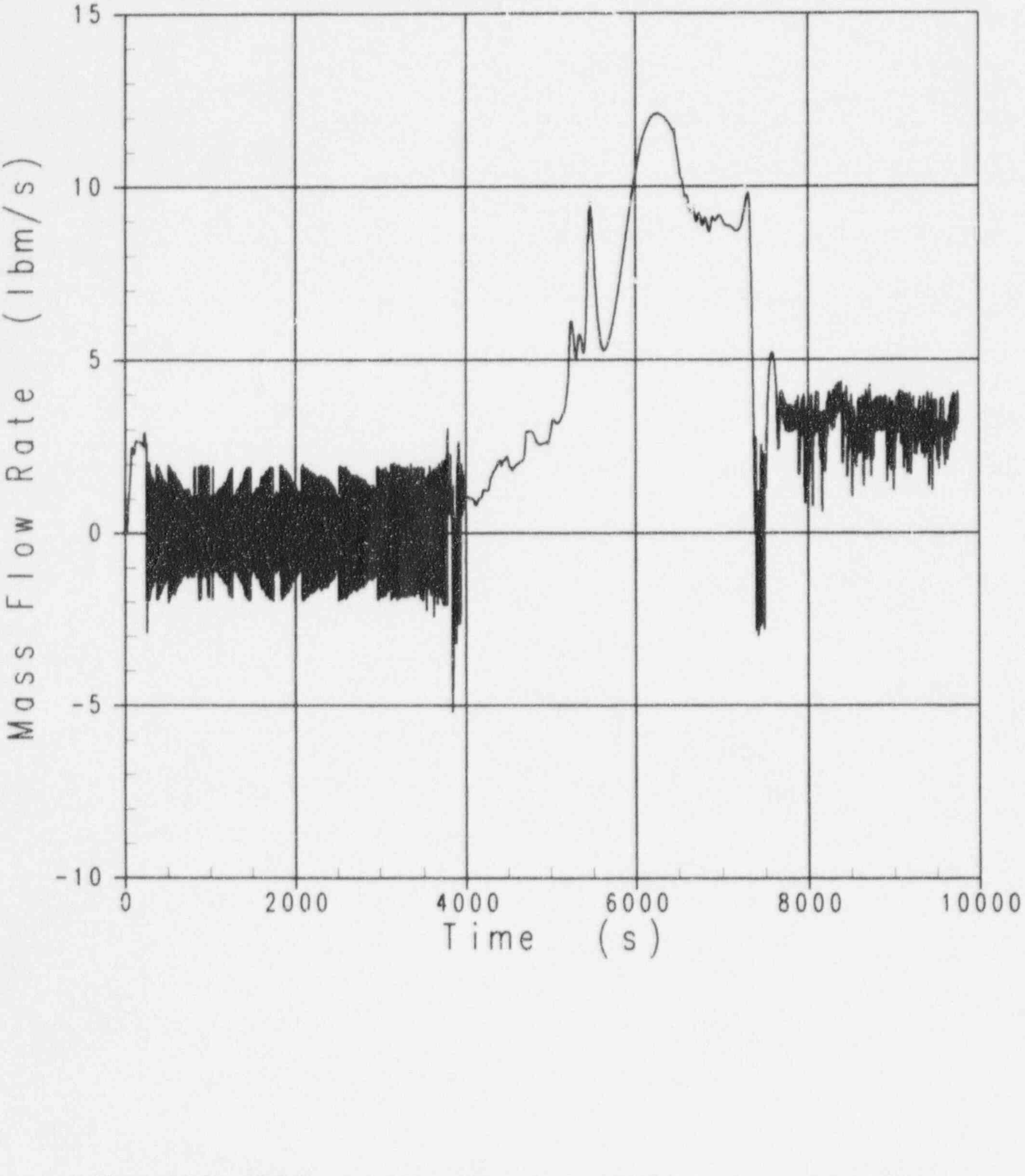


Figure 4.8-37 ADS Stages 1-3 Vapor Flow, Loss of RNS in Mode 5 with RCS Open

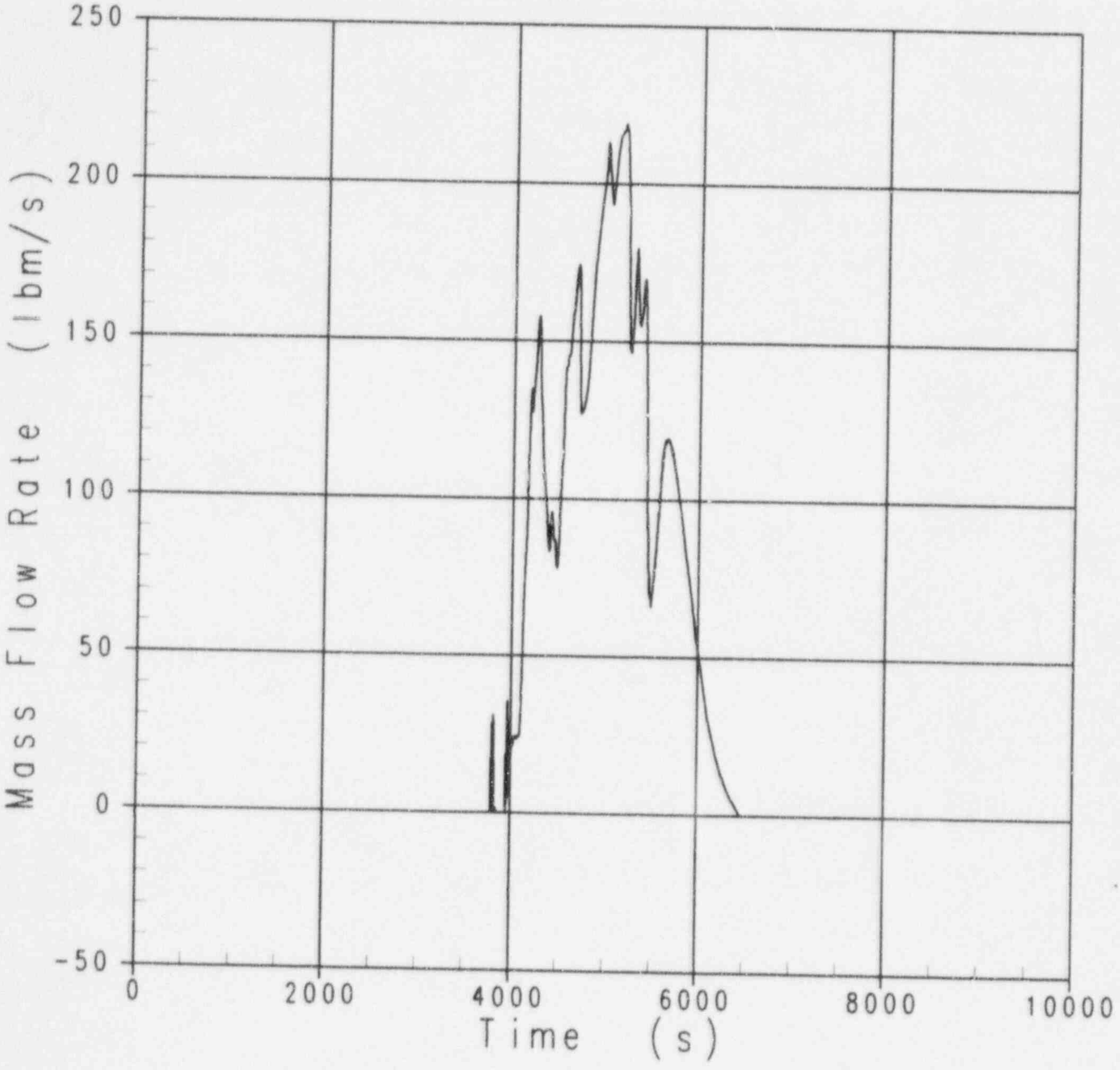


Figure 4.8-38 ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

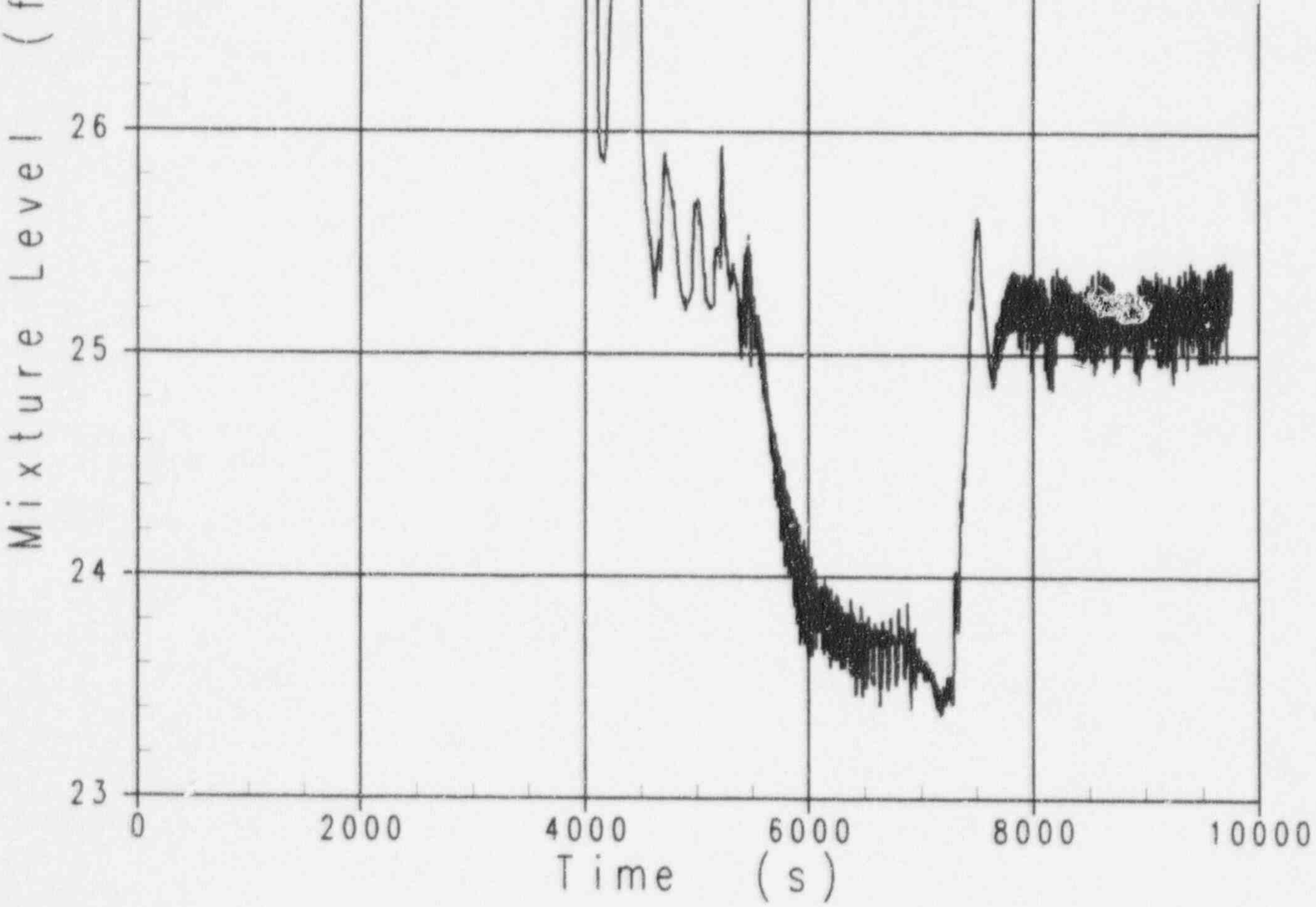


Figure 4.8-39 Core Stack Mixture Level, Loss of RNS in Mode 5 with RCS Open

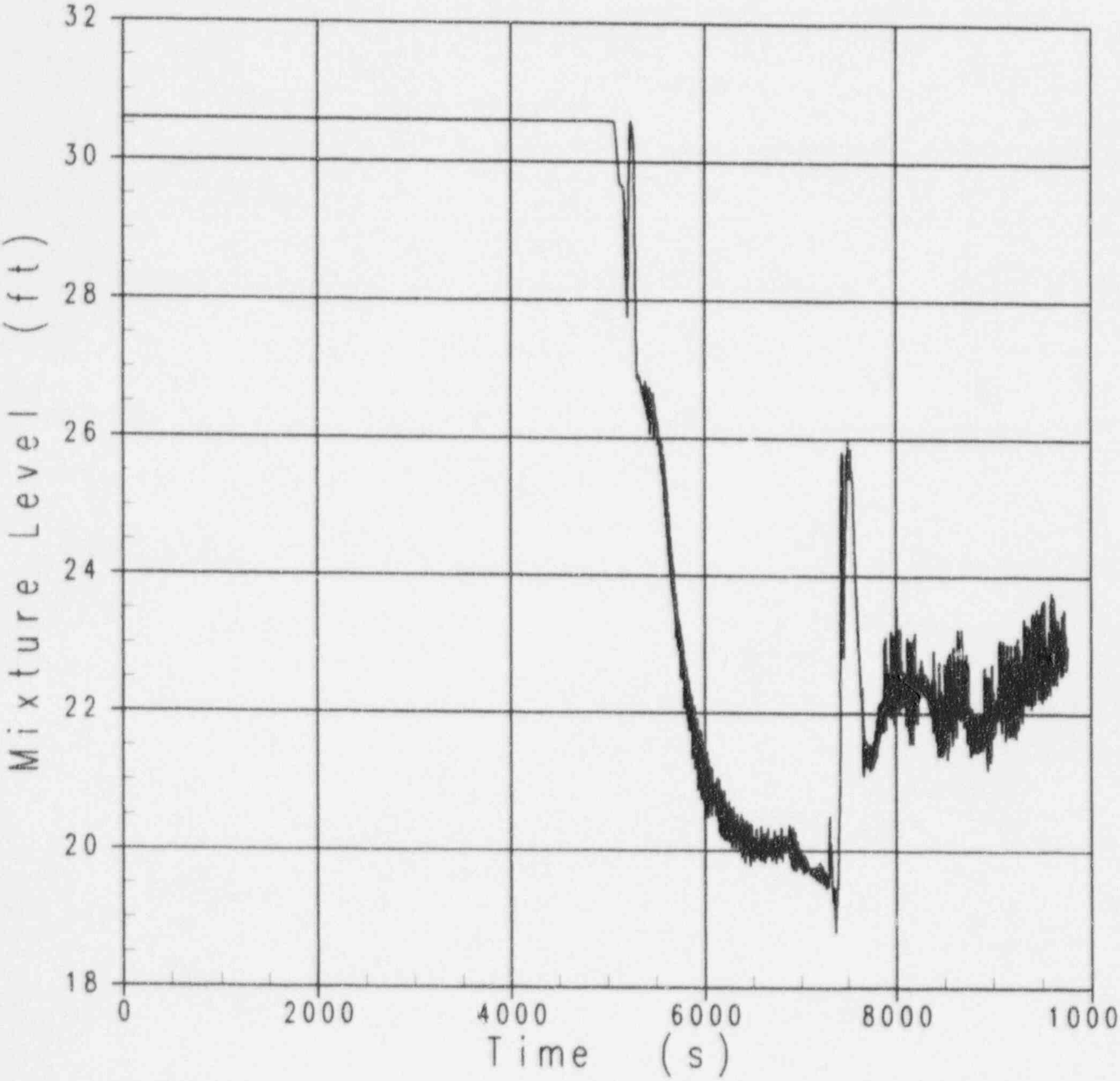


Figure 4.8-40 Downcomer Mixture Level, Loss of RNS in Mode 5 with RCS Open

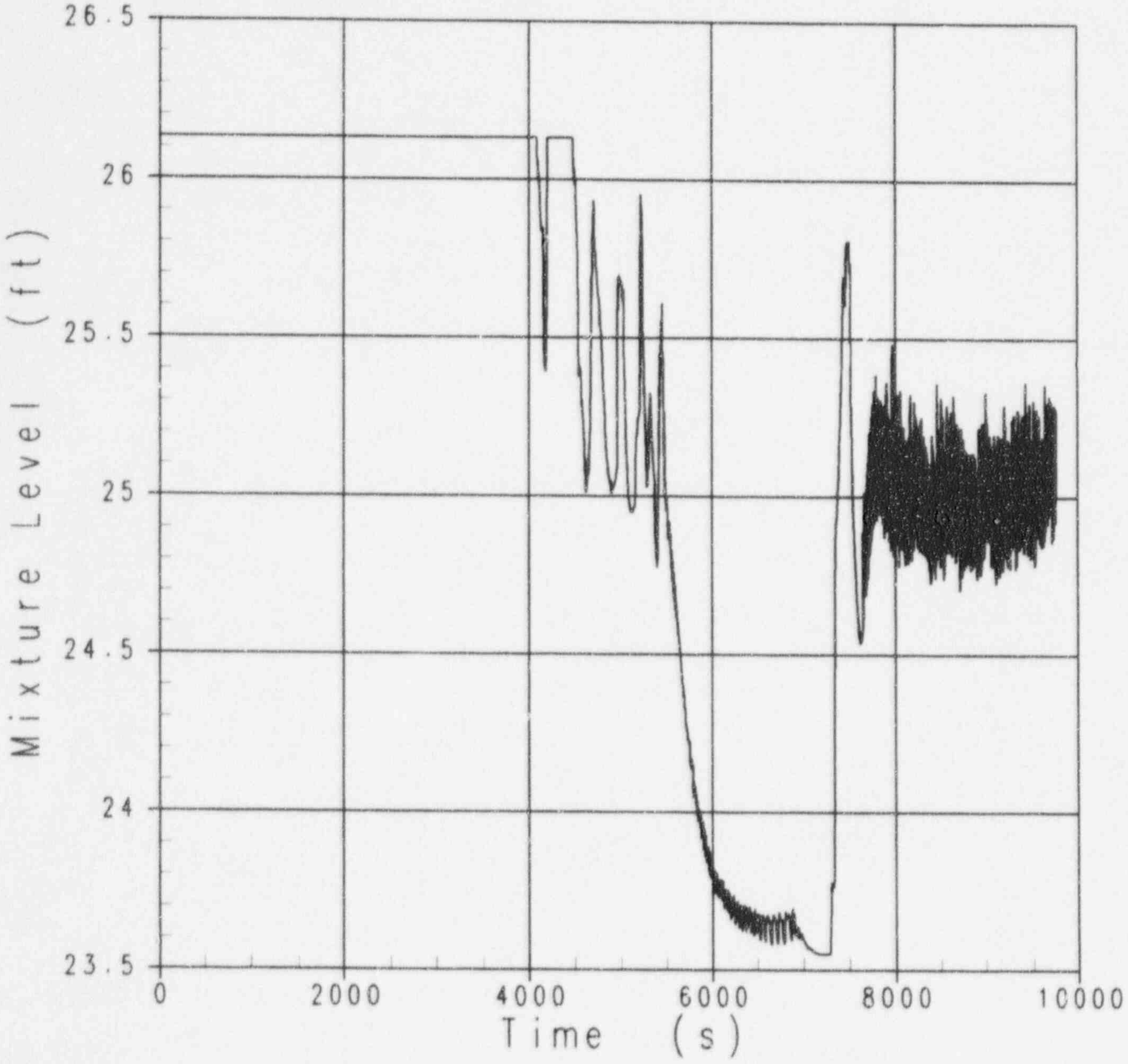


Figure 4.8-41 Loop 1 Hot Leg Mixture Level, Loss of RNS in Mode 5 with RCS Open

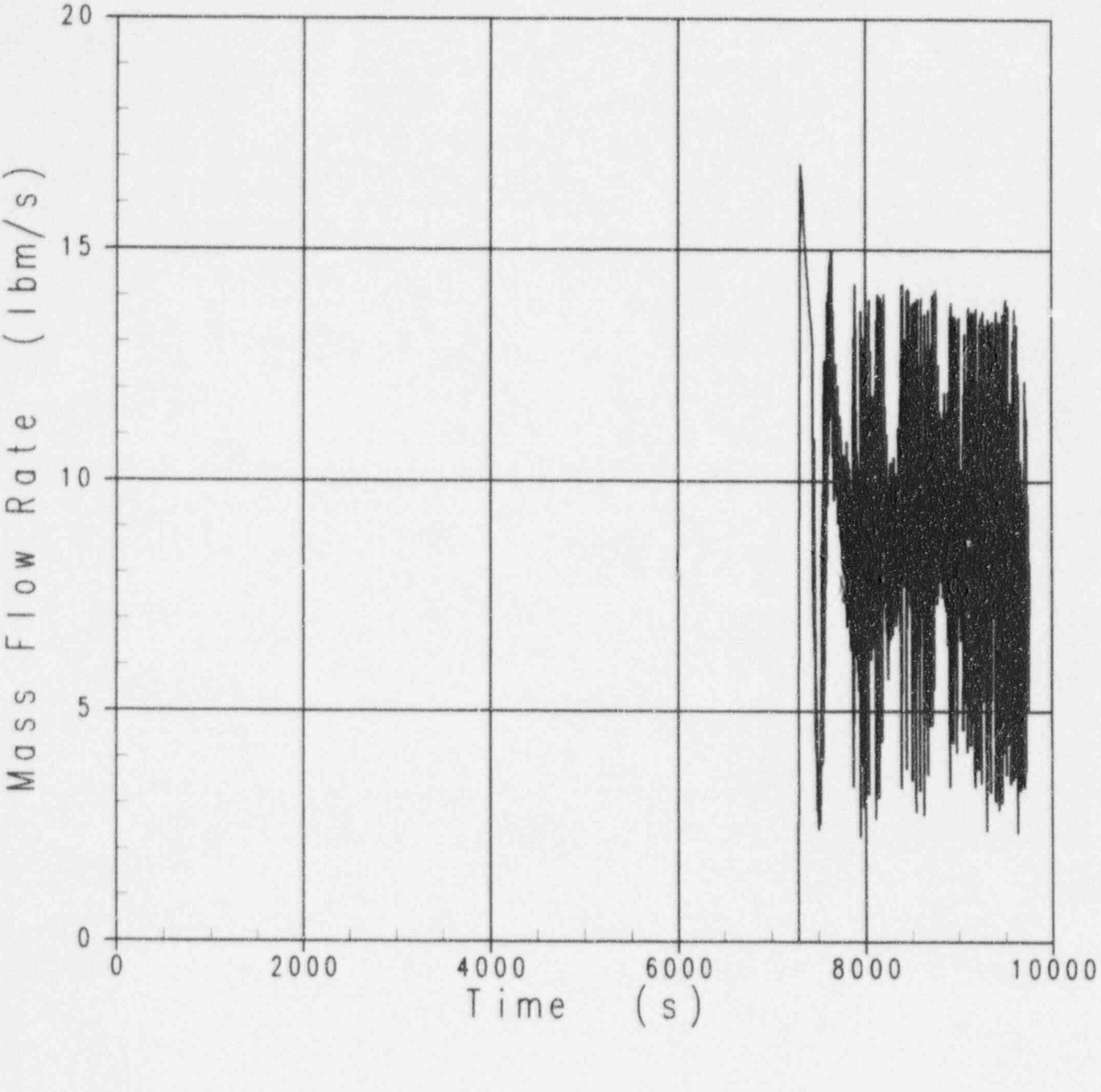


Figure 4.8-42 ADS Stage 4 Vapor Flow, Loss of RNS in Mode 5 with RCS Open

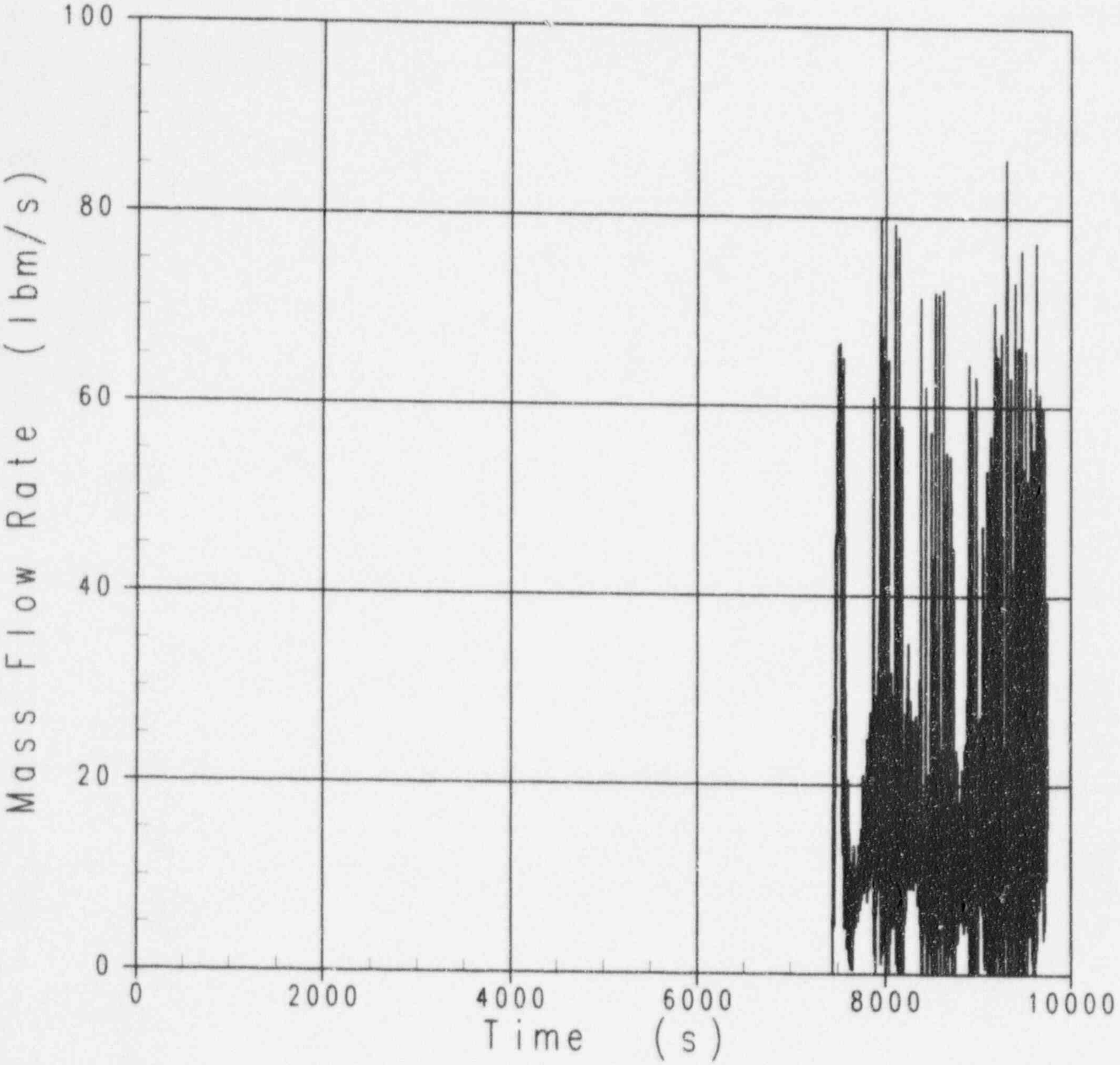


Figure 4.8-43 ADS Stage 4 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

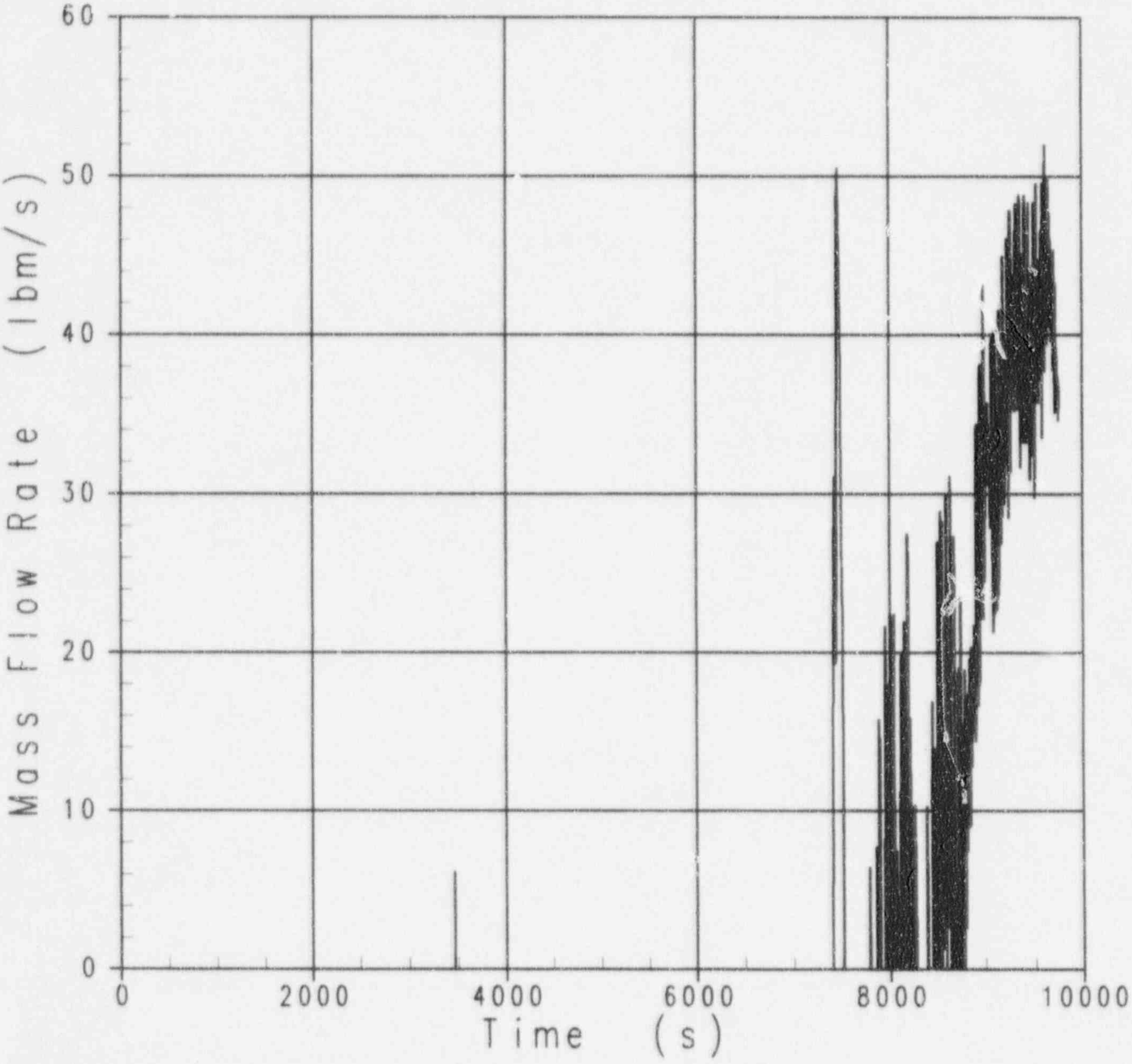


Figure 4.8-44 IRWST Injection Flow, Loss of RNS in Mode 5 with RCS Open

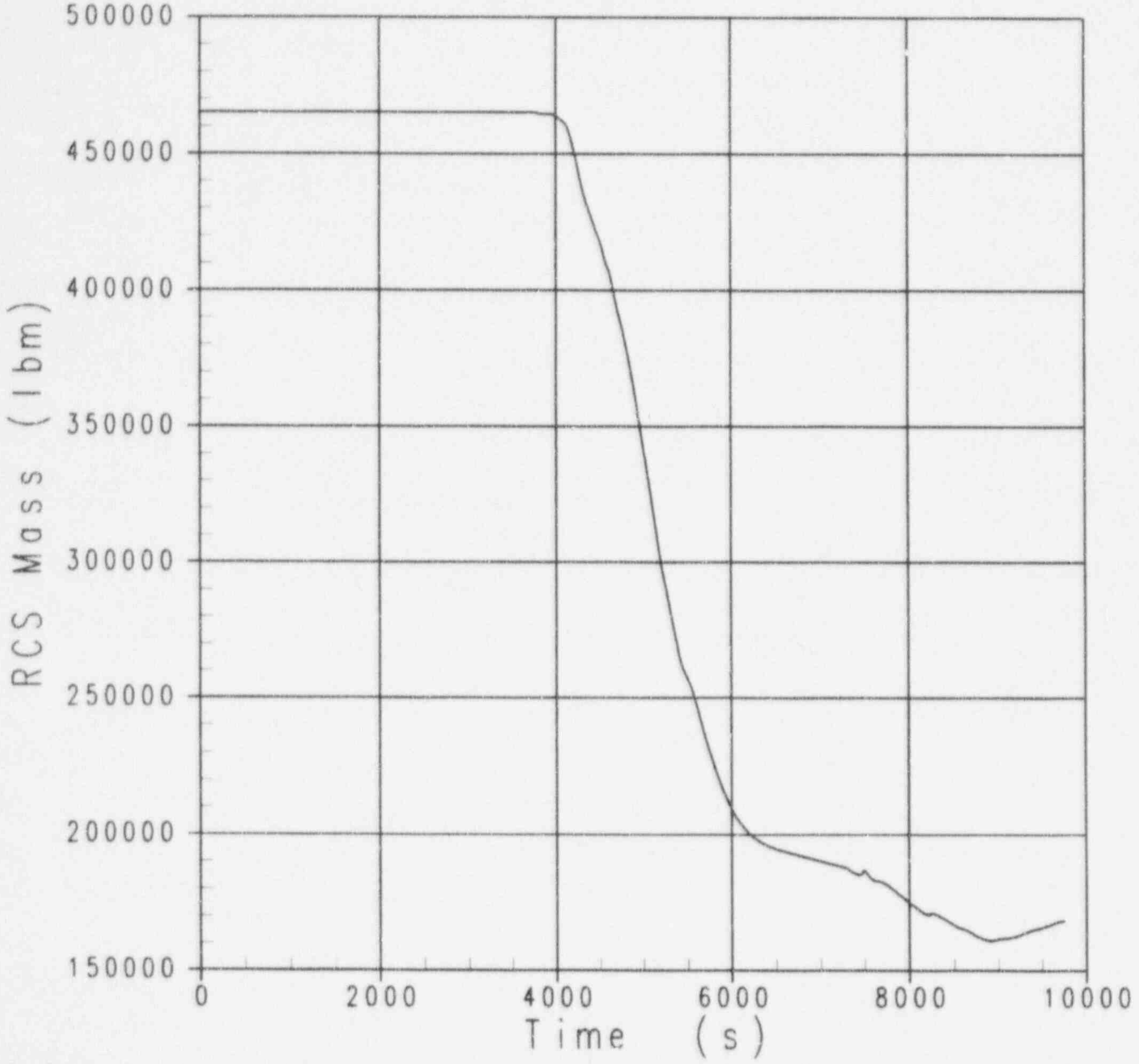


Figure 4.8-45 Primary Mass Inventory, Loss of RNS in Mode 5 with RCS Open

4.8.6 References

4.8-1 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.8-2 WCAP-14206, *Applicability of the NOTRUMP Computer Code to AP600 SSAR Small-Break LOCA Analyses*, November 1994.

4.8-3 WCAP-14601, *AP600 Accident Analyses, Evaluation Models*, March 21, 1996.

4.8-4 Hochreiter, L. E., Kemper, R. M., Bajorek, S. M., and Zhang, J., WCAP-14171, Revision 1, *WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident*, October 1996.

4.8-5 Title 10, Code of Federal Regulations, Part 50, Appendix K, "ECCS Evaluation Models," January 1, 1996.

4.8-6 Title 10, Code of Federal Regulations, Part 50, (10 CFR 50.56), January 1, 1996.

4.9 RADIOLOGICAL CONSEQUENCES (SSAR SECTION 15.7 AND APPENDIX 15A)

This section presents evaluations that confirm that all radioactive material release from the AP600 events postulated to be initiated in a shutdown mode have acceptable consequences.

- The Standard Review Plan (Reference 4.9-1) no longer includes the atmospheric releases from radioactive gas waste system failure and radioactive liquid waste system leak or failure events as part of the review. As discussed in SSAR subsections 15.7.1 and 15.7.2 (Reference 4.9-2), no analysis for these events is provided in the SSAR.

- Release of radioactivity to the environment due to a liquid tank failure is addressed in SSAR subsection 15.7.3 and is not mode dependent.

- The fuel handling accident described in SSAR subsection 15.7.4, while not mode dependent, is analyzed in the applicable and bounding mode and accounts for spent fuel pool boiling. This accident analysis will bound radioactivity releases from other SSAR chapter 15 events during low power and shutdown operations. The LOCA analysis results show PCT remains below 2200°F, and there are no fuel cladding failures.

- The spent fuel cask drop accident described in SSAR subsection 15.7.5 is not mode dependent.

- SSAR appendix 15A contains the evaluation models and parameters that form the basis of the radiological consequences analyses for the various postulated accidents. This methodology applies in all modes of operation.

In summary, there are no shutdown risks associated with the radiological consequences methodology or parameters, or the postulated or applicable events, which need to be considered outside the scope of what is already analyzed for AP600 SSAR section 15.7.

4.9.1 References

4.9-1 NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Revision 1, July 1981.

4.9-2 *AP600 Standard Safety Analysis Report*, Chapter 15, "Accident Analysis."

4.10 OTHER EVALUATIONS AND ANALYSES

4.10.1 Low Temperature Overpressure Protection

For the AP600, the normal residual heat removal system (RNS) suction relief valve is located immediately downstream of the RCS suction isolation valves. This relief valve protects the RNS from overpressurization and provides low temperature overpressure protection (LTOP) for the RCS components when the RNS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. The RNS relief valve is sized to ensure LTOP by limiting the RCS and RNS pressure to less than the 10 CFR 50 Appendix G (Reference 4.10-1) steady-state pressure limit of 621 psig (flange requirement).

For adequate sizing of the RNS relief valve, Westinghouse LTOP analyses consider the limiting mass-injection and energy- or heat-injection events. The RNS relief capacity must be greater than the design basis mass injection flow rate, which corresponds to a maximum makeup flow rate, assuming both CVS makeup pumps are operating. The RNS relief valve must accommodate the RCS fluid expansion resulting from the design basis heat injection event. This event is due to restarting one RCP in one loop, assuming a temperature asymmetry as large as 50°F between the steam generator and the RCS.

The NRC provided request for additional information (RAI) 440.78, which refers to SSAR subsection 5.2.2.1 (Reference 4.10-2). The LTOP analysis is discussed in more detail in the response to RAI 440.78 (Reference 4.10-3), which resolved NRC concerns related to the *Draft Safety Evaluation Report* (Reference 4.10-4) open item 5.2.2.2-1 (item 887 in the open item tracking system [OITS]).

The AP600 Technical Specifications (Reference 4.10-5) bases 3.4.15 for the LTOP system also refer to SSAR subsection 5.2.2. Those bases explain that in Modes 1, 2, and 3, and in Mode 4 when the RNS is isolated from the RCS, the pressurizer safety valves will prevent RCS pressure from exceeding the 10 CFR 50 Appendix G limits. Overpressure protection is provided by the RNS suction relief valve in Modes 4 and 5, when the RNS is aligned and open to the RCS and RCS temperature is less than or equal to 350°F, and in Mode 6 when the reactor vessel head is off.

This discussion addresses overpressure protection associated with NUREG-1449 (Reference 4.10-6) low-power and shutdown operations concerns, inherently addressed in the LTOP analyses used to design and size the RNS relief valve, based on ability to mitigate the consequences of design basis cold overpressure events.

4.10.2 Shutdown Temperature Evaluation

In SECY-94-084, Item C, Safe Shutdown (Reference 4.10-7), the NRC staff recommended the Commission's approval of 420°F or below, rather than cold shutdown condition as a safe stable condition, which the PRHR HX must be capable of achieving and maintaining following non-LOCA events, predicated on acceptable passive safety system performance and an acceptable resolution of the regulatory treatment of nonsafety systems (RTNSS) issue. The NRC has requested a safety analysis to demonstrate that the passive systems can bring the plant to a stable safe condition and maintain this condition so that no transients will result in the specified acceptable fuel design limit and pressure boundary design limit being violated and that no high-energy piping failure being initiated from this condition will result in 10 CFR 50.46 (Reference 4.10-8) criteria.

Westinghouse has previously responded to the NRC in the response to RAI 440.92 (Reference 4.10-9) that the PRHR HX was capable of reducing the RCS temperature to 420°F within 36 hours after shutdown following any design basis transient. As discussed in SSAR subsection 7.4.1.1 (Reference 4.10-10), the PRHR HX will operate to reduce the RCS temperature to the safe shutdown condition. An analysis of the loss of normal feedwater event has been performed to demonstrate that the passive systems can bring the plant to a stable safe condition following design basis transients. The results of this analysis are presented in Figures 4.10-1 through 4.10-5. The progression of this event is outlined in Table 4.10-1.

Summarizing this transient, the loss of normal feedwater occurs, followed by the actuation of the PRHR HX on low steam generator wide-range level. The PRHR HX initially operates with high flow due to the operation of the RCPs. Eventually a safeguards actuation signal is actuated on low cold leg temperature, the RCPs are tripped, and the PRHR HX operates with natural circulation flow.

Once actuated, the CMTs operate in recirculation mode, injecting cold, borated water into the RCS. The CMTs operate in conjunction with the PRHR HX to reduce RCS temperature. Once the CMTs are heated up to the RCS temperature (after about 7 hours of operation), they stop recirculating and the PRHR HX alone removes core decay heat. However, operation of the CMTs in conjunction with the PRHR HX causes the RCS temperature to be reduced to a temperature where the PRHR HX alone is not able to match decay heat at about 4000 seconds. This causes the RCS temperature to increase until the PRHR HX can match decay heat. At about 21,000 seconds, the PRHR HX can match decay heat and it continues to operate to reduce the RCS temperature to below 420°F within 36 hours. As seen from Figure 4.10-1, the cold leg temperature in the loop with PRHR HX is reduced to 420°F at 39,140 seconds, while RCS hot leg temperature in this loop reaches 420°F in 93,690 seconds (approximately 26 hours).

As discussed in a previous revision of SSAR subsection 7.4.1.1 and the response to RAI 440.92, the PRHR HX capability to meet the safe shutdown temperature is dependent on condensate from the containment shell being returned to the IRWST in the nonsafety-related gutter drain return. However, a design improvement has been implemented such that condensate return via the IRWST is now a safety-related function. The gutter isolation valves were upgraded to safety Class C and can perform their intended function while meeting the single failure criterion. As shown in Figure 4.10-5, the IRWST heats up to saturation in about 18,000 seconds. Once saturated, the IRWST inventory will begin to boil, and the steam will be condensed on the containment shell. If condensate is returned to the IRWST, the PRHR HX could operate indefinitely, provided that the passive containment cooling system (PCS) is available.

As shown in Figure 4.10-6, if condensate is not returned to the IRWST, the IRWST water level will drop to the top of the PRHR HX at approximately 30,000 seconds (about 8 hours). The IRWST water level will continue to drop; however, the PRHR HX will continue to operate. Although the PRHR HX is not able to match core decay heat indefinitely in this situation, the PRHR HX will continue to operate and effectively remove heat from the RCS. The RCS temperature profile as the PRHR HX tubes become uncovered is shown in Figure 4.10-7. This plot was generated by modifying LOFTRAN-AP such that when the IRWST water level reaches the top of a PRHR HX node, heat transfer in that node is turned off. This model conservatively bounds the PRHR HX heat transfer when the water level is below the top of the tube bundle.

As discussed in SSAR subsection 7.4.1.1, this mode of operation can last for up to 72 hours. However, in about 22 hours after the event, if no ac power was available, or if condensate return was not available, then the operator will be instructed to actuate the ADS. Operation of the ADS in conjunction with the CMTs, accumulators, and IRWST will reduce the RCS pressure and temperature to below 420°F. Prior to ADS, with no condensate return, the IRWST water level will be reduced to approximately the 22-foot level.

Actuation of ADS at this time will quickly reduce RCS temperatures to below 420°F. The SSAR section 15.6.5.4b analysis of an inadvertent actuation of ADS at full power takes place from an initial RCS T_{avg} condition of 565°F, and it shows that the ADS reduces RCS pressure below the saturation pressure (308.8 psia) of the 420°F temperature in less than 5 minutes by venting steam generated due to flashing of liquid. Note that the pressure in the post-shutdown inadvertent ADS actuation case of SDER subsection 4.8.2 drops below 308.8 psia more rapidly, in less than 100 seconds. The ADS operation leads to injection from the PXS, which reduces the reactor lower plenum temperature in the SSAR full-power case to a value below 200°F before the actuation of ADS stage 4 occurs. Given the much lower RCS energy content and power level 24 hours after trip and the fact that all of the PXS components are available during this event, the depressurization and energy release that ADS actuation must provide to reach an RCS temperature of 420°F will be easily achieved.

Twenty-four hours after reactor trip, the decay heat is less than 1 percent of the full-core power value and the primary temperature is less than 500°F. Due to the extended PRHR HX operation, the level of water in the IRWST has been reduced, so there is less head available at the initiation of IRWST injection than exists for a full-power LOCA case. For cases in which only the PXS is available, the SSAR long-term cooling analysis (SSAR subsection 15.6.5.4c) bounds the 24-hour IRWST injection condition. It presents sump injection scenarios in which lower levels of saturated water inject to the RCS at higher core power levels. Therefore, the IRWST will inject for this postulated event at an adequate rate to provide long-term core cooling. The ADS actuation provides a safety-related method not only to reach an RCS temperature of 420°F but also to achieve core cooling in the long term, if necessary.

Table 4.10-1
Sequence of Events Following a Loss of Normal Feedwater Flow
with Condensate From the Containment Shell Being Returned to the IRWST

Event	Time (seconds)
Feedwater is Lost	10.0
Low Steam Generator Water Level (Narrow-Range) Reactor Trip Setpoint Reached	83.9
Rods Begin to Drop	85.9
PRHR HX Actuation on Low Steam Generator Water Level (Wide-Range)	150.9
Low T_{cold} Setpoint Reached	1069.7
Steamline Isolation on Low T_{cold} Signal	1081.7
RCP Trip on Low T_{cold} Signal	1084.7
CMTs Actuated on Low T_{cold} Signal	1091.7
IRWST Reaches Saturation Temperature	18,540
Heat Extracted by PRHR HX Matches Core Decay Heat	~21,000
CMTs Stop Recirculating	~27,100
Cold Leg Temperature Reaches 420°F (loop with PRHR)	39,140
Hot Leg Temperature Reaches 420°F (loop with PRHR)	93,690

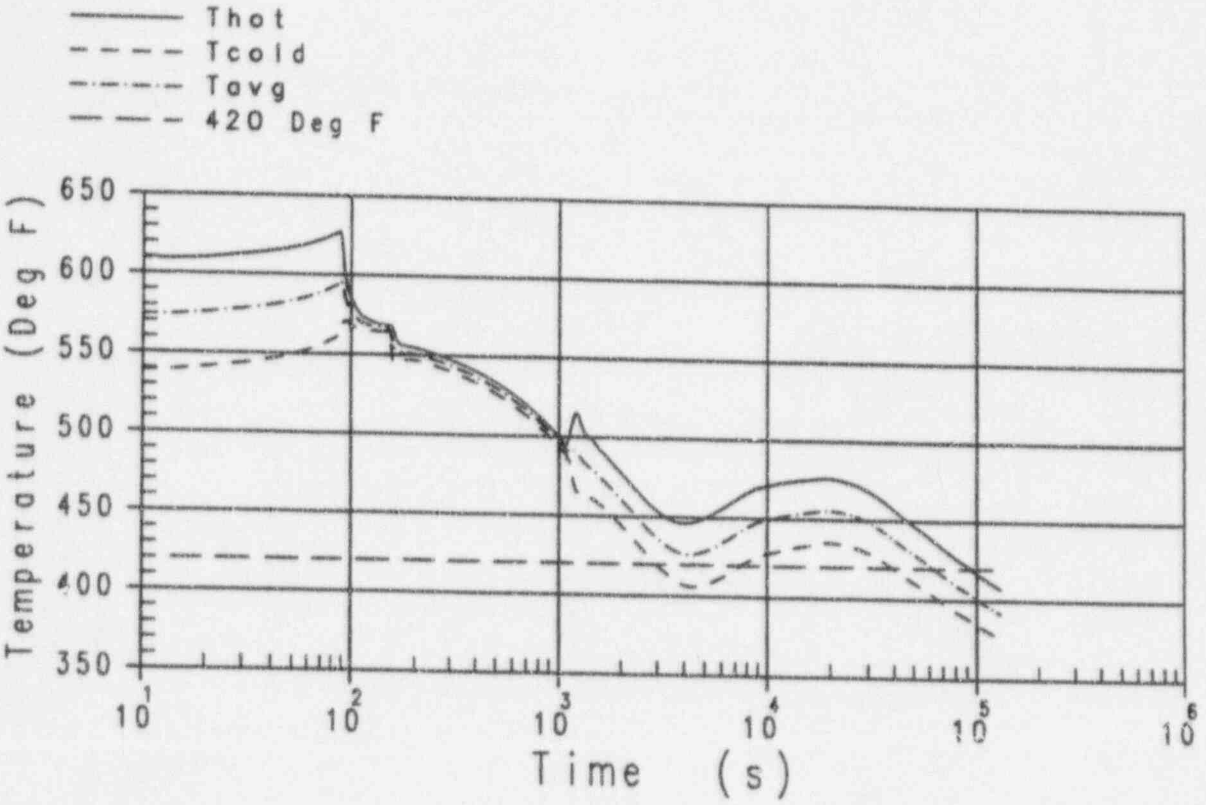


Figure 4.10-1 Shutdown Temperature Evaluation, RCS Temperatura (Loop with PRHR HX)

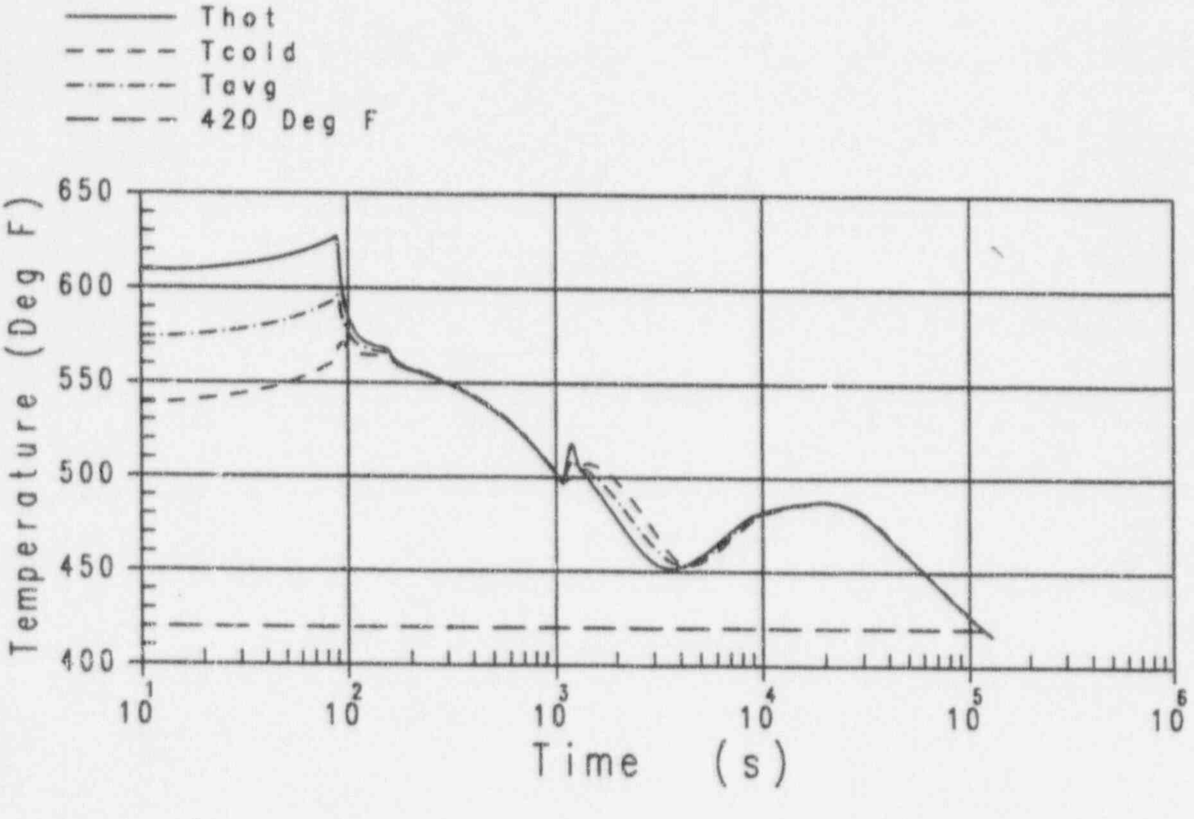


Figure 4.10-2 Shutdown Temperature Evaluation, RCS Temperature (loop Without PRHR HX)

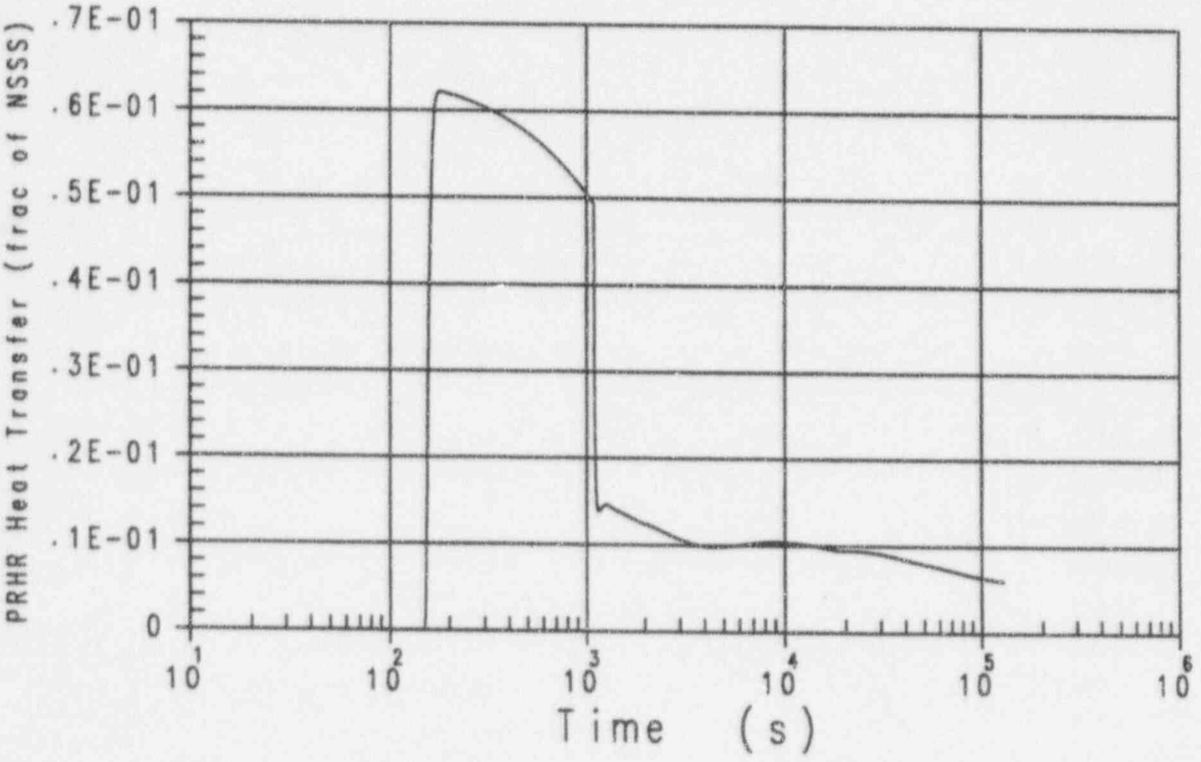


Figure 4.10-3 Shutdown Temperature Evaluation, PRHR Heat Transfer

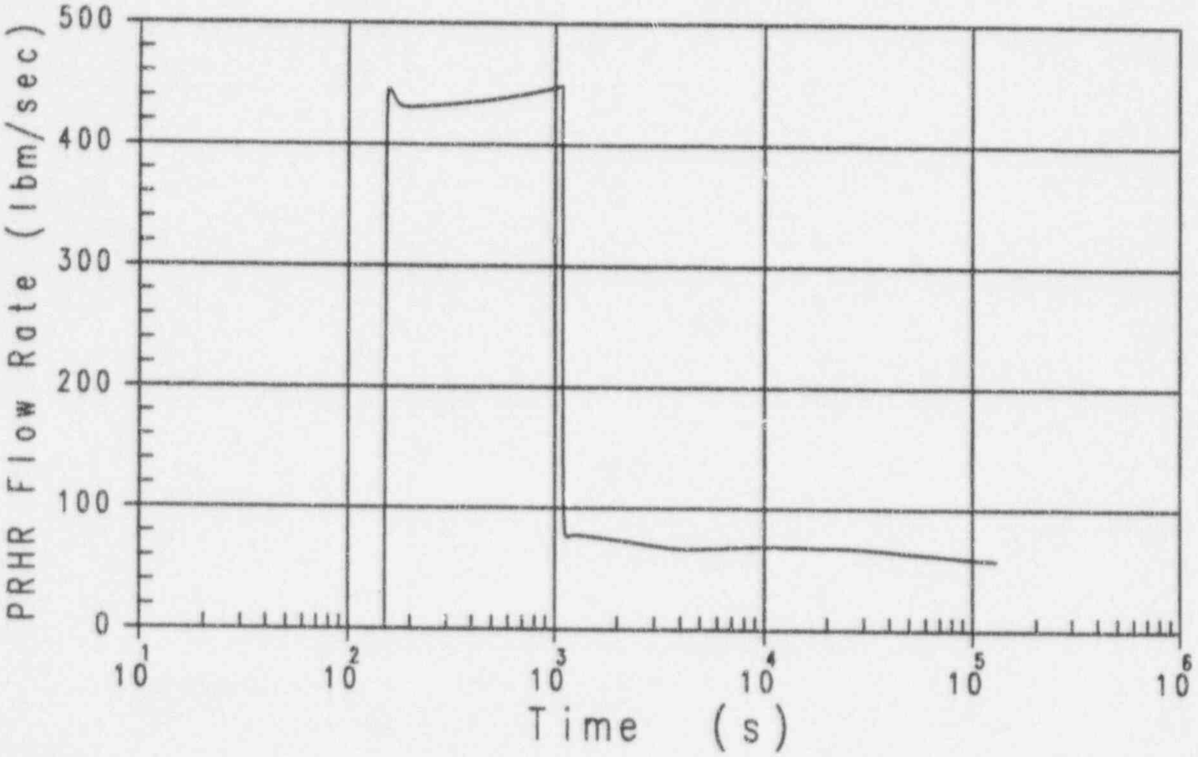


Figure 4.10-4 Shutdown Temperature Evaluation, PRHR Flow Rate

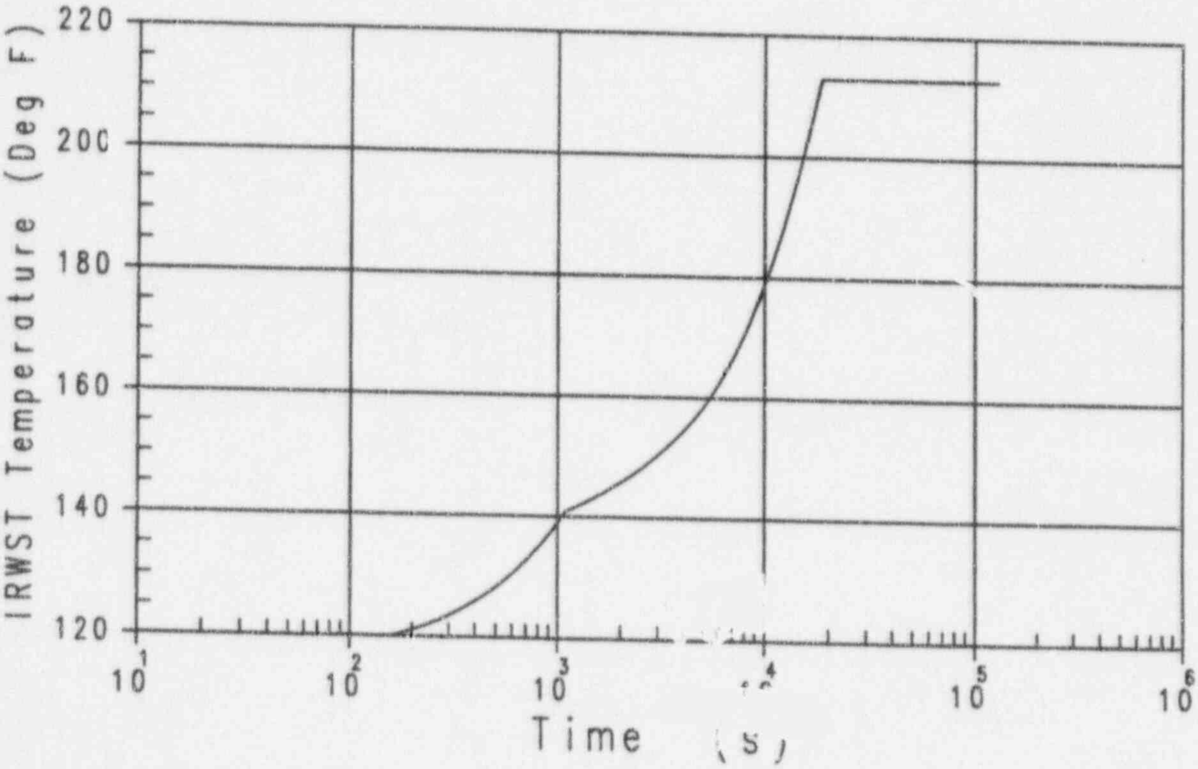


Figure 4.10-5 Shutdown Temperature Evaluation, IRWST Heatup

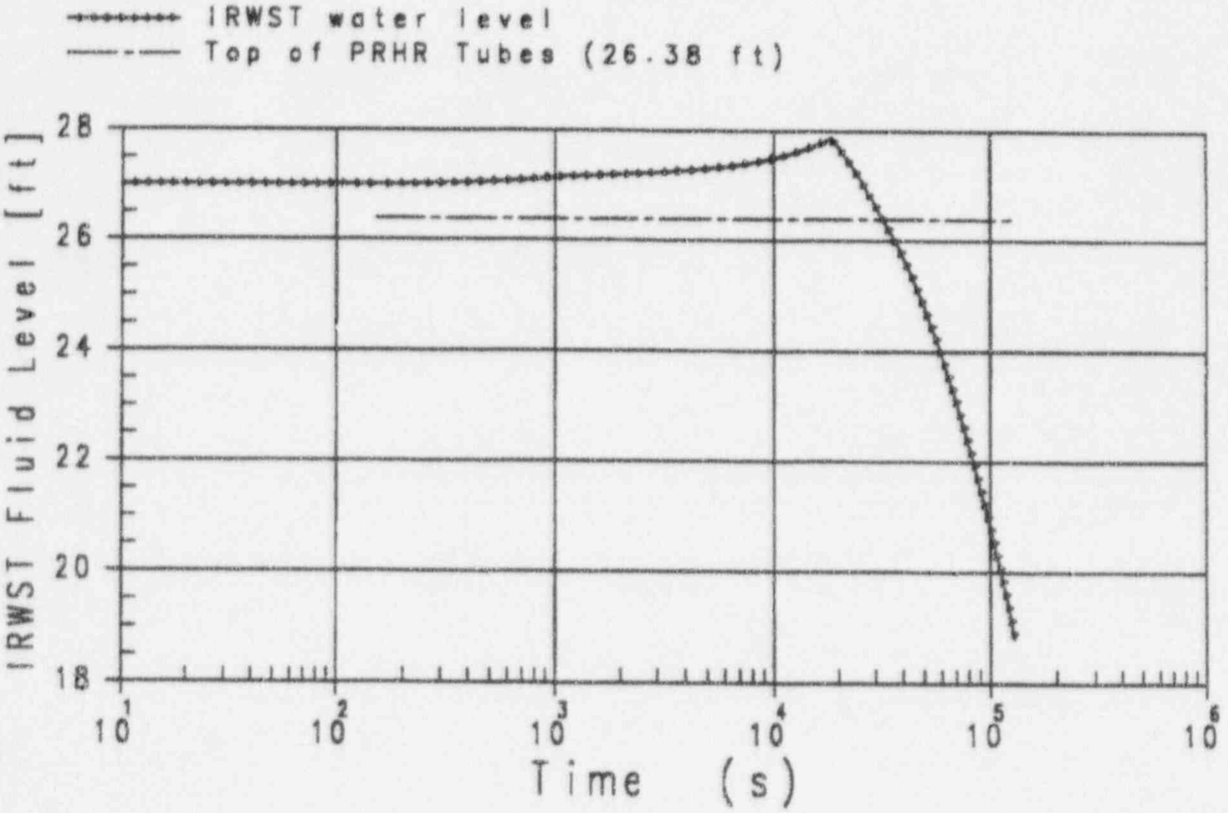


Figure 4.10-6 Shutdown Temperature Evaluation, IRWST Water Level

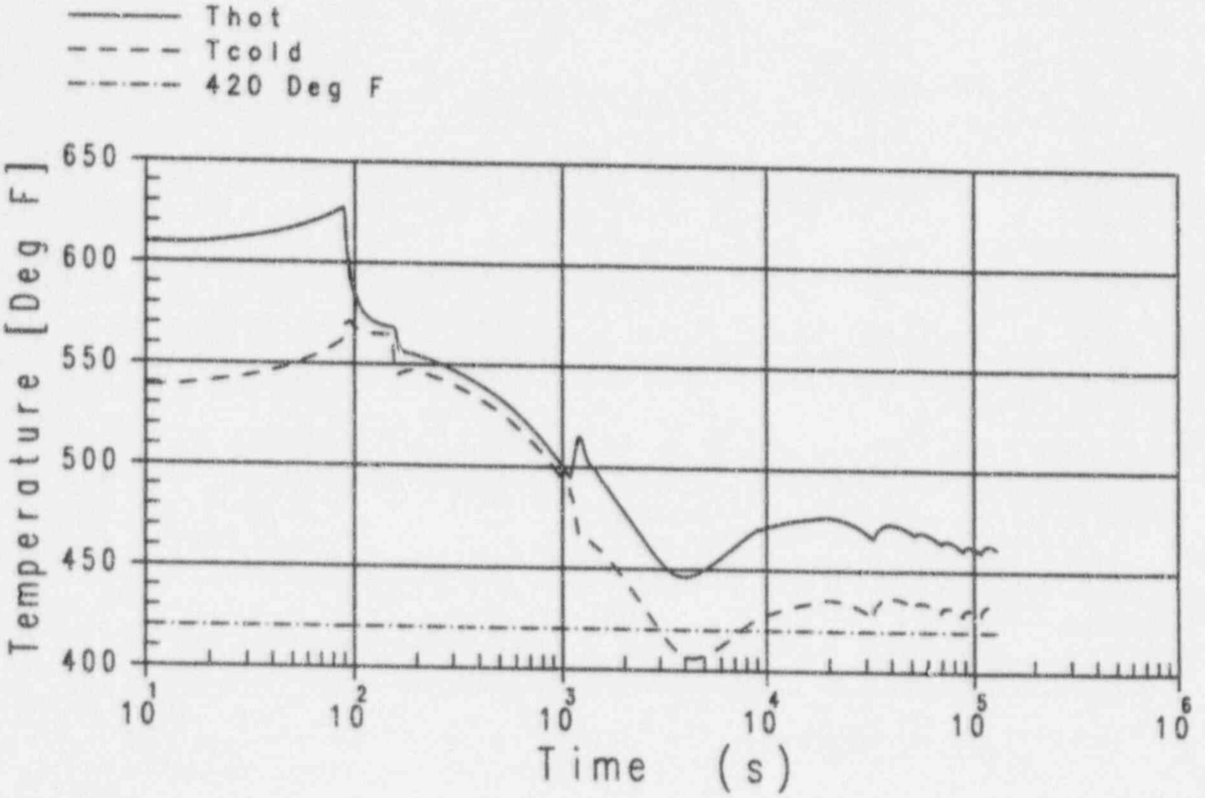


Figure 4.10-7 Shutdown Temperature Evaluation, RCS Temperature, No Condensate Return to IRWST

4.10.3 Rapid Boron Dilution

NUREG-1449, section 6.8 (Reference 4.10-6), is a study of rapid boron dilution sequences possible under shutdown conditions in PWRs. The staff issued this study as NUREG/C-5819. Related to the concerns presented in NUREG/C-5819, the NRC provided RAI 440.120 regarding boron dilution events for the AP600. Westinghouse responded to that RAI in NSD-NRC-96-4773 (Reference 4.10-11). Based on that response, the staff had additional questions addressed via telecon on October 25, 1996. During that telecon, the following occurred:

1. Westinghouse agreed to address concerns with respect to RCP restart and the combined operating license (COL) applicant maintenance procedures in the SDER. This is in SDER section 3.1.

2. Westinghouse committed to revise the response to RAI 440.120. OITS item 3960 will be closed with the transmittal of the RAI 440.120 response, revision 1.

   Completion of this revised response is pending completion of the NOTRUMP LOCA SSAR cases. However, the revisions being made to the non-LOCA portion of that revised response are provided in SDER subsection 4.10.3.1, in advance of the revised RAI response.

3. Westinghouse was asked to clarify numerical diffusion information contained in part b of the RAI 440.120 response. This was provided via facsimile on October 25 and is included in the advance revision provided in SDER subsection 4.10.3.1. This information is not related to shutdown.

4.10.3.1 Advance Copy of Revised Non-LOCA Portion of the Response to RAI 440.120

(b.) Transients or Accidents Addressed by Analysis

The safety-related method for decay heat removal for the AP600 consists of heat transfer to the IRWST by the PRHR, and borated makeup water addition to the RCS from the CMTs. Operation of the CMTs require that the RCPs are tripped. As the residual heat from the core is removed by the PRHR and CMTs, boric acid is added to the RCS by CMT injection flow. The RCS flow associated with the operation of the PRHR and CMT systems is caused by the thermal driving heat established by the convective heat transfer. Analyses have been performed (Reference 440.120-2) to investigate the flow behavior throughout the RCS while the PRHR and CMT systems are removing core decay heat, in order to quantify the resulting boron distributions that could form as convective flow rates approach stagnation. For this study a loss of normal feedwater (LONF) transient was chosen. ~~in order to quantify the resulting boron distributions. For this study a loss of normal feedwater transient was chosen.~~

The Reference 440.120-2 analysis effort utilized the TRAC-PF1/MOD2 code to perform transients that are very similar to the design basis loss of normal feedwater transient that is presented in the SSAR (Reference 440.120-3, ~~120-2 analysis effort utilized the TRAC-PF1/MOD2 code to perform transients that are very similar to the design basis loss of normal feedwater transient (Reference 2,~~ Section 15.2.6). A description of the AP600 TRAC-PF-1 thermal/hydraulic and neutronic models is presented as Sections 3.1 and 3.2, respectively, of the Reference 440.120-2 report. Conditions corresponding to beginning of life, equilibrium cycle, no xenon were assumed, as this would be the most limiting plant conditions in the event core recriticality were predicted. Benchmarking between the TRAC-PF1 code with the SSAR data, which is based upon output from the Westinghouse LOFTRAN-AP code, indicated good agreement. A detailed discussion of the thermal/hydraulic comparison between the TRAC-PF1 calculations and the SSAR data (i.e., Reference LONF) is presented in Section 4.3.1 (pages 4-26 through 4-47) of the Reference 440.120-2 report. An acceptable comparison of the neutronic model was obtained with Westinghouse reference core data. Specifically, the TRAC-PF1 calculated power distributions and rod worth values agreed within 6 to 7% of reference Westinghouse calculations. This degree of agreement for the neutronic model is acceptable given that this study focused on the mixing aspects of boron in the AP600 design and a detailed neutronic response as a result of a boron dilution was not necessary - a return to criticality was not challenged, thus a high level of agreement with the reference Westinghouse data is not required for this study. Furthermore, the TRAC-PF1 calculated reactivity was normalized to the reference Westinghouse data, as discussed on pages 5-48 and 5-49 of the Reference 440.120-2 report.

The results (see Section 5.1 of the Reference 440.120-2 report) of the loss of normal feedwater transients indicate that all regions of the RCS become sufficiently borated following RCP trip and CMT actuation as a result of RCS flow remaining high enough in all regions of the AP600 primary side system for a sufficient duration. The effects of reduced decay heat were also included in the analysis (Section 5.2 of the Reference 440.120-2 report).

~~The results of the loss of normal feedwater transients indicate that all regions of the RCS become sufficiently borated following RCP trip and CMT actuation as a result of RCS flow remaining high enough in all regions of the AP600 primary side system for a sufficient duration. The affects of reduced decay heat were also included in the analysis.~~ The low decay heat analysis arbitrarily assumed 1% of the ANS 1979 decay heat curve. Reduced heat generation in the core results in the passive cooling systems to lose their thermal driving head earlier in the transient, thereby providing a shorter duration for the CMTs to inject the higher concentration boron into the RCS. The results demonstrate that boron concentrations throughout the RCS were much greater than the critical boron concentration required for cold (200 °F), N-1 rods inserted (most reactive RCCA assumed to be stuck out of the core), ~~The results demonstrate that boron concentrations throughout the RCS were must greater than the critical boron concentration required for cold (200°F) N-1 rods inserted (most reactive RCCA assumed to be stuck out of the~~

~~core),~~ no Xenon conditions. Therefore, it can be concluded that subsequent RCS loop recovery, following CMT actuation and RCS cooldown to equilibrium temperatures, will not pose a recriticality potential.

Additional analysis were performed as part of the Reference 440.120-2 study to quantify the volume of unborated water that could collect in the RCP casings and steam generator channelhead without resulting in localized core inlet boron concentrations to decrease to the critical boron concentration following the restart of the RCPs. These additional analyses are discussed in Section 5.3 of the Reference 440.120-2 report. The affects of nominal and reduced decay heat situations were also considered. The initial conditions for these investigations were obtained from the pseudo-equilibrium conditions (i.e., transient times > 4000 seconds) for the loss of normal feedwater transients discussed previously. The findings of this unborated water investigation can be directly applied to the SGTR reverse-break flow scenario and also supplement the previously discussed "Finnish Center" scenario (which is the subject of part (a.) of this response), ~~The findings of this unborated water investigation can be directly applied to the SGTR reverse break flow scenario and also supplement the previously discussed "Finnish Center" scenario,~~ as discussed below.

A high order solute tracker, which is described extensively in Reference 440.120-4 (and is also included as Appendix D of Reference 440.120-2), and discussed to a lesser degree in Section 2.2 of the Reference 440.120-2 report, ~~120-21),~~ was employed to significantly reduce numerical diffusion. This high order solute tracking method employed for the unborated slug investigation has been benchmarked against experimental mixing data from a 1/5 scale model of a three loop Westinghouse PWR. The benchmark against the experimental data is described as Section 4.2.3 of the Reference 440.120-2 report. ~~This high order solute tracking method employed for the unborated slug investigation has been benchmarked against experimental mixing data from a 1/5 scale model of a three loop Westinghouse PWR, also discussed further in Reference 440.120-2.~~ The results of the comparison between the TRAC-PF1 high order solute tracker with the experimental data clearly demonstrate that the high order method is conservatively under-predicting the mixing that would occur, as indicated by the experimental mixing data. This is primarily due to the fact that the high order solute tracker calculations do not account for the mixing that results form the impinging jet of coolant onto the downcomer walls of the reactor vessel. As such the application of the high order solute tracker to the mixing transient calculations discussed below have significant conservatism inherent in the results. Furthermore, the mixing that would occur from the highly turbulent flow caused by the RCP impellers has not been credited. Thus, larger volumes of unborated coolant could be shown to be acceptable if the mixing that would occur from these ignored effects (i.e., inlet coolant jet impingement on the downcomer and RCP impellers), were explicitly modeled.

This high order solute tracking scheme was not employed for the previously discussed loss of normal feedwater transients, as the natural convection flow tends to distribute the boron being injected by the CMTs quite rapidly. This eliminates sharp fonts in the boron concentration and results in a steadily rising system boron concentration in a rather uniform way. Thus, numerical diffusion plays a very small role,~~as the boron transport was determined to be mainly convective, and numerical diffusion plays a very small role,~~ if any, in driving the solute distribution within the system. As such, the runs not modeling unborated slugs of coolant were not repeated with the high order solute transport methods, since the expected results would be basically the same.

The results of this unborated slug analysis, where the RCPs were started in the loop containing the unborated water (see Section 5.3.1 of the Reference 440.120-2 report), ~~where the RCPs were started in the loop containing the unborated water,~~ yielded unborated volumes greater than 115 ft^3 for the situation where nominal decay heat had been assumed, and unborated volumes greater than 66 ft^3 for the situation where the decay heat had been assumed to be 1% of the ANS 1979 curve. In contrast, one RCP casing can collect less than 21 ft^3 before being exposed to the cold leg connection to the RCP casing. In the absence of cold leg loop seal piping, volumes of unborated water larger than 21 ft^3 per RCP casing, would begin to spill into the cold leg piping to be mixed with the borated coolant in the RCS before reaching the reactor vessel. Thus, the maximum volume of unborated water that could collect in a steam generator channel head region cannot be greater than 42 ft^3 (i.e., two RCPs per team generator outlet channel head; this equates to approximately 3.5% of the AP600 reactor vessel inlet plenum volume). The analysis results presented above indicate that approximately one and one-half times this credible value can be accommodated (i.e., this volume can theoretically accumulate and not result in the core inlet boron concentration dropping below the critical concentration following RCP restart in the affected adjacent loops) under low decay heat conditions, and more than two and one half times as much under nominal decay heat conditions.

Unborated slug analyses were also performed assuming that the unborated slug of coolant existed in one loop, and the RCPs were restarted in the opposite loop, as described in Section 5.3.2 of the Reference 440.120-2 report. ~~and the RCPs were restarted in the opposite loop.~~ The findings from this set of analyses is directly applicable to SGTR recovery, as the recovery procedures regarding RCP restart will identify that the RCPs in the intact RCS loop must be restarted first. This analysis demonstrated that the resulting mixing due to the reverse flow through the faulted steam generator and associated RCS loop can accommodate extremely large volumes of unborated water in the faulted steam generator U-tubes and channel head and localized core inlet boron concentrations remain well above the critical boron concentration.

4.10.4 References

4.10-1 Title 10, Code of Federal Regulations, Part 50, Appendix G, "Fracture Toughness Requirements," January 1, 1996.

4.10-2 *AP600 Standard Safety Analysis Report*, Chapter 5, "Reactor Coolant System and Connected Systems."

4.10-3 NTD-NRC-94-4249 (DCP/NRC0173), "Westinghouse Responses to NRC Requests for Additional Information on the AP600," RAI 440.78, July 29, 1994.

4.10-4 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

4.10-5 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

4.10-6 NUREG-1449, *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States, Final Report*, September 1993.

4.10-7 SECY-94-084, "Policy and Technical Iss Associated with the Regulatory Treatment of Non-safety Systems in Passive Plant Designs," March 28, 1994.

4.10-8 Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors," January 1, 1996.

4.10-9 NTD-NRC-94-4184 (DCP/NRC0118), RAI 440.92, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," June 30, 1994.

4.10-10 *AP600 Standard Safety Analysis Report*, Chapter 7, "Instrumentation and Controls."

4.10-11 NSD-NRC-96-4773 (DCP/NRC0555), "Westinghouse Responses to NRC Requests for Additional Information on the AP600," July 18, 1996.

5.0 TECHNICAL SPECIFICATIONS

While the Technical Specification guidance provided in NUREG-1449 (Reference 5.0-1) relates to existing plant shutdown operation concerns, the underlying concerns relating to causes of events and recovery from those events during shutdown operations are applicable to the AP600. This section summarizes resolution of those concerns, many of which are resolved with incorporation of the Nuclear Regulatory Commission (NRC) review comments into the August 1996 revision of the AP600 Technical Specifications (Reference 5.0-2).

Section 5.1 of this *AP600 Shutdown Evaluation Report* (SDER) summarizes the shutdown Technical Specifications and resolves the related *Draft Safety Evaluation Report* (Reference 5.0-3) open item tracking system (OITS) items which support *Draft Safety Evaluation Report* subsection 5.4.7.

Discussion regarding compliance with SECY-93-190 (Reference 5.0-4), resolving OITS items 2053 and 4185, is included in SDER section 5.2.

5.0.1 References

5.0-1 NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," September 1993.

5.0-2 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

5.0-3 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

5.0-4 NRC letter, SECY-93-190, "Regulatory Approach to Shutdown and Low-Power Operations," July 12, 1993.

5.1 SUMMARY OF SHUTDOWN TECHNICAL SPECIFICATIONS

The content of the AP600 Technical Specifications meets the requirements of 10 CFR 50.36 (Reference 5.1-1) and is consistent with the guidance provided in NUREG-1431 (Reference 5.1-2). For the AP600, passive systems are used to safely shut down the plant. Because this design feature is different from existing plants, and because NUREG-1449 provides a reasonable basis for creating shutdown Technical Specifications, the AP600 Technical Specifications were improved to include specifications for these systems in the shutdown modes. These shutdown specifications are summarized in AP600 Technical Specification Table B 3.0-1 of Reference 5.1-3, which provides the passive systems shutdown mode matrix of system versus limiting conditions for operation (LCO), mode applicability, and required end state.

5.1.1 OITS Item 2300

OITS item 2300, for *Draft Safety Evaluation Report* subsection 5.4.7, discusses the response to request for additional information (RAI) 440.58 (Reference 5.1-4). That response describes the changes incorporated into the AP600 Technical Specifications to deal with shutdown operations and identifies any deviations from the guidance specified in NUREG-1449 (Reference 5.1-5), section 6.5 and subsection 7.3.2. A number of followup questions were resolved as follows:

- Issues related to regulatory treatment of nonsafety-related systems (RTNSS)
  - The overall RTNSS issue is still under staff review such that no Westinghouse action is required to resolve this issue at this time.
  - Pending completion of NRC RTNSS activities supporting *Draft Safety Evaluation Report* OITS item 2300, the NRC cannot confirm that no active systems are required to meet the core damage frequency goal. However, the focused probabilistic risk assessment (PRA) section of the RTNSS WCAP, section 2 (Reference 5.1-6), has been revised (see Reference 5.1-7). This issue is considered revised by Westinghouse.
  - Regarding the RNS affecting the initiating event frequency, NSD-NRC-96-4843 (Reference 5.1-8) provides a revision to WCAP-13856, section 3. This issue is considered revised by Westinghouse.
- Items from Table 440.58-1 (of the response to RAI 440.58) were included in the August 1996 revision of the Technical Specifications, SSAR section 16.1 (Reference 5.1-3), such that this issue is resolved.

- Identification of deviations from guidance provided in NUREG-1449 for shutdown Technical Specifications and a technical explanation of those deviations were provided during the Westinghouse and NRC (Reactor Systems Branch) meeting on April 25, 1995. Any pertinent information resulting from that meeting was included in the August 1996 Technical Specifications revision such that this issue is resolved.

5.1.2 OITS Item 2298

This item was discussed during the Westinghouse and NRC (Reactor Systems Branch) meeting of March 27, 1995. Westinghouse indicated that the Technical Specifications would consistently address the requirements for ADS valve configuration and vent capacity at shutdown. These concerns are addressed in Technical Specifications LCOs 3.4.13 (ADS - Shutdown, RCS Intact) and 3.4.14 (ADS - Shutdown, RCS Open). LCO 3.4.13 provides for enough operable ADS flow paths to ensure RCS depressurization consistent with the LOCA safety analyses. The bases for LCO 3.4.14 explain the ADS flow path requirements to ensure that sufficient vent area is available to support IRWST injection. Therefore, this issue was resolved.

As presented in the OITS status field for item 2298, this item relates to open items 2294, 2295, and 2296, which are discussed briefly as follows:

- OITS item 2294

  SDER section 4 addresses the NRC request for a systematic review of initiating SSAR chapter 15 events at lower modes, covering both operation using the normal residual heat removal system (RNS) and passive residual heat removal heat exchangers (PRHR HX).

- OITS item 2295

  SDER section 4.3.2.1 addresses the NRC question regarding loss of RNS during mid-loop operation.

- OITS item 2296

  The design change that moved the in-containment refueling water storage tank (IRWST) actuation on reactor coolant system (RCS) hot leg level to the protection and safety monitoring system (PMS) was discussed at the Westinghouse and NRC (Reactor Systems Branch) meeting on March 27, 1995. Also, the Emergency Response Guidelines (ERGs) (Reference 5.1-9) address shutdown conditions such that those portions of this item are considered to be resolved.

The NRC request for an analysis that identifies the operator action time to actuate the IRWST, because the automatic actuation is not safety-related, is addressed in subsection 4.8.5 of this report.

5.1.3 OITS Item 2306

This was a refueling pool cavity issue, previously addressed for the AP600 design. As noted in the OITS status field, automatic depressurization (ADS) and IRWST injection are available until the upper internals are removed. This is included in AP600 Technical Specification 3.3.2.

5.1.4 References

5.1-1 Title 10, Code of Federal Regulations, Part 50.36, "Technical Specifications," January 1, 1996.

5.1-2 NUREG-1431, "Standard Technical Specifications – Westinghouse Plants," April 1995.

5.1-3 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

5.1-4 NTD-NRC-92-4249, RAI 440.58, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," July 29, 1994.

5.1-5 NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," September 1993.

5.1-6 WCAP-13856, *AP600 Implementation of the Regulatory Treatment of Nonsafety Related Systems (RTNSS) Process Summary Report*, September 1993.

5.1-7 NSD-NRC-96-4869, "Advance Copy of Section 2 of WCAP-13856," November 4, 1996.

5.1-8 NSD-NRC-96-4843, "Advance Copy of Section 3 of WCAP-13856," October 14, 1996.

5.1-9 NSD-NRC-97-4936 (DCP/NRC0702), *Submittal of AP600 Emergency Response Guidelines*, Revision 2, January 10, 1997.

5.2 COMPLIANCE WITH SECY-93-190

OITS item 2053 is two-fold. The first part, which deals with a systematic evaluation of the AP600 design against the shutdown and low-power issues identified in NUREG-1449, is addressed, as the primary objective, in this report. The second part of this issue requests that Westinghouse confirm that the AP600 Technical Specifications (Reference 5.2-1) comply with SECY-93-190 (Reference 5.2-2). This is also OITS item 4185, entered into the system to track closure of key licensing issue 27 from the NRC letter of December 6, 1996 (Reference 5.2-3). This is addressed as follows.

SECY-93-190, published in July 1993, discusses the staff positions preparatory to final staff positions in the area of shutdown and low-power operations. This SECY pre-dates the September 1993 issuance of NUREG-1449 (Reference 5.2-4) and the April 1995 issuance of NUREG-1431 (Reference 5.2-5). Given these more current guidelines for shutdown operation Technical Specifications, the AP600 Technical Specifications aspire to comply with the guidance provided in NUREGs 1449 and 1431, not SECY-93-190. This approach appears to have been accepted by the NRC based on the following.

During a Westinghouse/NRC meeting on March 10, 1994, to discuss shutdown issues, Westinghouse agreed to write an AP600 shutdown report to address the concerns in SECY-93-190, based on receipt of a forthcoming RAI. But when related RAIs 440.53, 440.55, 440.56, 440.58, 440.71, and 440.72 (Reference 5.2-6) were received, they referred to NUREG-1449 rather than SECY-93-190. (All of these RAIs have been answered except 440.53, which requests a systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449. The response to RAI 440.53 will reference this AP600 SDER.)

In summary, as documented in the response to RAIs 440.53, 440.55, 440.56, 440.58, 440.71, and 440.72, and as reflected in the shutdown Technical Specifications), the AP600 Technical Specifications adequately comply with the guidance provided in NUREGs 1149 (Reference 5.2-7) and 1431 to address shutdown-related operations. The final staff positions regarding shutdown Technical Specifications as documented in these NUREGs are considered to supersede SECY-93-190 Technical Specification guidance.

5.2.1 References

5.2-1 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

5.2-2 NRC letter, SECY-93-190, "Regulatory Approach to Shutdown and Low-Power Operations," July 12, 1993.

5.2-3 NRC letter to Westinghouse, Martin to Liparulo, "List of Key Licensing Issues on the AP600 Design," December 6, 1996.

5.2-4 NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," September 1993.

5.2-5 NUREG-1431, "Standard Technical Specifications – Westinghouse Plants," April 1995.

5.2-6 NTD-NRC-92-4249, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," July 29, 1994.

NTD-NRC-94-4184, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," June 30, 1994.

NTD-NRC-94-4264, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," August 12, 1994.

NTD-NRC-92-4257, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," August 8, 1994.

NTD-NRC-94-4254, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," August 3, 1994.

NTD-NRC-94-4279, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," August 26, 1994.

NTD-NRC-95-4213, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," March 7, 1995.

NTD-NRC-94-4194, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," July 8, 1994.

NTD-NRC-94-4237, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," July 27, 1994.

NTD-NRC-94-4291, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," September 2, 1994.

5.2-7 NUREG-1149, *Technical Specifications Limerick Generating Station*, Unit No. 1, June 1985.

6.0 SHUTDOWN RISK EVALUATION

The *AP600 Probabilistic Risk Assessment* (PRA) (Reference 6.0-1) provides an evaluation of the plant risk associated with events at shutdown. PRA chapter 54 addresses the 'ow-power and shutdown risk baseline assessment, chapter 52 includes the shutdown focused PRA, chapter 56 includes the flooding analysis at shutdown, chapter 57 includes the internal fire risk at shutdown, and chapter 59 discusses the plant risk results. The main objective of these studies was to confirm that the AP600 design provides adequate capability to achieve safe shutdown conditions following events at shutdown, by showing that the associated plant risk at shutdown is sufficiently small.

The shutdown PRA evaluates the risk associated with plant operational states during safe/cold shutdown condition when the reactor coolant system (RCS) is filled and intact and with plant states during mid-loop/vessel-flange condition when the RCS is drained and depressurized.

This section summarizes the shutdown risk evaluation results. Section 6.1 provides the shutdown PRA results, and section 6.2 addresses the risk from internal fires and floods at shutdown.

6.0.1 References

6.0-1 *AP600 Probabilistic Risk Assessment*, September 30, 1996.

6.1 SUMMARY OF SHUTDOWN PRA RESULTS AND INSIGHTS

This section summarizes the insights drawn from the PRA (Reference 6.1-1) results. Subsection 6.1.1 provides the level 1 baseline shutdown PRA results, subsection 6.1.2 provides the level 2 baseline shutdown PRA results, subsection 6.1.3 provides the results from level 1 baseline sensitivity analysis, subsection 6.1.4 provides the shutdown-focused PRA level 1 results, and subsection 6.1.5 provides the shutdown-focused PRA level 2 results.

The level 1 baseline shutdown PRA base case has a core damage frequency (CDF) of 5.50E-08 events per year and is discussed in subsection 6.1.1. This low CDF compares to the AP600 level 1 baseline at-power PRA CDF of 1.7E-07 events per year, which is approximately two orders of magnitude less than a typical pressurized water reactor (PWR) plant currently in operation. The reasons for this low CDF at shutdown are the many AP600 design features discussed in section 2.0 of this report. These include:

- Passive safety-related systems are available in all shutdown modes. Planned maintenance of passive features is performed only during shutdown modes when that feature is not risk-important.

- Reliable nonsafety-related active systems that provide a first level of defense. Planned maintenance of nonsafety-related defense-in-depth features used during shutdown is performed at-power.

- Passive safety-related systems do not depend on support systems, such as ac power, component cooling water system (CCS), service water system, and compressed air.

- Automatic actuation of the passive safety-related systems backed up by proceduralized operator action are reflected in the AP600 shutdown Emergency Response Guidelines (ERGs) (Reference 6.1-2) discussed in section 3.3 of this report.

The following major insights are deduced from the results of the AP600 shutdown PRA. Supporting details for these insights are summarized in the results of the baseline and sensitivity cases provided in later subsections of this report.

a. The problem of overdraining the RCS while draining to mid-loop that exists in operating plants is not a major concern in the AP600. The reliability of the hot leg level instrumentation together with automatic isolation backed by manual isolation capabilities of the drain paths relegate overdraining of the RCS to an extremely unlikely event.

b. Although operator actions are important, serving as manual backup to automatic actuation of systems or equipment, they are not risk significant at the level of plant risk obtained from shutdown PRA – evidenced by a decrease of only 9 percent when all human error probabilities are set to zero. However, operator actions are indeed important in maintaining a low CDF, as shown by an increase of approximately two orders of magnitude when all operator actions are assumed to fail 50 percent of the time.

c. The reliability of the normal residual heat removal system (RNS) function is important in maintaining the current low CDF. In particular, loss of decay heat removal capability, during drained condition, due to failure of the CCS or service water system, dominates the shutdown initiating events. The analysis has also shown that, if the RNS function is assumed to always fail, the shutdown CDF increases by approximately four orders of magnitude, which is still relatively low.

d. The components providing in-containment refueling water storage tank (IRWST) injection function are among the most risk-significant AP600 components, evidenced by their contribution to the shutdown CDF. In particular, common cause failure of the IRWST strainers or valves in the injection lines dominate failures of the IRWST subsystem and are significant contributors to the CDF for each dominant sequence. However, common cause failure of the IRWST strainers is believed to be conservative because the IRWST water is regularly sampled and purified via the lines that connect to the strainer. This considerably reduces the chance of clogging.

e. The reliability of the IRWST subsystem is important in maintaining the current low CDF, because given loss of the RNS during reduced inventory conditions, the IRWST provides the only mitigating function; events at mid-loop dominate the shutdown CDF. If the IRWST function is assumed to always fail, the shutdown CDF increases by approximately four orders of magnitude, which is still relatively low.

f. The loss of offsite power event during mid-loop operation could be a risk-significant event. This is true for cases where the diesel generators fail and the grid is not recovered in time to permit operation of the RNS pumps. In that regard, the reliability of the diesel generators is important in reducing potential loss of decay heat removal capability during reduced inventory conditions.

g. The reliability of the instrumentation and control (I&C) equipment is important in maintaining the current level of shutdown CDF. Common cause failure of the logic cards in the control and protection system and common cause failure of the protection and safety monitoring system power interface output boards dominate the I&C failures.

h. Performing tests and maintenance on electrical components, RNS components, or components of RNS support systems during mid-loop operation could significantly impact the reliability of the plant if an initiating event develops during that time. Therefore, it is important to ensure equipment operability before entering drained conditions and, if vital equipment for operation during drained conditions fails, assessment of the associated risk should consider taking the plant to the filled RCS condition for maintenance or repairs.

i. Because many of the water sources to the containment are valved off during shutdown, a significant percentage of the severe accidents at shutdown result in dry reactor cavities in which the vessel fails and the ex-vessel debris cannot be cooled. Therefore, accident management strategies should consider a timely means of flooding the reactor cavity; this would reduce the potential basemat penetration frequency which, in turn, would significantly reduce the overall large-release frequency.

The overall CDF and large-release frequency at shutdown for the AP600 has been shown to be small as indicated in the following discussions.

6.1.1 Level 1 Base Case Results

The level 1 shutdown PRA base case has a CDF of 5.50E-08 events per year. This CDF is obtained from quantifying the 10 shutdown initiating events shown in Table 6.1-1. The level 1 shutdown quantification results are summarized in Table 6.1-1, which indicates that the three events dominating the CDF are loss of CCS/service water system during drained condition, loss of offsite power during drained condition, and loss of RNS during drained condition.

Six dominant accident sequences comprise 92 percent of the level 1 shutdown CDF. These dominant sequences are as follows:

1. Loss of CCS or service water system initiating event during drained condition contributes 54.1 percent of the CDF.

2. Loss of offsite power initiating event during drained condition with failure of grid recovery within 1 hour contributes 13.6 percent of the CDF.

3. Loss of RNS initiating event during drained condition contributes 10.4 percent of the CDF.

4. Loss of offsite power initiating event during drained condition with success of grid recovery within 1 hour contributes 5.4 percent of the CDF.

5. LOCA initiating event due to inadvertent opening of RNS-V024 during safe/cold shutdown conditions contributes 5.0 percent of the CDF.

Table 6.1-1
Level 1 Accident Sequences Quantification Results

Event	Plant Condition	Event Tree Identifier	Sequence Frequency	Core Damage Contribution
Loss of offsite power during RCS safe/cold shutdown condition	RCS filled and pressurized	LOSP-ND	8.13E-03	5.44E-10
Loss of offsite power during RCS drained condition	RCS drained to mid-loop	LOSP-D	1.E-03	1.05E-08
Loss of decay heat removal due to failure within the RNS during RCS safe/cold shutdown condition	RCS filled and pressurized	RNS-ND	9.61E-04	4.14E-10
Loss of decay heat removal due to failure within the RNS during RCS drained condition	RCS drained to mid-loop	RNS-D	8.15E-05	5.73E-09
Loss of decay heat removal due to failure of the CCS or service water system during RCS safe/cold shutdown condition	RCS filled and pressurized	CCW-ND	3.21E-03	1.38E-09
Loss of decay heat removal due to failure of the CCS or service water system during RCS drained condition	RCS drained to mid-loop	CCW-D	4.23E-04	2.98E-08
LOCA due to RNS pipe break during RCS safe/cold shutdown condition	RCS filled and pressurized	LOCA-PR-ND	1.51E-05	1.44E-10
LOCA due to draining the RCS into the IRWST through valve RNS-V024 during RCS safe/cold shutdown condition	RCS filled and pressurized	LOCA-V024-ND	1.68E-05	2.79E-09
LOCA due to draining the RCS into the IRWST through valve RNS-V024 during RCS drained condition (LOCA-V024-D)	RCS drained to mid-loop	LOCA-V024-D	1.13E-05	7.96E-10
RCS overdrain during drainage to mid-loop condition	RCS depressurized	RCS-OD	4.44E-06	2.96E-09

6. RCS overdraining event during drainage to mid-loop contributes 3.4 percent of the CDF.

The following subsections describe the dominant sequences.

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

This seqtence is described as the loss of decay heat removal initiated by failure of the CCS or service water system during drained condition. The loss of decay heat removal occurs following loss of CCS 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 IRWST injection valves and manual actuation of the RNS pump suction valve fail.

The major contributors to risk due to loss of CCS/service water system during drained condition are:

- Hardware failures of both service water pumps or common cause failure of the output logic input/output from the plant control system (PLS)

- Common cause failure of the strainers in the IRWST tank

- Common cause failure of the IRWST injection valves

6.1.1.2 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. Following this initiating event, the RNS does not restart automatically and the grid is not recovered within 1 hour. Core damage occurs if manual actuation of the IRWST injection valves and manual actuation of the RNS pump suction valve fail.

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

- Software common cause failure of all cards
- Failure of RNS pump to run or restart
- Failure of a diesel generator to start and run
- Failure of the main breaker 100 (or 200) to open
- Failure to recover ac power within 1 hour

- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the IRWST injection valves

6.1.1.3 Loss of RNS Initiating Event during Drained Condition

This sequence is described as the loss of decay heat removal initiated by failure of the RNS during drained condition. The loss of decay heat removal occurs following loss of RNS during mid-loop/vessel flange operation, which has an estimated duration of 120 hours. Core damage occurs if automatic and manual actuation of the IRWST injection valves and manual actuation of the RNS pump suction valve fail.

The major contributors to risk due to loss of RNS during drained condition are:

- Common cause failure of the RNS pumps to run
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the IRWST injection valves

6.1.1.4 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, which has an estimated duration of 120 hours. Following this initiating event, the RNS does not restart automatically and the grid is recovered within 1 hour, but manual RNS restart after grid recovery fails. Core damage occurs if automatic and manual actuation of the IRWST injection valves and manual actuation of the RNS pump suction valve fail.

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

- Software common cause failure of all cards
- Failure of RNS pumps to run or to restart
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the IRWST injection valves

6.1.1.5 LOCA Initiating Event due to Inadvertent Opening of RNS-V024 During Safe/ Cold Shutdown Conditions

This sequence is described as the loss-of-coolant accident (LOCA) initiated by inadvertent opening of RNS-V024 during cooldown when the RCS is filled and pressurized. The LOCA occurs during safe/cold shutdown conditions, which have an estimated duration of 220 hours. Following the initiating event, the core makeup tanks (CMTs) are actuated and the automatic depressurization system (ADS) actuates. Core damage occurs if the IRWST injection valves do not open automatically.

The major contributors to risk due to LOCA through RNS-V024 during safe/cold shutdown conditions are:

- Inadvertent opening of RNS-V024 due to cperator error
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the IRWST injection valves

6.1.1.6 RCS Overdraining Event During Drainage to Mid-loop

This sequence is described as RCS overdraining initiated 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 RNS fails. Core damage occurs if manual actuation of the IRWST injection valves and manual actuation of the RNS pump suction valve fail.

The major contributors to risk due to RCS overdraining initiated during drainage to mid-loop are:

- Common cause failure of the chemical and volume control system (CVS) air-operated valves to close automatically upon receipt of low hot leg level signals and failure of the operator to stop draining

- Operator failure to isolate the RNS

- Operator failure to open the IRWST injection valves

- Operator failure to open the RNS pump suction valve

- Common cause failure of the strainers in the IRWST tank

- Common cause failure of the IRWST injection valves

6.1.2 Severe-Release Frequency Results for Shutdown

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 failed either because of the initiating event or because it was 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 presents the results of the containment event tree quantification with respect to large-release frequency and contributions of the different failure types.

- Overall results and contributions

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

  – The frequency of the containment integrity being compromised from the initiation of the accident 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 percent of the overall shutdown large-release frequency.

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

  – 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 dry reactor cavities in which the vessel fails and the ex-vessel debris cannot be cooled. The frequency of basemat penetration is 1.1E-08 events per reactor-year. This frequency is 78 percent of the overall large-release frequency.

- Initially impaired containment

  – Approximately 63 percent of the initially impaired containment frequency consists of unisolated interfacing systems LOCA initiating events. Approximately 1.4 percent of the initially impaired containment frequency is attributed to steam generator tube ruptures (SGTRs) induced by high pressure and temperature severe accident sequences.

  – Approximately 23 percent of the initially impaired containment frequency is due to failure of the containment isolation system to close the containment to the environment.

  – Approximately 13 percent of the initially impaired containment frequency is due to a containment which is isolated, but leaks excessively.

- Containment failures induced by high energy phenomena

  The timing of induced containment failure 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 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. Because the frequency of the high-pressure melt ejection cases is small, no further analyses of the associated phenomena have been performed. Instead, high-pressure melt ejection cases are lumped into the early containment failure. The frequency of high-pressure melt ejection cases (1.3E-11 events per reactor-year) is less than 0.02 percent of the CDF and contributes less than 0.1 percent of the large-release frequency. Given the insignificant fraction of the CDF involved, no effort was made 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 PWRs afford considerable promise that integrity would be maintained.

  - Intermediate and late containment failures contribute less than 0.1 percent to the large-release frequency.

  - The following are the estimated frequencies of the phenomena that may challenge containment integrity at shutdown:

    - Frequency of core damage combined with failure of passive containment cooling water is 3.8E-12 events per reactor-year

    - Frequency of global combustion is 2.7E-10 events per reactor-year

    - Frequency of unmitigated core-concrete interaction is 1.1E-08 events per reactor-year

- Frequency of ex-vessel fuel coolant interaction is 4.4E-10 events per reactor-year

- Frequency of high-pressure melt ejection is 1.3E-11 events per reactor-year

- Frequency of in-vessel fuel coolant interactions that threaten containment integrity negligible

6.1.3 Shutdown Level 1 Base Case Sensitivity Analysis

The results of the Shutdown Level 1 PRA Importance and Sensitivity study (Reference 6.1-1) are summarized in this subsection. Twelve cases were evaluated, and the most significant conclusions and insights drawn from the results are as follows:

- Initiating events importance: Initiating events during RCS drained conditions contribute approximately 85 percent of the total CDF; loss of decay heat capability (during drained condition) due to failure of the CCS or service water system has the greatest contribution (54 percent of the CDF).

  However, overdraining the RCS during drainage to mid-loop, LOCAs due to inadvertently opening RNS-V024 during drained and nondrained conditions, and loss of decay heat during drained condition are major initiating event categories contributing to risk increase (achievement). A high-risk achievement indicates it is important that the reliability of the system, component, or human error that contributes to the initiating event frequency is (and remains) as good as shown in the PRA.

- Common cause failure importance: Common cause failure of the IRWST components contributes approximately 83 percent of the total CDF; common cause failure of valves in the IRWST injection lines contributes approximately 63 percent of the total CDF.

  However, common cause failures of the I&C (logic cards in the control and protection systems, and protection and safety monitoring system [PMS] power interface output boards) and common cause failure of valves in the IRWST injection lines are contributors to risk increase.

  Common cause failures of the IRWST components are significant contributors to both the risk decrease and risk increase worths. The conclusion drawn from these components significant to the risk decrease worth is that if improving common cause failure is considered to reduce the CDF at shutdown, then common cause failure of IRWST injection valves and strainers should be likely candidates. Similarly, the conclusion drawn from these components relative to the risk increase worth is that the reliability of the IRWST injection valves and strainers is important in maintaining the current level of CDF at shutdown.

Also, the reliability of the I&C is extremely important in maintaining the current level of CDF at shutdown.

- Human error importance: Human errors contribute approximately 18 percent of the total CDF but are not overly important; no particular dominant contributor exists.

  However, operator failure to recognize the need for RCS depressurization during safe/cold shutdown conditions is a contributor to risk increase. A high-risk achievement indicates it is important that the human reliability is (and remains) as good as shown in the PRA for this operator action.

- Component importance: Component failures contribute approximately 15 percent of the total CDF but are not overly important; no particular dominant contributor exists. This indicates that single independent component failures are not particularly important to the shutdown CDF.

  However, failure of the passive residual heat removal heat exchanger (PRHR HX) system due to failure of the IRWST tank is a contributor to risk increase. A high-risk achievement indicates it is important that the reliability of this component is (and remains) as good as shown in the PRA.

- IRWST system failure sensitivity: If the IRWST is assumed to be completely unavailable, the CDF increases (by a factor of 11709) to 6.44E-04. The benefit and importance of the IRWST during low power and shutdown conditions is evidenced by this result. The results of this sensitivity indicate that failure of the IRWST directly affects the drained cases, which already dominate the CDF, because the RNS is also not available.

- RNS system failure sensitivity: If the RNS is assumed to be completely unavailable, the CDF increases (by a factor of 5745) to 3.16E-04. The benefit and importance of the RNS during RCS drained conditions is evidenced by this result. The results of this sensitivity indicate that failing the RNS causes the RNS initiating event sequences during drained conditions to dominate the CDF.

- Set all human error probabilities to 0.0 sensitivity: If operator response is assumed to be perfect, the CDF decreases by 9 percent. This decrease of 9 percent in the base CDF indicates that the operator actions are not risk important at the level of plant risk obtained from the base case study.

- Set all human error probabilities to 0.5 sensitivity. If operator response is assumed to fail 50 percent of the time, the CDF increases (by a factor of 54) to 2.99E-06. This increase in the base CDF is high, even though a CDF cf 2.99E-06 is low. The result indicates that the operator actions are important in maintaining a low CDF for internal events at shutdown.

- Allowing test and maintenance of electrical components during drained condition sensitivity: If test and maintenance unavailability of electrical components is allowed during drained condition, the CDF increases by a factor of 2. This increase in the base CDF is moderate even though a CDF of 1.07E-07 is low. The result indicates that it is important to ensure equipment operability before entering drained conditions and, of equal importance, if vital equipment for operation during drained condition fails, the plant should be taken to the filled RCS condition for maintenance or repairs.

- Allowing unscheduled maintenance of RNS components during drained conditions: If unscheduled maintenance is allowed on RNS components during drained conditions, the CDF increases by 18 percent. This increase of 18 percent in the base CDF is low and indicates that performing unscheduled maintenance on one loop of the RNS is not risk important at the level of plant risk obtained from the base case shutdown study.

- Allowing unscheduled maintenance of CCS components during drained conditions: If unscheduled maintenance is allowed on CCS components during drained conditions, the CDF increases by 16 percent. This increase of 16 percent in the base CDF is low and indicates that performing unscheduled maintenance on one loop of the CCS is not risk important at the level of plant risk obtained from the base case shutdown study.

- Allowing unscheduled maintenance of service water system components during drained conditions: If unscheduled maintenance is allowed on service water system components during drained conditions, the CDF increases by 27 percent. This increase in the base CDF is low and indicates that performing unscheduled maintenance on one loop of the service water system is not risk important at the level of plant risk obtained from the base case shutdown study.

The I&C systems currently model corrective maintenance in the shutdown PRA. Mean times tc detect and repair failures are incorporated into the calculation of individual basic event unavailabilities. Therefore, no sensitivity for corrective maintenance is required for the I&C systems.

6.1.4 Shutdown Focused PRA Sensitivity Study Core Damage Quantification Results

This section presents the results of the CDF calculation for the shutdown focused PRA sensitivity study. The CDF for the shutdown focused PRA sensitivity study is calculated to be 4.1E-07 events per year. Table 6.1-2 presents CDF contribution by initiating event for the shutdown focused PRA sensitivity study. The last column of the table shows the baseline PRA contribution for the associated basic event for comparison.

The focused PRA sensitivity study for shutdown events shows a relatively smaller increase in the CDF from the baseline assessment than that of the at-power focused PRA sensitivity study. This is because the shutdown assessment credits fewer nonsafety-related systems, structures, and components (SSCs) in the PRA assessment than the at-power assessment. With the exception of the loss of offsite power models in the shutdown PRA, no nonsafety-related front-line systems are credited in the event tree models. Nonsafety-related support system credit (that is, non-class 1E power systems and the diverse actuation system [DAS]) is modeled in the baseline PRA. Removal of these nonsafety-related systems accounts for most of the increase in CDF. In general, initiating events in both the shutdown baseline PRA and the shutdown focused PRA sensitivity study have maintained the relative contributions to respective total CDF.

The largest contributors to the shutdown focused PRA sensitivity study CDF are loss of offsite power events during mid-loop operation, accounting for over 75 percent of the total shutdown focused PRA sensitivity study CDF. The assumed failure of the RNS, DAS, and the non-class 1E power systems account for the increase by a factor of 30.

Other events during mid-loop conditions account for most of the remaining CDF for the shutdown-focused PRA sensitivity study. The increase in CDF by factors of two or three can be attributed to the assumed failure of DAS and non-class 1E power systems. The same applies to the RCS overdraining condition.

For the safe/cold shutdown LOCA events, the contribution to the total shutdown focused PRA sensitivity study CDF increases by less than a factor of two. The assumed loss of DAS and main ac power system accounts for the difference because all systems modeled in the baseline event trees are safety-related.

Table 6.1-2
Shutdown-focused PRA Sensitivity Study – Core Damage Frequency Contribution by Initiating Event (System Unavailability = 4.11E-07)

Basic	Event[1]	Basic Event Probability	Percentage of Core Damage	Focused PRA Contribution to Core Damage	Baseline PRA Contribution to Core Damage
1	IEV-LOSPD	1.483E-03	76.60	3.15E-07	1.05E-08
2	IEV-CCWD	4.23E-04	16.70	6.86E-08	2.98E-08
3	IEV-RNSD	8.15E-05	3.21	1.32E-08	5.73E-09
4	IEV-RCSOD	4.44E-06	1.93	7.92E-09	2.96E-09
5	IEV-LOCA24ND	1.68E-05	1.02	4.17E-09	2.79E-09
6	IEV-LOCA24D	1.13E-05	.45	1.83E-09	7.96E-10
7	IEV-LOCAPRND	1.51E-05	.05	2.07E-10	1.44E-10
8	IEV-LOSPND	8.13E-03	.03	1.33E-10	5.44E-10
9	IEV-CCWND	3.21E-03	.01	5.27E-11	1.38E-09
10	IEV-RNSND	9.61E-04	.00	1.58E-11	4.14E-10
TOTALS			~100	4.11E-07	5.50E-08

[1] Event descriptions are shown in Table 6.1-1, column 1.

In the case of loss of offsite power, loss of the RNS, and loss of the CCS or service water system for safe and cold shutdown conditions, an improvement in CDF occurs. This is due to the assumed loss of main ac power and subsequent loss of compressed air. Loss of compressed air means that the passive core cooling system (PXS) air-operated valves will assume their intended fail-safe state, given enough time for the air supply pressure to drop due to leakage or cycling of valves. Therefore, for these events, I&C modeling to the air-operated valves is removed. The assumption that DAS and non-class 1E power systems fail otherwise tends to increase the CDF of these cases.

6.1.5 Shutdown Focused PRA Sensitivity Study Release Frequency Results Summary

The results of the focused PRA sensitivity study release frequency assessment for shutdown and low-power operation for the AP600 are discussed below:

- The overall shutdown focused PRA sensitivity study large-release frequency for the AP600 is 2.6E-07 events per reactor-year. This frequency includes containment bypass, containment isolation failure, excessive containment leakage, and containment failures.

- The frequency of the containment integrity being compromised from the initiation of the accident is 4.4E-09 events per reactor-year. This impaired containment frequency includes containment bypass, containment isolation failure, and excessive containment leakage. It accounts for 1.7 percent of the overall shutdown focused PRA sensitivity study large-release frequency.

- The frequency of containment failure within 24 hours of core damage is 2.1E-07 events per reactor-year. This frequency includes early and intermediate containment failures. It accounts for 81 percent of the overall large-release frequency.

- Approximately 55 percent of the initially impaired containment frequency consists of containment bypass initiating events with a frequency of 2.4E-09 events per reactor-year. Approximately 1.2 percent of the initially impaired containment frequency is attributed to induced SGTRs with a frequency of 5.1E-11 events per reactor-year.

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

- Approximately 1 percent of the early containment failure frequency is due to high-pressure melt ejection cases. Because th. frequency of the high-pressure melt ejection cases is small, no further analyses of the associated phenomena have been performed. Instead, high-pressure melt ejection cases are lumped into the early containment failure release category. The frequency of high-pressure melt ejection cases (1.6E-11 events per reactor-year) is less than 0.01 percent of the CDF and contributes less than 0.01 percent of the large-release frequency. Given the insignificant fraction of the CDF involved, no effort was made 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 PWRs afford considerable promise that integrity would be maintained.

- The frequency of containment failure after 24 hours of core damage due to basemat failure is 4.3E-08 events per reactor-year. Basemat failure occurs more than 72 hours after the onset of core damage. The frequency accounts for 17 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 dry reactor cavities in which the debris cannot be cooled. Core-concrete interaction produces a large amount of combustible gases. Nonsafety-related igniters cannot be credited in the focused PRA sensitivity study evaluation and, therefore, there is a significant increase in the frequency of cases that result in intermediate containment failure from hydrogen combustion compared to the baseline analysis.

- The following are the estimated frequencies of the shutdown containment challenges from severe accident high-energy events:

  - Frequency of core damage combined with failure of passive containment cooling water is 1.4E-13 events per reactor-year

  - Frequency of global combustion is 3.7E-07 events per reactor-year

  - Frequency of unmitigated core-concrete interaction is 2.5E-07 events per reactor-year

  - Frequency of ex-vessel fuel coolant interaction is 1.6E-09 events per reactor-year

  - Frequency of high-pressure melt ejection is 1.6E-11 events per reactor-year

  - Frequency of in-vessel fuel coolant interactions which threaten containment integrity is approximately 0.0 events per reactor-year

6.1.6 References

6.1-1 *AP600 Probabilistic Risk Assessment*, September 30, 1996.

6.1-2 NSD-NRC-97-4936 (DCP/NRC0702), *Submittal of AP600 Emergency Response Guidelines*, Revision 2, January 10, 1997.

6.2 RISK FROM INTERNAL FIRES AND FLOODS AT SHUTDOWN

The *AP600 Standard Safety Analysis Report* (SSAR) describes design requirements and features intended to ensure that the plant can achieve safe conditions following an internal fire or internal flood. Internal fires and floods are those resulting from plant-related structures, systems, components, or other inside-the-plant sources. This safe shutdown capability is required whether the plant is in power or shutdown conditions.

6.2.1 Design Features that Minimize Fire and Flooding Risk at Shutdown

6.2.1.1 Internal Fire Protection Design Features

AP600 SSAR section 9.5.1 ˎ‹eference 6.2-1) describes the fire protection design features and bases. These features protect the plant during all operating modes, including shutdown, by the following:

- Minimizing the chances of fire occurrence
- Providing the means to promptly detect and suppress any fires that do occur
- Mitigating the consequences of fires

Fire occurrence minimization features include:

- Use of noncombustible structural materials (for example, reinforced concrete, gypsum, masonry, and structural steel) in plant buildings

- Control of combustible materials (for example, separation of turbine lube oil system and diesel fuel oil storage from safety-related equipment areas using 3-hour fire barriers)

- Procedural guidance expected to be implemented by combined operating license (COL) applicant regarding safe work practices for hot work, control of combustible materials, and housekeeping

Fire detection and suppression features include:

- Fire detection and alarm system (including smoke, flame, heat, and product of combustion detectors as appropriate to the various areas; audible and visual alarms in the main control room and the security central alarm station; uninterruptible power supply to fire detection and alarm equipment)

- Fire water supply system designed according to appropriate National Fire Prevention Association (NFPA) and NRC requirements

- Automatic and manual fire suppression capabilities (including wet, dry, preaction, and deluge sprinklers as appropriate to the various fire areas; manual fire fighting hose stations and hydrants; and fire extinguishers)

Fire mitigation features include:

- Subdivision of the plant into fire areas to minimize the potential for fire spread

- Enclosure of plant areas containing safety-related components with 3-hour fire barriers

- Separation of redundant safe shutdown components and associated instrumentation and cabling with 3-hour fire barriers (except in the main control room and containment, where this is not practical)

- Use of sealed fire barrier penetrations

- Design, routing, and separation of electrical cables according to applicable fire protection requirements (as documented in the AP600 SSAR)

- Enclosed emergency escape/fire fighting access routes for plant personnel

AP600 SSAR section 9A (Reference 6.2-1) presents the results of a fire protection analysis to demonstrate the capabilities of the fire protection system and the ability to safely shut down the plant following a fire.

6.2.1.2 Internal Flood Protection Design Features

AP600 SSAR subsection 3.4.1 (Reference 6.2-2) describes plant features intended to protect against floods, including internal flooding.

Flooding occurrence minimization features include:

- Embedding process piping penetrating below the maximum flood level either in walls or in floors, or welding to a steel sleeve embedded in the wall or floor

Flooding detection features include:

- Water leak detection systems (level sensors and alarms)

Flooding mitigation features include:

- Physical separation of redundant safe shutdown components using structural enclosures or structural barriers
- Minimization of the number of penetrations through enclosure or barrier walls below the flood level
- Use of watertight penetrations in instances where flood protection walls below the flood level must be penetrated
- Design of walls, floors, and penetrations to withstand the maximum anticipated hydrodynamic loads associated with a pipe failure
- Use of curbs and elevated thresholds to localize flooding effects
- Drain systems and sump pumps
- Provision of limits on the supply of fire water in the auxiliary building non-radiological area

AP600 SSAR subsection 3.4.1.2.2 (Reference 6.2-2) presents an internal flooding analysis to show that for each area of the plant containing safety-related equipment, the most adverse postulated flooding conditions do not prevent safety-related systems, structures, or components from performing their required safe shutdown functions.

6.2.2 Evaluation of Risk from Internal Fire and Internal Flooding at Shutdown

The AP600 PRA provides an evaluation of the plant risk associated with internal fires and floods at shutdown. PRA chapter 57 (Reference 6.2-3) discusses the internal fire risk at shutdown, and PRA chapter 56 (Reference 6.2-4) discusses the internal flooding risk at shutdown. The objective of these analyses was to confirm that the design incorporates adequate capability to achieve safe shutdown following these events, by showing that the associated plant risk is sufficiently small.

6.2.2.1 Shutdown Internal Fire Risk

Shutdown Internal Fire Risk Evaluation

The internal fire risk evaluation began with a process to determine which fire areas were to be evaluated and which could be eliminated from further evaluation, based on the presence or absence of fire initiation sources or equipment important to safe shutdown as modeled in the internal events PRA. Areas cont ining no significant fire initiation sources or safe shutdown equipment posed little fir risk and were not considered beyond this stage of the evaluation. Because the plant is already shut down, an initiating event for the shutdown analysis was considered as one that threatens or fails the normal decay heat removal function. That is, the event either fails or degrades the normal decay heat removal success path or initiates a loss of RCS integrity resulting in a LOCA, which in turn threatens the ability of the normal decay heat removal systems to remove decay heat.

A bounding estimate of fire initiation frequency and an evaluation of associated fire damage conditions were made for each fire area retained for analysis. The fire ignition frequencies used in the shutdown fire analysis reflect the fraction of a year that the plant is expected to spend in safe shutdown and in mid-loop conditions. The CDF for each scenario was then quantified using the models from the shutdown internal events focused PRA. In the quantification, it was assumed that all fire-susceptible equipment in the exposing and potentially exposed fire areas fails due to the fire. Because as-built equipment location and cable routing information is not available, the focused PRA models, which credit only safety-related equipment, were used to bound the quantification results. Thus, in the quantification process, the nonsafety-related systems (for example, main feedwater system, startup feedwater system, RNS, or DAS) were not credited. In reality, few AP600 fire areas would be susceptible to fires that might disable all the nonsafety-related systems.

In deriving the predicted scenario frequencies, the calculation combined the area ignition frequency with estimates of failure probabilities for fire barriers, automatic fire suppression systems (if present), and faulted conditions that could initiate additional failures, such as spurious actuation of the ADS from fire-induced cable hot shorts. All plant fire areas identified in the AP600 SSAR chapter 9A (Reference 6.2-1) fire analysis were evaluated, including the main control room and the remote shutdown workstation area. In addition, although not typically done in fire PRAs, an evaluation of the effects of fires inside containment was made for AP600. This containment evaluation considered transient sources of combustibles and welding activity inside containment because there may be a large amount of maintenance activity.

Shutdown Internal Fire Risk Results Summary

The results from the shutdown fire analyses confirmed that the inherent design characteristics of the AP600 provide an effective barrier against potential internal fire hazards. This is true even given the pessimistic assumptions used throughout the study, which include the following:

- A major conservatism used in the fire analysis is the use of the AP600 focused PRA model for the quantification of the conditional core damage probabilities. The focused PRA model does not take credit for any nonsafety-related equipment for achieving shutdown following an initiating event. In reality, fires in only a few AP600 fire areas would be capable of disabling all the nonsafety-related systems. Fires in the containment building, for example, would not have an impact on the availability of important nonsafety-related systems (such as RNS, startup feedwater system, and DAS). Therefore, this modeling approach has an impact on the estimated contribution of this area to the fire-induced CDF.

- A fire originating from any ignition source in an area is assumed to disable all equipment located in the fire area. A review of the historical evidence shows that most fires are localized fires with limited severity.

- Manual fire suppression is not credited to limit the extent of damage in an area nor to prevent fire propagation to an adjoining area. Historical evidence shows that most fires were manually suppressed with little or no additional damage.

- Fire-induced open shorts and hot shorts in I&C and power circuits were considered. It was assumed that a single hot short could result in spurious ADS actuation, whereas, in reality, at least two simultaneous shorts are expected to be required for actuation.

The total calculated contribution to CDF caused by fires that occur during safe shutdown is estimated, on a bounding basis, as 2.6x10^{-8} per year. The contribution to CDF from fires that occur during mid-loop operation is estimated, on a bounding basis, as 3.6x10^{-7} per year. Of these totals, the contribution from control room fires is small, on the order of 10^{-12} per year for safe shutdown and less than 10^{-9} per year for mid-loop operation.

Large release frequency calculations were not performed for the fire analysis because the total shutdown fire CDF using the focused PRA models with bounding fire frequency assumptions was similar in magnitude to the shutdown focused PRA core damage frequency. The AP600 containment isolation design is such that at least one component random failure would be required to result in containment isolation failure via a given line, even if a fire caused failure of another isolation component in that line. Further, there are only a few areas in which a fire affecting a containment isolation component could occur. As a result, the frequency of fire-induced core damage with fire-related containment isolation failure is sufficiently small that no significant change would be expected from the large release or plant risk profiles determined for the shutdown focused PRA.

Shutdown Internal Fire Risk Contributors

The shutdown internal fire risk contributors are as follows:

- Safe shutdown

  The dominant contributors to core damage from fire at safe shutdown are listed in Table 6.2-1. Together these areas contribute approximately 90 percent of the total CDF contribution from fires that occur during safe shutdown. The reason that several of these individual contributors rose to the top was that the fire scenario as modeled resulted in a hot short actuation of ADS valves, resulting in a LOCA, and simultaneously disabled at least one division of Class-1E power, a condition that has a relatively high conditional core damage probability. Containment fires at safe shutdown contribute less than 1 percent of the total fire-related CDF in this mode. The contribution from control room fires is low.

- Mid-loop operation

  The dominant contributors to core damage from fires at mid-loop are shown in Table 6.2-2. The fire areas listed in that table contribute an aggregate total of approximately 90 percent of the mid-loop fire CDF, showing that the contributions are distributed over the entire plant and are not dominated by any specific area. The relatively important contributing areas generally have similar characteristics. That is, the modeled fires result in the loss of one division of safety-related power or one division of nonsafety-related power.

  The single largest contribution to mid-loop fire CDF is from fires in the yard (approximately 21 percent of the mid-loop total). These have been assumed to result in non-recoverable loss of offsite power, despite fire location, severity, or affected equipment. The CDF for this scenario is large because the initiating event frequency is roughly an order of magnitude higher than the other scenario frequencies and because no credit has been taken for nonsafety-related systems in the quantification. The total contribution from fires in containment during mid-loop operation is less than 20 percent of the total. The evaluation identified zones inside containment where it was assumed that safety-related cables from more than one division of power and control (but related to only one train of safety-related equipment) would be located. For these zones, it was further assumed that a fire of any size would result in fire-induced loss of the two divisions of safety-related power and control which, for focused PRA mid-loop scenarios, results in a significant probability of failure of IRWST injection resulting in core damage. The contribution from control room fires is less than 1 percent of the total.

Table 6.2-1
Dominant Fire Core Damage Contributors – Safe Shutdown

Fire in Area	Affected Equipment	Modeled Event[1]
1202 AF 05	Division C Electrical Equipment	Hot-short LOCA + Loss of 1 Div.[2]
1222 AF 02	Division B RCP Trip Switchgear	Hot-short LOCA + Loss of 1 Div.
1201 AF 03	Division D DC Equipment/I&C	Hot-short LOCA + Loss of 1 Div.
1202 AF 04	Division A Electrical Equipment	Hot-short LOCA + Loss of 1 Div.
1222 AF 01	Division B Electrical Equipment	Hot-short LOCA + Loss of 1 Div.
1230 AF 03	Non-1E Electrical Zone (100'el)	Hot-short LOCA + Loss of DAS

1. In addition to failure of all nonsafety-related equipment through use of the focused PRA model
2. "Loss of 1 Div." in this table means loss of one division of safety-related control, modeled as loss of Division B.

6.2.2.2 Shutdown Internal Flooding Risk

Shutdown Internal Flooding Risk Evaluation

The process used to examine flooding risk was similar to that used for internal fire risk. Deterministic criteria were used to screen out any areas in which the risk from flooding is clearly insignificant, based on lack of flood initiation sources or absence of equipment important to safe shutdown, as modeled in the internal events PRA. Because the plant is already shut down, an initiating event for the shutdown analysis was considered an event leading to a threat to equipment needed for the normal decay heat removal function through water submergence or spray.

A quantitative analysis was performed to identify flooding sources and estimate the frequency and associated flood damage conditions for each flooding area for which credible flood or damaging spray initiation scenarios were identified. The potential for flood propagation to surrounding areas was evaluated as well. The flooding frequencies used in the shutdown flooding analysis reflect the fraction of a year that the plant is expected to spend in safe shutdown and in mid-loop conditions. The CDF impact of each scenario was then quantified using the models from the shutdown internal events PRA, assuming that all equipment subject to submergence (based on maximum anticipated flood height) or water spray in the area fails. An assessment using the focused PRA models was also made.

Table 6.2-2
Dominant Fire Core Damage Contributors – Mid-loop

Fire in Area	Affected Equipment	Modeled Event[1]
0000 AF 00	(All Fires in Yard/Outside Bldgs.)	Loss of Offsite Power (LOOP)
1100 AF 11500	Containment Operating Floor	LOOP[2] + Loss of 1 Div.[3]
1202 AF 05	Division C Electrical Equipment	LOOP[2] + Loss of 1 Div.[3]
1222 AF 02	Division B RCP Trip Switchgear	LOOP[2] + Loss of 1 Div.[3]
2053 AF 01	Generator Panel Room	LOOP[2]
1201 AF 03	Division D DC Equipment/I&C	LOOP[2] + Loss of 1 Div.[3]
1202 AF 04	Division A Electrical Equipment	LOOP[2] + Loss of 1 Div.[3]
1231 AF 01	Division B I&C Equipment	LOOP[2] + Loss of 1 Div.[3]
1222 AF 01	Division B Electrical Equipment	LOOP[2] + Loss of 1 Div.[3]
1200 AF 01	RCA/Auxiliary Building	Loss of RNS
4031 AF 04	Demineralizer Water Degasifier Room	Loss of RNS
1201 AF 02	Division B Batteries	LOOP[2] + Loss of 1 Div.[3]
1201 AF 03	Division C Batteries	LOOP[2] + Loss of 1 Div.[3]
6030 AF 02	Diesel Generator Room B	LOOP[2]
6030 AF 01	Diesel Generator Room A	LOOP[2]
4031 AF 05	Electrical Equipment Room	LOOP[2]
1100 AF 11300C	Containment Maintenance Floor	LOOP[2] + Loss of 2 Div.[3]
1211 AF 01	Division D Battery Room	LOOP[2] + Loss of 1 Div.[3]
1212 AF 01	Division A Battery Room	LOOP[2] + Loss of 1 Div.[3]

1. In addition to failure of all nonsafety-related equipment through use of the focused PRA model

2. Although loss of power is not expected due to the fire, the loss of offsite power model from the shutdown focused PRA was used to represent core damage scenarios.

3. "Loss of 1 Div." in thus table means loss of one division of safety-related power and control (modeled as Div. B); "Loss of 2 Div." means loss of two divisions (modeled as A and C) of safety-related power and control.

In deriving the predicted scenario frequencies and effects, the evaluation considered flow based on double-ended ruptures of piping in each area and storage tank rupture and spillage of entire tank inventory. Water submergence was assumed to result in equipment failure, and water spray of equipment without an appropriate environmental qualification rating was assumed to result in failure or power short-to-ground. All plant areas identified in the AP600 SSAR internal flooding analysis (Reference 6.2-4) were considered in the screening evaluation.

Shutdown Internal Flooding Risk Results Summary

The results from the shutdown flooding analyses confirmed that the inherent design characteristics of the AP600 provide an effective barrier against potential internal flooding hazards. This is true even considering several pessimistic assumptions used in the study, such as assuming total system failure for nonsafety-related fluid systems if they are affected by flooding in any area, and taking no credit for operation of sump pumps to mitigate consequences of flooding.

Eight internal flooding at shutdown scenarios were identified in the analysis. The total calculated contribution to CDF from internal flooding during safe shutdown is estimated to be 5×10^{-11} per year, an insignificant value. The calculated contribution to CDF from internal flooding during mid-loop operation is estimated to be 1.5×10^{-9} per year.

The internal flooding analysis was also performed using the focused PRA models as a sensitivity. The total calculated CDF from internal flooding is estimated, on the more pessimistic focused PRA basis, as 3.9×10^{-9} per year.

Large release frequency calculations were not performed for the internal flooding analysis because the total shutdown internal flooding CDF was so much smaller than the large-release frequency goal of 1×10^{-6} per year.

Shutdown Internal Flooding Risk Contributors

The shutdown internal flooding risk contributors are as follows:

- Safe shutdown

  There were no significant contributors to internal flooding risk at safe shutdown.

- Mid-loop operation

  Two mid-loop internal flooding scenarios contribute over 95 percent of the total internal flooding at shutdown CDF. In both of these scenarios, decay heat removal capability is lost as a result of flooding-induced failure of the RNS, either directly or through loss of the CCS or service water system, which both remove heat from the RNS. In the first scenario, the initiating event is rupture of a CCS, service water system, or fire protection water pipe in the turbine building; in the other scenario, the initiating event is rupture of a chemical and volume control or fire protection water pipe in one of the auxiliary building RCA areas.

6.2.3 Important Plant Features That Minimize Internal Fire and Flooding Risk at Shutdown

The analysis highlights several important features of AP600 that minimize risk due to fire and flooding during all operating modes including shutdown.

The AP600 fire and flooding protection scheme provides separation of the equipment and cabling for each of the four divisions of safe shutdown equipment using 3-hour-fire-rated structural barriers. Areas containing safety-related equipment or cabling are physically separated from one another and from areas that do not contain safety-related equipment by sealed 3-hour-fire-rated barriers with no openings in the barriers. This defense-in-depth feature results in a small probability that a fire or flood would affect more than one safety-related system or division. In addition, the design minimizes location of potential flooding sources in safety-related equipment areas to the extent possible. This further reduces the impact of internal floods.

Individual fires resulting in loss of offsite power, or affecting onsite diesel generator operability, do not affect safe shutdown capability. This is because the AP600 does not rely on ac power for safe shutdown capability and the safety-related (defense-in-depth) passive systems do not require ac power or cooling for operation.

Fire barrier integrity detection likelihood is enhanced because each fire door is alarmed and monitored in the control room, so the probability of inadvertently leaving one open and undetected for a significant period of time is expected to be small. Whenever a fire door must be blocked open to allow specific maintenance activities, additional compensatory measures (for example, a fire watch established in the area) are expected to be taken. Requirements for fire barrier and fire barrier penetration seal (for example, electrical and mechanical seals, fire doors, and fire dampers) design, installation, and maintenance will be as specified, at a high level, in Appendix R and applicable NFPA requirements, and will be implemented in COL programs subject to NRC review.

Fire and flooding detection and mitigation capability is provided in the design and is maintained during shutdown, even when parts of the automatic systems are rendered unavailable for preventive maintenance or testing. This is because compensatory measures are expected to be taken to maintain the detection and mitigation capability. In addition, capability is provided for manual fire fighting using local hose stations (this was not credited in the analysis).

A detailed assessment of the effects of fires in the main control room showed that the calculated CDF from fires in the AP600 main control room is small for the following reasons:

- The AP600 main control room fire ignition frequency is low because of the use of low-voltage, low-current (48 volt, 10mA dc) equipment. This equipment does not produce enough energy to be a likely source of ignition.

- There are redundant means available to shut down and control the plant. Redundancy in control room operations is provided within the control room itself for fires in which control room evacuation is not required. The remote shutdown workstation provides complete redundancy of control and monitoring, in a fire area separate from the main control room, for all safe shutdown functions in the event that main control room evacuation is required. There are no differences between the main control room and remote shutdown workstation controls and monitoring that would be expected to affect safety system redundancy and reliability. All important main control room operator actions credited in the PRA that might be required following an main control room fire (for example, actuation of PRHR HX, CMTs, ADS, IRWST gravity injection, and containment recirculation) can be accomplished from the remote shutdown workstation. A fire in the main control room does not affect the transfer of control to the remote shutdown workstation. The remote shutdown workstation transfer switches are located in a fire area outside the main control room. The main control room/remote shutdown workstation transfer will use separate multiplexers for control inputs which originate in the main control room and remote shutdown workstation. The multiplexers will be enabled and disabled by the control transfer switches. There will be separate multiplexer sets associated with each of the four PMS divisions so that a single failure cannot result in the transfer (or return) of more than one division. (A further discussion of the main control room/remote shutdown workstation transfer was provided in the response to RAI 720.345.)

- The PMS is designed such that, although an main control room fire may defeat remote manual actuation of equipment, it will not affect the automatic functioning of safe shutdown equipment. Because the AP600 design includes diverse and redundant safe shutdown equipment that is designed to operate automatically, the operator actions that may be disrupted by an main control room fire are backup actions that are generally not risk-significant. This was shown in the fire analysis by taking no credit for operator response in main control room fire scenarios requiring control room evacuation.

The AP600 is designed such that containment isolation functions are not compromised by fire. Redundant containment 'solation valves in a given line are located in separate fire areas or zones and, if powered, are served by different electrical divisions. Containment isolation for a typical penetration is provided by two series valves: one served by division A or C power and control (if powered) and located in a fire area or fire zone containing only division A or C equipment, and a second valve served by division B or D power and control (if powered), and located in a fire area or fire zone containing only division B or D equipment. Further, one isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire barrier. Thus, the probability of a fire that would cause failure of containment isolation in lines penetrating containment is not significant.

6.2.4 Shutdown Internal Fire and Flooding Risk Conclusions

The results of the AP600 fire PRA study show that the system and layout designs of the plant promote low internal-fire- and internal-flooding-induced CDFs, even when nonsafety-related systems are not credited. Because of the scoping nature of the fire and flooding analyses performed for AP600, it is inappropriate to compare the numerical results of these analyses directly to the results of the internal-events analysis. It is expected that an evaluation using as-built plant information will result in much lower frequencies for most scenarios.

The results of the AP600 shutdown internal fire and internal flooding analyses show that the AP600 design is sufficiently robust that internal fires or floods during shutdown do not represent a significant risk contribution. In addition, the Technical Specifications require availability of the safety-related systems during lower modes such that design basis accident (DBA) acceptance criteria are met. Therefore, the DBA evaluations for fire and flooding, provided in the SSAR (Reference 6.2-1), is applicable during lower modes. The relevant information presented in the SSAR (References 6.2-1 and 6.2-2), in the internal fire risk analysis (Reference 6.2-3), and in the internal flooding risk analysis (Reference 6.2-4) shows the ability of t e plant to achieve or reestablish safe shutdown conditions following an internal fire or flooding event. The requirements of *Draft Safety Evaluation Report* (Reference 6.2-5) open item tracking system (OITS) item 2303 have, therefore, been met.

The results further show that safe shutdown following internal fires or internal floods can be achieved, and an acceptably low level of risk attained, using only safety-related equipment.

Draft Safety Evaluation Report OITS item 3441 is addressed as follows. On page 15 of the NRC letter of June 24, 1996, (Reference 6.2-6), the NRC provides a definition of "safe shutdown condition" in relation to a fire event. This definition is reiterated in RAI 280.12 and designated as open item 9.5.1.6-1 of Reference 6.2-6. RAI 280.12, and therefore item 9.5.1.6-1, was consequently assigned to the *Draft Safety Evaluation Report* OITS as item 3441. The response to RAI 280.12 was provided in NSD-NRC-96-4823 (Reference 6.2-7) and item 3441 was closed, with a commitment to discuss it in this section of the SDER. The requirements of *Draft Safety Evaluation Report* OITS item 3441 have, therefore, been met.

6.2.5 List of RAIs Relating to Internal Fire and Internal Flooding Shutdown Analyses

Responses were provided to the following Request for Additional Information (RAIs) for the internal fire analysis at shutdown: 720.353, 720.354, 720.355, 720.356, 720.357, 720.360, and 720.365 (Reference 6.2-8), and 720.358, 720.359, 720.361, 720.362, 720.363, and 720.364 (responses in progress).

Responses were provided to the following RAIs for the internal fire analysis at power, which are also relevant to the shutdown analysis: 720.334, 720.337, 720.338, 720.339, 720.340, 720.341, 720.342, 720.344, 720.345, 720.346, 720.347, 720.348, 720.349, 720.350, and 720.351 (Reference 6.2-9), and 720.335, 720.336, and 720.352 (Reference 6.2-10).

Responses were provided to the following RAIs for the internal flooding analysis at shutdown: 720.322 and 720.323 (Reference 6.2-11).

Responses were provided to the following RAIs for the internal flooding analysis at power, which are also relevant to the shutdown analysis: Responses to questions related to *Draft Safety Evaluation Report* open items 19.1.3.2-15, -17, -18, -19, -20, -21, and 22, as provided in Westinghouse letter NSD-NRC-96-4856 (Reference 6.2-11).

6.2.6 References

6.2-1 *AP600 Standard Safety Analysis Report,* Chapter 9, "Auxiliary Systems," and Appendix 9A, "Fire Protection System and Analysis."

6.2-2 *AP600 Standard Safety Analysis Report,* Chapter 3, "Design of Structures, Components, Equipment, and Systems."

6.2-3 *AP600 Probabilistic Risk Assessment,* Chapter 57, "Internal Fire Analysis," September 30, 1996.

6.2-4 *AP600 Probabilistic Risk Assessment,* Chapter 56, "PRA Internal Flooding Analysis," September 30, 1996.

6.2-5 Draft NUREG-1512, *Draft Safety Evaluation Report,* November 1994.

6.2-6 Letter from NRC to Westinghouse, Jackson to Liparulo, "Open Issues in Standard Safety Analysis Report Sections Regarding Fire Protection for the AP600 Design," June 24, 1996.

6.2-7 NSD-NRC-96-4823 (DCP/NRC0606), "Westinghouse Responses to NRC Requests for Additional Information on the AP600," September 20, 1996.

6.2-8 NSD-NRC-97-4994 (DCP/NRC0748), "AP600 Response to Requests for Additional Information," February 21, 1997.

6.2-9 NSD-NRC-97-4941 (DCP/NRC0707), "AP600 Response to Requests for Additional Information," January 14, 1997.

6.2-10 NSD-NRC-97-4943 (DCP/NRC0708), "AP600 Response to Requests for Additional Information," January 16, 1977.

6.2-11 NSD-NRC-96-4856 (DCP/NRC0634), "Westinghouse Response to NRC Request for Additional Information on the AP600," October 23, 1996.

7.0 COMPLIANCE WITH NUREG-1449

The Diablo Canyon event of April 10, 1987, and the loss of ac power event at the Vogtle plant on March 20, 1990, led the Nuclear Regulatory Commission (NRC) staff to issue NUREG-1449, *Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States* (Reference 7.0-1), to provide an evaluation of the shutdown risk issue. The scope of NUREG-1449 includes subjects such as operating experiences as documented in generic letters, operator training, technical specifications, residual heat removal capacity, temporary reactor coolant boundaries, rapid boron dilution, containment capacity, fire protection, outage planning and control, and instrumentation.

In request for additional information (RAI) 440.53 (Reference 7.0-2), the NRC requested Westinghouse to assess the compliance AP600 with NUREG-1449. In the RAI, the NRC recognized that some of the issues discussed in NUREG-1449 are the responsibility of the plant owners because they relate to operation, maintenance, and refueling plans, procedures, and risk management. However, the NRC believed that the level of defense-in-depth against shutdown events would be improved if clear guidance is provided to the areas discussed above by the plant designer. The NRC requested that Westinghouse perform a systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449 as they are applicable to the AP600 design and document the results in a dedicated section in the *AP600 Standard Safety Analysis Report* (SSAR) (Reference 7.0-3).

This *AP600 Shutdown Evaluation Report* (SDER) provides the systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449. As discussed in SDER section 1, this report provides the results of the systematic evaluation of the AP600 during shutdown operations. This assessment includes design basis evaluations of events that can occur during shutdown and a probabilistic assessment of plant risk at shutdown. The design of the AP600 builds on the lessons-learned from the industry with regard to shutdown safety, including the guidance provided in NUREG-1449. SDER section 2 discusses the various design features included in the AP600 that have been incorporated to improve shutdown safety and shutdown risk. SDER section 3 includes maintenance insights and guidance related to shutdown operations to provide the combined operating license (COL) applicant with insights from the plant designers to assist the plant owner with shutdown risk management.

SDER section 4 provides the design basis evaluations of events that can occur at shutdown. These analyses are performed with conservative assumptions to demonstrate the safety of the AP600 during shutdown modes. SDER section 5 addresses the technical specifications that have been incorporated to cover shutdown modes. The inclusion of appropriate shutdown technical specifications was an important observation noted in NUREG-1449, and the AP600

Technical Specifications (Reference 7.0-4) embody the rigorous application of the technical specification screening criteria to shutdown modes.

SDER section 6 provides a summary of the probabilistic risk assessment (PRA) of the AP600 with regard to events that can occur at shutdown. This assessment demonstrates the low risk associated with the AP600 during shutdown operations.

In addition to this report, responses have been provided to a series of RAIs that requested Westinghouse to address compliance to specific portions of NUREG-1449. These RAIs are summarized in Table 7-1.

This section closes out *Draft Safety Evaluation Report* (Reference 7.0-5) open item tracking system (OITS) item 944. In addition, the response to RAI 440.56 (Reference 7.0-6) closes out *Draft Safety Evaluation Report* OITS item 2292.

7.0.1 References

7.0-1 NUREG-1449, *Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States*, Final Report, September 1993.

7.0-2 DCP/WMS0331, "RAI Management Review," RAI 440.53, July 29, 1994.

7.0-3 *AP600 Standard Safety Analysis Report.*

7.0-4 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

Table 7-1
Additional RAIs Relating to NUREG-1449

RAI	NUREG-1449 Section	Subject
440.55	6.7	Temporary RCS Boundaries
440.56	6.6, 7.3	Instrumentation Available During Shutdown
440.58	6.5, 7.3	Technical Specifications
440.71	2	Industr Operating Experiences
440.72	5.2	Compliance with Generic Letter 88-17

7.0-5 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

7.0-6 NTD-NRC-94-4264, RAI 440.56, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," August 12, 1994.

8.0 SUMMARY OF AP600 SHUTDOWN EVALUATION RESULTS AND CONCLUSIONS

This section summarizes the closure of open items and design changes brought about by the AP600 shutdown evaluations. This summary for closure supports the conclusion provided in section 8.3 of this *AP600 Shutdown Evaluation Report* (SDER).

8.1 CLOSURE OF OPEN ITEMS

This section includes a summary for closure of *Draft Safety Evaluation Report* (Reference 8.1-1) open item tracking system (OITS) open items and completion of request for additional information (RAI) responses related to the AP600 shutdown concerns addressed in this SDER.

943 - To resolve this item, the response to RAI 440.53 (Reference 8.1-2) refers to the SDER. In addition, this RAI is referenced in SDER section 7.0.

944 - Responses to RAIs 440.54 through 440.72 and 440.168 (refer to Reference 5.2-6, subsection 5.2.1 of this report) were issued and provide adequate technical information.

1612 - A discussion in SDER subsection 4.1.2 demonstrates that the AP600 analysis codes, as validated by testing programs, can be relied upon to accurately represent shutdown conditions in the AP600.

2053 - This item is closed with SDER section 5.0 (technical specifications), SDER section 6.0 (shutdown risk), and SDER section 4.0 (events that initiate at shutdown).

2255 - This item is closed with SDER section 4. Section 4 presents the results of accidents that can occur from shutdown modes including LOCAs postulated to occur from Mode 4, safe shutdown.

2256 - This item is closed with SDER subsection 4.10.2.

2291 - This item is addressed in SDER section 2.1.

2292 - This was addressed in the response to RAI 440.56 and is referenced in the NUREG-1449 (Reference 8.1-3) discussion included in SDER section 7.0.

2293 - This item is addressed in the response to RAI 440.24 (Reference 2.1-3) and is discussed in SDER section 2.1.

2294 - This item is closed with SDER section 4, which presents the design basis analyses of events that can occur from shutdown modes.

2295 - This item is closed with the submittal of SDER subsection 4.8.5.

2296 - This item is closed with the submittal of SDER subsection 4.8.5.

2297 - This item was previously closed. Remaining concerns are addressed by open item 2291.

2298 - This was addressea in the *AP600 Standard Safety Analysis Report* (SSAR) Technical Specifications (Reference 8.1-4) as discussed in SDER section 5.0.

2299 - This item is addressed in the reactor coolant system (RCS) system description, SDER section 2.1.

2300 - This item was addressed in the Technical Specifications as discussed in SDER section 5.0.

2303 - This fire protection question is addressed in SDER subsection 6.2.4.

2304 - This was addressed in the Emergency Response Guidelines (ERGs) (Reference 8.1-5) as mentioned in SDER section 3.3.

2305 - This item is addressed in SDER section 2.1.

2306 - This item was addressed in the Technical Specifications and is mentioned in SDER section 5.0.

2308 - This item is addressed in containment SDER section 2.7.

2309 - This item is addressed in shutdown risk SDER section 6.1.

2939 - This item is addressed in SDER section 2.1.

3007 - This item is closed with the submittal of section 4.8.5.

3441 - RAI 280.12 and closure of item 9.5.1.6-1 in NSD-NRC-96-4755 (Reference 8.1-7) are addressed in SDER subsection 6.2.4.

3960 - See discussion regarding rapid boron dilution in SDER subsection 4.10.3. This item is resolved with issuance of RAI 440.120, revision 1 (Reference 8.1-8).

4185 - Same as OITS item 2053; see SDER section 5.2.

4524 - This item is closed with WCAP-14837, Revision 1 (Reference 8.1-9).

8.1.1 References

8.1-1 Draft NUREG-1512, *Draft Safety Evaluation Report*, November 1994.

8.1-2 NSD-NRC-97-5062 (DCP/NRC0809), "AP600 Shutdown Evaluation Report and RAI 440.53," April 11, 1997.

8.1-3 NUREG-1449, *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States*, Final Report, September 1993.

8.1-4 *AP600 Standard Safety Analysis Report*, Chapter 16, "Technical Specifications."

8.1-5 NSD-NRC-97-4936 (DCP/NRC0702), *Submittal of AP600 Emergency Response Guidelines*, Revision 2, January 10, 1997.

8.1-6 NSD-NRC-96-4680 (DCP/NRC0487), "Westinghouse Responses to NRC Requests for Additional Information on the AP600," April 1, 1996.

8.1-7 NSD-NRC-96-4755 (DCP/NRC0539), "Evaluation of Low Flow DNB Data of the Modified V5H/IFM Fuel for AP600," June 24, 1996.

8.1-8 NSD-NRC-97-5126 (DCP/NRC0864), "Revised Response to RAI 440.120 for Rapid Boron Dilution Scenarios," May 14, 1997.

8.1-9 NSD-NRC-97-5164 (DCP/NRC 0897), "Submittal of WCAP-14837 Revision 1 and Response to NRC Shutdown Risk Assessment Question 23 Received 1/21/97," June 6, 1997.

8.2 SUMMARY OF CHANGES TO THE SSAR

Pursuant to the AP600 shutdown evaluation documented in this SDER, changes are being made to various SSAR sections and their source documents. These changes are summarized in Table 8.2-1.

Table 8.2-1
AP600 SSAR Changes Based on the SDER

Change	Description	Design Change Implementation
1	The power division for the RCS hot leg 1 level instrument was changed from power division A (24-hour battery) to C (72-hour battery) because the shutdown ERGs include monitoring of the hot leg level to determine the status of shutdown safety.	SSAR appendix 9A, revision 11
2	The safeguards actuation signal can be blocked only after the RCS boron concentration is increased to the cold shutdown (200°F) boron concentration. This provides for maintaining shutdown margin following a steamline break in lower modes.	SSAR chapter 16.1, T.S. 3.3.2, next revision of AP600 Technical Specifications
3	The CMT actuation signal can be blocked only after the pressurizer level is reduced to below the P-12 setpoint. The previous requirement was that it will not be blocked when a visible level exists in the pressurizer. The revised logic will allow the plant to be drained to mid-loop without actuating the CMTs.	SSAR chapter 16.1, T.S. 3.3.2, next revision of AP600 Technical Specifications
4	The block of CVS isolation on high-2 pressurizer level is changed from P-11 (pressurizer pressure) to a new function based on RCS pressure (P-19). The previous requirement made the signal available above P-11 (low pressurizer pressure interlock). However, this would not provide adequate protection from inadvertent CVS makeup pump operation in Modes 3 and 4 while the RCS is being cooled by the steam generators. Once the RNS is aligned, this signal can be disabled because the RNS LTOP relief valve provides the required protection.	SSAR chapter 16.1, T.S. 3.2.2, next revision of AP600 Technical Specifications
5	CVS letdown isolation on low-1 RCS hot leg level to maintain RCS inventory was incorporated into the SSAR.	SSAR chapter 7, revision 11
6	A block of IRWST actuation on low-2 RCS hot leg level is added to avoid inadvertent IRWST actuation at power due to instrument failures. This block is automatic when the block of CMT actuation on low pressurizer level (P-12) is enabled as pressurizer water level is restored.	SSAR chapter 7, revision 12, and SSAR chapter 16.1, T.S. 3.2.2, next revision of AP600 Technical Specifications
7	CMT actuation on first-stage ADS actuation was added. This addresses inadvertent ADS actuated by spurious failures in the PMS during shutdown modes, after the low RCS pressure and low RCS temperature actuation signals have been blocked.	SSAR chapter 7, revision 12, and SSAR chapter 16.1, T.S. 3.2.2, next revision of AP600 Technical Specifications
8	The fourth-stage ADS valves are actuated on low (empty) hot leg level during reduced inventory operations. This signal was added to increase the reliability of the AP600 during shutdown.	SSAR chapter 7, revision 13, and SSAR chapter 16.1, T.S. 3.2.2, next revision of AP600 Technical Specifications

8.3 CONCLUSION

To support the *AP600 Final Safety Evaluation Report*, the *AP600 Shutdown Evaluation Report* provides a systematic evaluation of the AP600 during shutdown operations. As demonstrated in this report, the AP600 is designed to mitigate all design basis events that can occur during shutdown modes. In addition, the risk of core damage as a result of an accident that may occur during shutdown has been demonstrated to be acceptably low. This report serves as the single-source reference to address the various AP600 shutdown safety and shutdown risk issues, including those referred to in NRC RAIs.