Westinghouse

Westinghouse Electric Company
Nuclear Plant Projects
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-5355
Direct fax: 412-374-5456
e-mail: corletmm@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP/NRC1623

September 9, 2003

SUBJECT: Transmittal of Westinghouse Document, WCAP-15985 Revision 2, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," dated August 2003

Attached please find Revision 2 of WCAP-15985, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process." This report has been revised consistent with the Westinghouse Response to Open Item 20.7-2 from the AP1000 Draft Safety Evaluation Report that was transmitted to the NRC in Westinghouse letter DCP/NRC1598 dated June 23, 2003. This report contains no Westinghouse proprietary information.

Please contact me at 412-374-5355 if you have any questions concerning this submittal.

Very truly yours,

M. M. Corletti
Passive Plant Projects & Development
AP600 & AP1000 Projects

/Attachment
WCAP-15985, Revision 2, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," dated August 2003

D063

WCAP-15985, Revision 2

"AP1000 Implementation of the Regulatory Treatment of

Nonsafety-Related Systems Process"

dated August 2003

Westinghouse Non-Proprietary Class 3

WCAP-15985
Revision 2

August 2003

AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process

Westinghouse

AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____ S _____

RFS#: _____ RFS ITEM #: _____

AP1000 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
APP-GW-GL-026	2	Page 1 of 111	W–R. P. Vijuk

ALTERNATE DOCUMENT NUMBER: WCAP-15985, Revision 2 WORK BREAKDOWN #:

ORIGINATING ORGANIZATION: Westinghouse Electric Company LLC

TITLE: **AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: Class 3 change to incorporate Draft Safety Evaluation Report Open Item Response 20.7-2.
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
6123r2.doc	Microsoft Word	

(C) WESTINGHOUSE ELECTRIC COMPANY LLC - 2003

☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC 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)

ORIGINATOR T. L. Schulz	SIGNATURE/DATE T. L. Schulz 8/25/03	
REVIEWERS	SIGNATURE/DATE	
INDEPENDENT VERIFIER M. M. Corletti	SIGNATURE/DATE M. M. Corletti 8/22/03	VERIFICATION METHOD
AP1000 RESPONSIBLE MANAGER R. P. Vijuk	SIGNATURE* R. P. Vijuk	APPROVAL DATE 8/25/03

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

WCAP-15985
Revision 2

AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process

Terry Schulz

August 2003

AP1000 Document: APP-GW-GL-026

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2003 Westinghouse Electric Company LLC
All Rights Reserved

TABLE OF CONTENTS

LIST OF TABLES v

LIST OF FIGURES vii

EXECUTIVE SUMMARY ix

1 INTRODUCTION 1-1

2 PROBABILISTIC RISK ASSESSMENT EVENT MITIGATION EVALUATION 2-1
- 2.1 EVALUATION 2-1
- 2.2 RESULTS 2-1
- 2.3 UNCERTAINTY 2-2

3 PROBABILISTIC RISK ASSESSMENT INITIATING EVENT FREQUENCY EVALUATION 3-1
- 3.1 MAIN STEAM LINE STUCK OPEN SAFETY VALVE 3-2
- 3.2 REACTOR COOLANT SYSTEM LEAK 3-3
- 3.3 LOSS-OF-COOLANT ACCIDENTS 3-3
- 3.4 SECONDARY SIDE BREAKS 3-4
- 3.5 TRANSIENTS 3-5
- 3.6 ANTICIPATED TRANSIENT WITHOUT SCRAM 3-7
- 3.7 MISCELLANEOUS SPECIAL INITIATORS 3-8
- 3.8 SHUTDOWN LOSS-OF-COOLANT ACCIDENT 3-8
- 3.9 SHUTDOWN LOSS OF OFFSITE POWER 3-9
- 3.10 SHUTDOWN LOSS OF DECAY HEAT REMOVAL 3-10
- 3.11 REACTOR COOLANT SYSTEM OVERDRAIN 3-10
- 3.12 SUMMARY 3-11

4 ANTICIPATED TRANSIENT WITHOUT SCRAM (10 CFR 50.62) 4-1
- 4.1 EVALUATION 4-1
- 4.2 CONCLUSION 4-1

5 LOSS OF ALL AC POWER (10 CFR 50.63) 5-1
- 5.1 EVALUATION 5-1
- 5.2 CONCLUSION 5-1

6 POST-72-HOUR ACTIONS 6-1
- 6.1 EVALUATION 6-1
- 6.2 CONCLUSION 6-2

7 CONTAINMENT PERFORMANCE 7-1
- 7.1 EVALUATION 7-1
- 7.2 CONCLUSION 7-1

TABLE OF CONTENTS (cont.)

8 ADVERSE SYSTEMS INTERACTION 8-1
8.1 EVALUATION 8-1
8.2 CONCLUSION 8-1

9 SEISMIC CONSIDERATIONS 9-1
9.1 EVALUATION 9-1
9.2 CONCLUSION 9-1

10 MISSION STATEMENTS AND PROPOSED REGULATORY OVERSIGHT RECOMMENDATIONS 10-1
10.1 IMPORTANT NONSAFETY-RELATED STRUCTURES, SYSTEMS, AND COMPONENTS 10-1
10.1.1 Probabilistic Risk Assessment Event Mitigation 10-1
10.1.2 Probabilistic Risk Assessment Initiating Event Frequency 10-1
10.1.3 Probabilistic Risk Assessment Uncertainty 10-3
10.1.4 Anticipated Transient Without Scram (10 CFR 50.62) 10-3
10.1.5 Loss of All AC Power (10 CFR 50.63) 10-3
10.1.6 Post-72-Hour Actions 10-3
10.1.7 Containment Performance 10-3
10.1.8 Adverse Systems Interaction 10-4
10.1.9 Seismic Considerations 10-4
10.2 MISSION STATEMENTS 10-4
10.2.1 Instrumentation Systems 10-4
10.2.2 Plant Systems 10-4
10.2.3 Electrical Systems 10-6
10.3 PROPOSED REGULATORY OVERSIGHT RECOMMENDATIONS 10-7
10.3.1 Instrumentation Systems 10-7
10.3.2 Plant Systems 10-8
10.3.3 Electrical Systems 10-14
10.4 DIVERSE ACTUATION SYSTEM MANUAL CONTROL TECHNICAL SPECIFICATION 10-60

LIST OF TABLES

Table 1 Summary List of Investment Protection Short-Term Availability Controls xi

Table 1-1 Nonsafety-Related Systems Evaluated in AP1000 RTNSS Process 1-4

Table 2-1 Systems and Functions Credited in Focused PRA Sensitivity Study 2-5

Table 2-2 PRA Results for Baseline and Focused PRA Sensitivity Study 2-6

Table 3-1 Initiating Event Criteria Application 3-12

Table 10-1 List of Investment Protection Short-Term Availability Controls 10-16

Table 10-2 Investment Protection Short-Term Availability Controls 10-17

Table 10-3 Technical Specifications 10-61

LIST OF FIGURES

Figure 1-1 RTNSS Process Evolution 1-7

Figure 1-2 AP1000 RTNSS Process Implementation 1-8

Figure 3-1 Evaluation of Impact of Nonsafety-Related Structures, Systems, and Components on Initiating Event Frequency 3-13

EXECUTIVE SUMMARY

Westinghouse has submitted an application for Final Design Approval and Design Certification of the AP1000 standard plant under the provisions of 10 CFR Part 52. The AP1000 standard plant design is based closely on the AP600 standard plant, which received Final Design Approval in 1998 and Design Certification in 1999. In SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," the Nuclear Regulatory Commission (NRC) set forth policy regarding those systems in passive light water reactors that are designated nonsafety-related, but may have a significant role in accident and consequence mitigation. Westinghouse resolved the regulatory treatment of nonsafety systems (RTNSS) policy issue for AP600 Design Certification by its submittal of WCAP-13856, "AP600 Implementation of the Regulatory Treatment of Nonsafety-Related System Process," Revision 1. The NRC documented its review and approval of the RTNSS policy issue for the AP600 in Chapter 22 of NUREG-1512, "Final Safety Evaluation Report Related to Certification of the AP600 Standard Design." The RTNSS in the AP1000 is closely modeled after the regulatory treatment of nonsafety systems for the AP600. The basis for selecting risk-important nonsafety systems for the AP600 was reevaluated for the AP1000 in this assessment. This report provides the resolution of the RTNSS policy issue for the AP1000 and contains a similar scope and content as WCAP-13856.

The RTNSS in advanced reactor passive plant designs has a wide-ranging effect on both the design and licensing of the AP1000. Unlike the current generation of light water reactors, the AP1000 uses passive safety systems that rely exclusively on natural forces such as density differences, gravity, and stored energy to provide water for core and containment cooling. These passive systems do not include active equipment such as pumps. One-time alignment of safety-related valves actuates the passive safety-related systems using valve operators such as dc motor-operators with power provided by Class 1E batteries, air-operators that reposition to the safeguards position on a loss of the nonsafety-related compressed air that keeps the safety-related equipment in standby, or check valves that operate by the pressure differential across the valve disc. The operation of the safety-related passive systems does not require ac electrical power. For the AP1000, the active systems are designated as nonsafety-related systems except for limited portions of the systems that provide safety-related isolation functions, such as containment isolation.

In current operating plants, many of these active systems provide the accident mitigation capability credited in the Design Control Document (DCD). As a result, they are classified as safety-related systems. However, for AP1000, the active systems do not provide accident mitigation capability credited in the Chapter 15 licensing design basis accident analyses unless their operation makes the consequences of an accident more limiting. As a result, they are not classified as safety-related systems.

The nonsafety-related active systems in the AP1000 provide defense-in-depth functions and supplement the capability of the safety-related passive systems. Thus, the NRC and industry have defined a process to evaluate the importance of the nonsafety-related systems and for maintaining appropriate regulatory oversight, as necessary, of these active systems in the AP1000. This process of identifying regulatory oversight on nonsafety-related systems is referred to as RTNSS.

The AP1000 RTNSS evaluation closely follows the process used for the AP600. The significant nonsafety-related structures, systems, and components (SSCs) identified for the AP600 are retained for

the AP1000. In addition, a similar evaluation process to that performed for the AP600 was used to determine if any additional SSCs were identified for the AP1000 as RTNSS important.

The RTNSS process summarized in this report includes three parts:

- Identification of the significant nonsafety-related SSCs
- Development of specific reliability/availability missions for the significant nonsafety-related SSCs
- Specification of proposed regulatory treatment for each of the missions developed

The RTNSS evaluation was performed in the following probabilistic and deterministic areas:

- Probabilistic risk assessment (PRA) event mitigation evaluation
- PRA initiating event frequency evaluation
- Anticipated transient without scram (ATWS) (10 CFR 50.62)
- Loss of all ac power (10 CFR 50.63)
- Post-72-hour actions
- Containment performance
- Adverse interactions with the AP1000 safety-related systems
- Seismic considerations

The results of the RTNSS evaluation of the AP1000 confirmed that portions of several nonsafety-related systems identified in the AP600 RTNSS evaluation are RTNSS important for the AP1000 and should have additional regulatory oversight. This includes selected manual Diverse Actuation System (DAS) controls that should have additional regulating oversight in the form of technical specifications because of PRA accident mitigation (refer to section 2.1). It also includes the systems listed in Table 1 along with the basis for their importance.

Section 10 of this report provides the proposed regulatory oversight recommendations, including short-term availability controls where appropriate. Section 10.4 includes an additional Technical Specification that was identified by the AP1000 RTNSS evaluation.

Table 1 Summary List of Investment Protection Short-Term Availability Controls

Structures, Systems, and Components	Number Trains [a]	MODES Operations [b]	Basis [c]
1.0 Instrumentation Systems			
1.1 DAS ATWS mitigation	2	1	(B,C)
1.2 ESF actuation	2	1,2,3,4,5,6 (3)	(B)
2.0 Plant Systems			
2.1 RNS	1	1,2,3	(B)
2.2 RNS – RCS open	2	5,6 (2,3)	(C)
2.3 CCS – RCS open	2	5,6 (2,3)	(C)
2.4 SWS – RCS open	2	5,6 (2,3)	(C)
2.5 PCS water makeup – long-term shutdown	1	1,2,3,4,5,6	(F)
2.6 MCR cooling – long-term shutdown	1	1,2,3,4,5,6	(F)
2.7 I&C room cooling – long-term shutdown	1	1,2,3,4,5,6	(F)
2.8 Hydrogen ignitors	1	1,2,5,6 (2,3)	(B)
3.0 Electrical Power Systems			
3.1 AC power supplies	1	1,2,3,4,5	(B)
3.2 AC power supplies – RCS open	(1)	5,6 (2,3)	(C)
3.3 AC power supplies – long-term shutdown	1	1,2,3,4,5,6	(F)
3.4 DC power supplies – DAS	2	1,2,3,4,5,6 (3)	(B,D)

Alpha Notes:

(a) Refers to the number of trains covered by the availability controls.
(b) Refers to the MODES of plant operation where the availability controls apply.
(c) Refers to the RTNSS evaluation that identified the SSC as RTNSS important.

Notes:

(1) Two of three AC power supplies (two standby diesel generators and one offsite power supply).
(2) MODE 5 with RCS open.
(3) MODE 6 with upper internals in place and cavity level less than full.

Basis Notes:

(A) PRA accident mitigation; see section 2.1.
(B) PRA uncertainty; see section 2.3.
(C) PRA initiating event frequency; see section 3.
(D) ATWS Rule, 10 CFR 50.62; see section 4.
(E) Loss all ac power rule, 10 CFR 50.63; see section 5.
(F) Post-72-hour actions; see section 6.
(G) Containment performance; see section 7.
(H) Adverse systems interactions; see section 8.
(I) Seismic considerations; see section 9.

Definitions:

CCS = Component Cooling Water System
DAS = Diverse Actuation System
ESF = Engineered Safety Feature
I&C = Instrumentation and Control
MCR = Main Control Room
PCS = Passive Containment Cooling System
RCS = Reactor Coolant System
RNS = Normal Residual Heat Removal System

1 INTRODUCTION

This report summarizes the evaluation performed to determine the significant nonsafety-related structures, systems, and components (SSCs) for the AP1000 and the appropriate additional regulatory oversight associated with these SSCs. This evaluation is consistent with the process agreed to between the industry and the Nuclear Regulatory Commission (NRC) on May 20, 1993, documented in SECY-95-132, and also with the process used for the AP600 (WCAP-13856, Revision 1).

Figure 1-1 depicts the evolution of the process documented in the SECY paper to assess the importance of nonsafety-related SSCs. Figure 1-2 depicts this process as it was implemented on the AP1000. Table 1-1 lists the nonsafety-related AP1000 systems evaluated in the regulatory treatment of nonsafety-related systems (RTNSS) process.

This summary report relies on the AP1000 Probabilistic Risk Assessment (PRA) and Design Control Document (DCD) as supporting documentation. The PRA report provides information concerning the development of the PRA, including methodology, assumptions, models, quantifications, and results. The DCD provides information for the AP1000 nonsafety-related SSCs, including drawings, system descriptions, and system functions.

Various AP1000 nonsafety-related SSCs are classified as Equipment Class D. Equipment Class D is defined by NRC Regulatory Guide 1.26 as an intermediate, nonsafety-related equipment classification, with specific AP1000 criteria based on SSC functions. This equipment class is part of a comprehensive, graded-classification process used for AP1000 mechanical, electrical, and instrumentation and control equipment, as described in section 3.2 of the DCD.

This document summarizes the RTNSS process used to evaluate the nonsafety-related SSCs. The specific detailed results, such as the supporting PRA quantified results, are included in the PRA report.

The RTNSS process summarized in this report includes three parts:

- Identification of the significant nonsafety-related SSCs
- Development of specific reliability/unavailability missions for the significant nonsafety-related SSCs
- Specification of proposed regulatory treatment for each of the missions developed

The first step in the process is to identify the significant nonsafety-related SSCs. The AP1000 nonsafety-related systems were evaluated against criteria in the following probabilistic and deterministic areas to identify the significant nonsafety-related SSCs:

- Probabilistic
  - PRA event mitigation evaluation
  - PRA initiating event frequency evaluation

- Deterministic
  - Anticipated transient without scram (ATWS) rule (10 CFR 50.62)
  - Loss of all ac power rule (10 CFR 50.63)
  - Post-72-hour actions
  - Containment performance
  - Adverse interactions with the AP1000 safety-related systems
  - Seismic considerations

Section 2 of this report summarizes the evaluation of the importance of nonsafety-related SSCs with respect to their PRA event mitigating capabilities. A PRA sensitivity study (focused PRA) has been performed in the AP1000 PRA with the nonsafety-related systems failed. Quantified results are included in Chapter 50 of the PRA report. This focused PRA sensitivity study calculates core damage frequency (CDF) and large release frequency (LRF) assuming nonsafety-related SSCs fail to mitigate at-power events. The objective of this PRA mitigation evaluation is to show that without credit for nonsafety-related SSCs in mitigating events, the AP1000 can meet the NRC safety goal for CDF and also meet the LRF goal. In addition, uncertainties in the PRA are considered in selecting RTNSS important nonsafety-related SSCs.

Section 3 of this report summarizes the evaluation of the importance of nonsafety-related SSCs with respect to the PRA initiating event frequencies. Since the focused PRA sensitivity study was performed using the baseline PRA at-power initiating event frequencies, an evaluation was performed to identify those nonsafety-related systems important to the PRA initiating event frequencies.

Section 4 summarizes an evaluation of the functions relied upon to comply with 10 CFR 50.62 (ATWS rule).

Section 5 summarizes an evaluation of the functions relied upon to comply with 10 CFR 50.63 (loss of all ac power rule).

Section 6 summarizes the evaluation of the post-72-hour actions. Although event scenarios that result in an extended loss of both offsite and onsite ac power sources for 72 hours or longer are very unlikely, this potential is considered in the AP1000 design. As part of this process, the post-72-hour actions have been evaluated to identify installed, nonsafety-related SSC functions relied upon in the AP1000 design.

Section 7 summarizes the evaluation of the SSCs needed to meet the containment performance goal (SECY-93-087, issue I.J), including containment bypass, during severe accidents.

Section 8 summarizes the evaluation of the potential for the nonsafety-related SSCs to adversely interact with the safety-related systems.

Section 9 summarizes the evaluation of nonsafety-related SSCs with respect to seismic considerations.

Section 10 provides concise reliability/unavailability mission statements for those nonsafety-related SSC functions identified as important by the evaluations described in sections 2 through 9. Section 10 also provides proposed regulatory oversight corresponding to each system mission. The proposed regulatory

oversight includes consideration for short-term availability controls. Long-term availability considerations are not provided in the recommendations from this evaluation since long-term availability considerations will be addressed in the plant-specific implementation of the maintenance rule. In addition, section 10.3 includes an additional Technical Specification identified by the AP1000 RTNSS evaluation.

Table 1-1 Nonsafety-Related Systems Evaluated in AP1000 RTNSS Process

Annex/Aux Building Nonradioactive Ventilation
Auxiliary Steam Supply

Cathodic Protection
Central Chilled Water
Chemical and Volume Control
Circulating and Service Water Chemical Injection
Circulating Water
Closed Circuit TV
Communications
Component Cooling Water
Component and Instrument Air
Condensate Polishing
Condensate
Condenser Air Removal
Condenser Tube Cleaning
Containment Air Filtration
Containment Leak Rate Test
Containment Recirculation Cooling
Cooling Tower

Data Display and Processing
Demineralized Water Transfer and Storage
Demineralized Water Treatment
Diesel Generator Building Ventilation
Diverse Actuation

Excitation and Voltage Regulation

Fire Protection
Fuel Handling and Refueling

Gaseous Radwaste
Generator Hydrogen and CO_2
Gland Seal
Gravity and Roof Drain Collection
Grounding and Lightning Protection

Table 1-1 (cont.) Nonsafety-Related Systems Evaluated in AP1000 RTNSS Process

Health Physics and Hot Machine Shop HVAC
Heater Drain
Hot Water Heating
Hydrogen Seal Oil
In-core Instrumentation
Liquid Radwaste
Main AC Power
Main and Startup Feedwater
Main Generation
Main Steam
Main Turbine and Generator Lube Oil
Main Turbine Control and Diagnostics
Main Turbine
Mechanical Handling
Meteorological and Environmental Monitoring
Non-Class 1E DC and UPS
Normal Residual Heat Removal
Nuclear Island Nonradioactive Ventilation
Onsite Standby Power
Operation and Control Centers
Plant Control
Plant Gas
Plant Lighting
Plant Security
Potable Water
Primary Sampling
Pump House Ventilation

Table 1-1 (cont.) Nonsafety-Related Systems Evaluated in AP1000 RTNSS Process

Radiation Monitoring
Radioactive Waste Drain
Radiologically Controlled Area Ventilation
Radwaste Building HVAC
Raw Water
Sanitary Drainage
Secondary Sampling
Security Lighting
Seismic Monitoring
Service Water
Solid Radwaste
Special Monitoring
Special Process Heat Tracing
Spent Fuel Pit Cooling
Standby Diesel and Auxiliary Boiler Fuel Oil
Stator Cooling
Steam Generator
Storm Drainage
Transmission Switchyard and Offsite Power
Turbine Building Closed Cooling Water
Turbine Building Ventilation
Turbine Island Chemical Feed
Turbine Island Vents, Drains and Relief
Waste Water

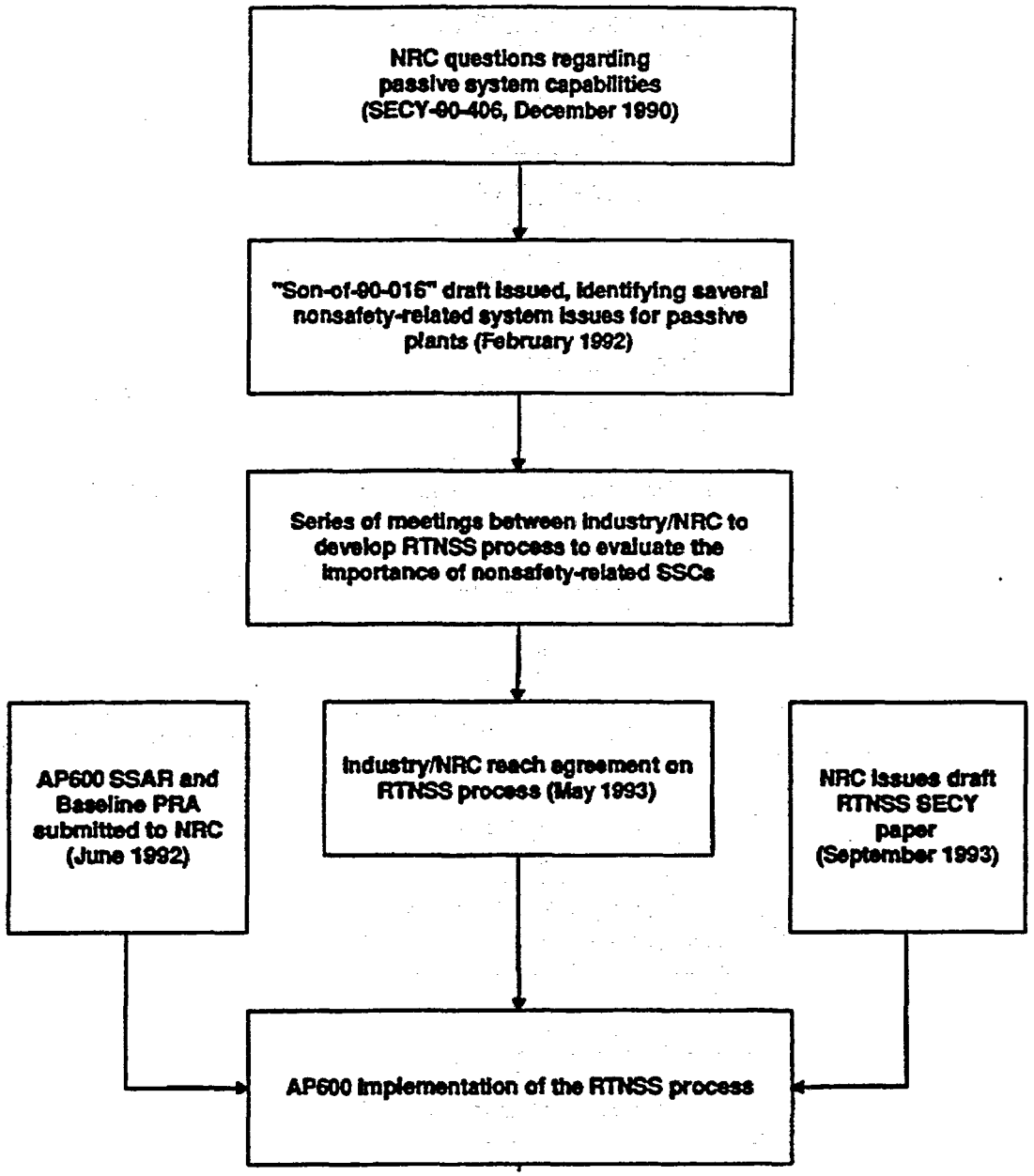

Figure 1-1 RTNSS Process Evolution

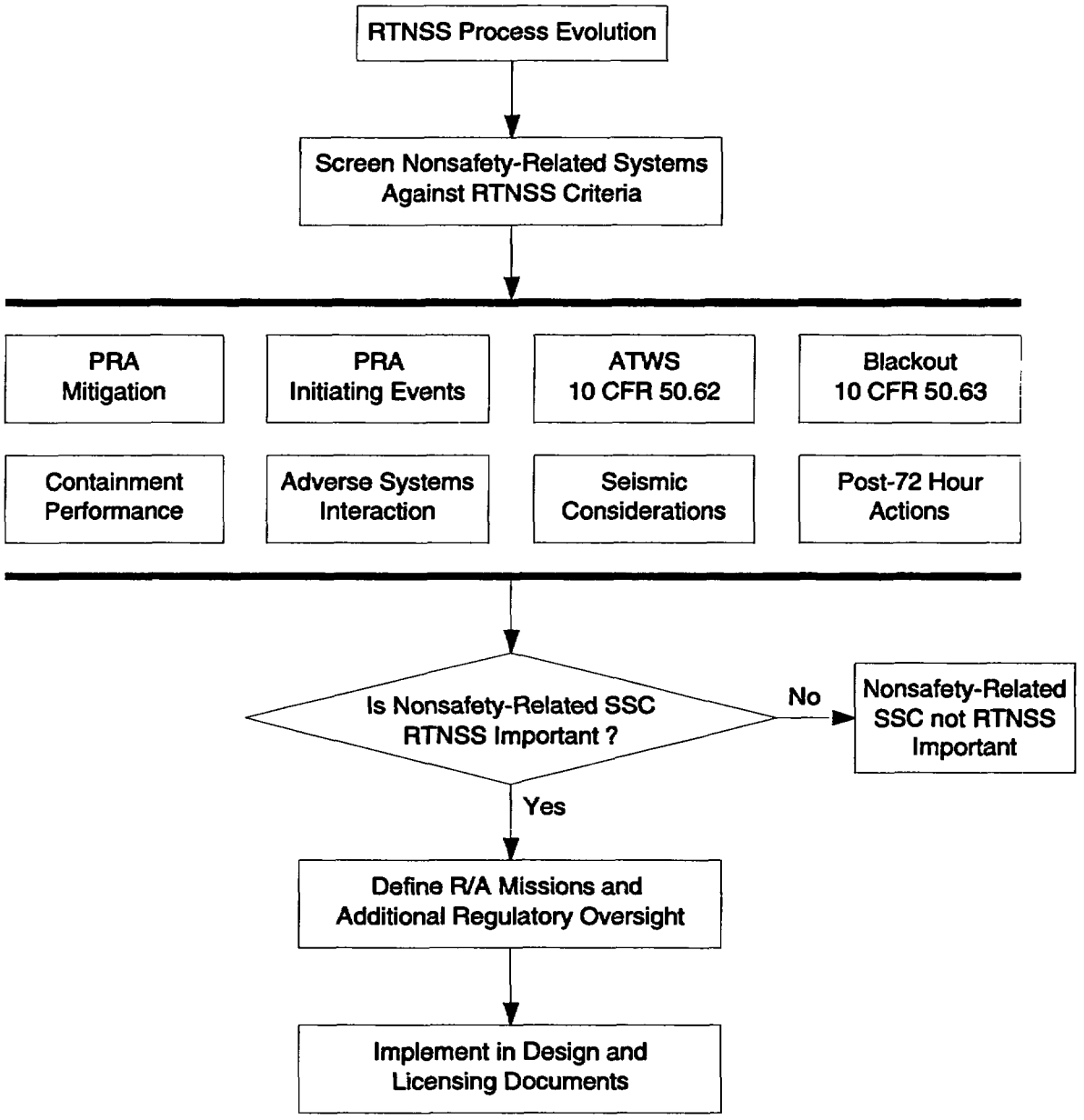

Figure 1-2 AP1000 RTNSS Process Implementation

2 PROBABILISTIC RISK ASSESSMENT EVENT MITIGATION EVALUATION

PRA sensitivity studies were performed to quantify the importance of nonsafety-related systems in mitigating PRA events. These sensitivity studies, referred to as the focused PRA sensitivity study, calculate the CDF and LRF without reliance on nonsafety-related SSC mitigation. Nonsafety-related SSCs are considered not important for PRA mitigation if the resulting CDF is less than the NRC safety goal of 1×10^{-4} events per year and the resulting LRF is less than 1×10^{-6} per year. If nonsafety-related SSC mitigation functions are relied upon in the focused PRA sensitivity study to meet the safety goals, they will be assigned reliability/unavailability missions as appropriate and will be subject to additional regulatory oversight.

The focused PRA sensitivity study is based on the AP1000 baseline PRA. It includes an evaluation of internal events that occur at-power. Internal fire and flood events are not included in this evaluation because the AP1000 PRA quantification has shown them to have a much lower risk. Seismic margins are used to evaluate seismic events (section 9).

For the focused PRA sensitivity study, the initiating event frequencies remain the same as in the baseline PRA. The mitigation functions of the nonsafety-related systems are failed, and then the CDF and LRF are calculated. If the CDF and LRF calculated in this focused PRA sensitivity study are acceptable and no mitigation credit is taken for nonsafety-related SSCs, then no additional regulatory oversight is necessary for the nonsafety-related SSCs.

Table 2-1 lists the AP1000 nonsafety-related systems modeled in the baseline PRA and assumed to fail to provide mitigation. Table 2-1 also contains a list of the safety-related systems modeled in the PRA.

2.1 EVALUATION

The focused PRA sensitivity study is performed using the same methodology as the baseline PRA. In the quantification of the CDF and LRF, the failure probability of each nonsafety SSC is set to 1. The focused PRA sensitivity study for CDF and LRF is described in Chapter 50 of the AP1000 PRA report. In addition, the improvement to these results, due to crediting manual Diverse Actuation System (DAS) controls, was estimated by evaluating the cutsets associated with these results.

2.2 RESULTS

The PRA CDF and LRF – with assumed failure of the nonsafety-related mitigation functions of the nonsafety-related SSCs – are reported in Chapter 50 of the AP1000 PRA report. Summary results from the focused PRA sensitivity studies for CDF and LRF are also found in Table 2-2.

Table 2-2 shows that use of the focused PRA sensitivity study results in an LRF that is higher than the safety goal. This result is caused by using more conservative assumptions in the focused PRA sensitivity studies for AP1000 than were used for AP600. The main difference is that AP600 assumed that all initiating events had loss of offsite AC power, whereas AP1000 assumed that offsite power was available for all events except for loss of offsite power (LOOP). As a result, the Protection and Safety Monitoring

System (PMS) is required to actuate passive safety features, such as the rods, PRHR heat exchanger (PRHR HX), and containment isolation. By crediting the manual DAS controls, the LRF as well as the CDF are reduced so that the PRA safety goals are met.

As a result, the following DAS manual controls need to be credited for PRA mitigation:

- Reactor trip
- PRHR HX and in-containment refueling water storage tank (IRWST) gutter valves
- Core makeup tank (CMT) isolation valves
- Automatic Depressurization System (ADS) stages 1, 2, 3, and 4
- IRWST injection isolation valves
- Containment recirculation isolation valves
- PCS water drain valves
- Containment isolation valves

Since the DAS manual controls are credited to meet the LRF safety goal, it was concluded that these DAS manual controls should be included in the AP1000 Technical Specifications. (See section 10.4 for a draft of the DAS manual control Technical Specification.)

2.3 UNCERTAINTY

For resolving the RTNSS issue with the NRC, several additional nonsafety-related SSCs are designated as RTNSS-important. These additional SSCs are selected using insights from the AP1000 PRA to compensate for potential uncertainties identified by the NRC. These areas of potential uncertainty include the following:

- Thermal/hydraulic uncertainty – The thermal/hydraulic calculations used to justify the PRA success criteria may have uncertainty. Some low-margin, high-risk accident sequences have been identified for both short-term and long-term conditions. These low-margin, high-risk sequences include large loss-of-coolant accidents (LOCAs), direct vessel injection (DVI) line breaks, and long-term cooling. A thermal/hydraulic uncertainty evaluation was performed as described in the AP1000 PRA, Appendix A. The result of the evaluation confirms that the majority of the success criteria specified in the AP1000 PRA for passive-only accident sequences leads to successful core cooling, even when conservatisms consistent with design basis methodology are applied. The effect of thermal/hydraulic uncertainty on the PRA is small. In the PRA sensitivity study without nonsafety SSC mitigation, total CDF and LRF remain within the goals established in SECY-94-084.

- Equipment failure rate uncertainty – The equipment failure rates used for the PXS check valves (IRWST injection, containment recirculation), squib valves (ADS stage 4, IRWST injection, containment recirculation), and reactor trip breakers may have more uncertainty than other equipment. An uncertainty analysis was performed for equipment failure rates, human error probabilities, and initiating event frequencies. The results of the uncertainty analysis are reported in AP1000 PRA Chapter 51. The result of the uncertainty analysis confirmed that the results are within the required safety goals.

- Initiating event frequency uncertainty – The large pipe break LOCA and the steam generator tube rupture (SGTR) initiating event frequencies may have more uncertainty than other events. The uncertainty with the large LOCA frequency is a result of events that have occurred in operating plants; these events have affected portions of the RCS that operate at or near the hot-leg temperature. Since hot-leg-side large LOCAs are much less severe, the success criteria used in the PRA is overly conservative for these breaks. For example, the spurious LOCA (ADS stage 4) is a large hot-leg LOCA that requires only one accumulator. Another factor is the use of Inconel 600 in welds. The AP1000 uses Inconel 690, which is recognized to be much less susceptible to cracking.

  The SGTR frequency is based on plant operating experience from more recent plants using steam generators with similar design features and materials.

  As a result, neither of these uncertainties is considered significant enough to warrant compensation by the addition of short-term availability controls.

- Hydrogen standing flames uncertainty – In case of a core damage with failure of all ADS stage 4 valves, there was a concern with the ability of the AP600 containment to withstand standing hydrogen flames located at the IRWST vents. For the AP600, Westinghouse performed analysis that showed that the containment could withstand such flames. To address potential certainty with this analysis for the AP1000, Westinghouse has introduced design features that prevent such flames from being located close to the containment. These design features are safety-related spring-loaded dampers on the IRWST vents located close to the containment and no spring loading on the IRWST vents located well away from the containment. As a result, the vents located close to the containment will not open during such a serve accident and any standing flames would be located well away from the containment.

The objective of this PRA uncertainty evaluation is to determine which nonsafety-related SSCs should be identified to compensate for the PRA uncertainties. The approach is to identify SSCs that directly compensate for the uncertainty. It is recognized that for some of these uncertainties, there are no nonsafety-related SSCs that can directly compensate for these uncertainties. In such situations, margin is provided in the PRA by adding regulatory oversight on nonsafety-related SSCs that improve the PRA sensitivity study results for other sequences. For example, there are no nonsafety-related SSCs that can improve the PRA sensitivity study results associated with DVI line breaks. During a DVI line break, the Normal Residual Heat Removal System (RNS) injection flow spills out the break and does not inject water into the RCS. Providing short-term availability controls on a system such as the DAS for ATWS events is a way to add margin to the PRA sensitivity study by improving the overall PRA sensitivity study results, even though it does not add margin to DVI line break events.

The result of this PRA uncertainty evaluation is that a few additional nonsafety-related SSCs are designated as RTNSS-important to add margin to compensate for these potential uncertainties. The nonsafety-related SSCs in the AP600 designated by this process include the following:

- Automatic DAS ATWS and engineered safety feature (ESF) actuation (provides margin for reactor trip breaker uncertainty, thermal/hydraulic analysis uncertainty, and for PMS software

uncertainty). The Technical Specification added for DAS manual controls (Table 10-3) provides additional margin.

- RNS injection capability (provides margin for ADS stage 4 squib valves, IRWST injection/containment recirculation check and squib valve reliability uncertainty, and long-term cooling thermal/hydraulic analysis uncertainty)

- Onsite ac power supplies (provide margin for ADS/IRWST injection/containment recirculation valve reliability certainty, and long-term cooling thermal/hydraulic uncertainty)

- Hydrogen ignitors (provide margin for uncertainty in hydrogen burn consequences)

Section 10 provides a list of the RTNSS-important SSCs, a description of the functions they perform, and the proposed short-term availability control regulatory oversight for these SSCs. Note that the short-term availability controls, identified for these RTNSS-important SSCs in Table 10-2, indicate that an availability of 90 percent is expected for these functions during the specified MODES considering both maintenance unavailability and failures.

Table 2-1 Systems and Functions Credited in Focused PRA Sensitivity Study
Nonsafety-Related Systems and Functions Failed in Focused PRA Sensitivity Study
• Chemical and Volume Control System (CVS) • Normal Residual Heat Removal System (RNS) • Startup Feedwater System (SFWS) • Main AC Power System (ECS) (diesel only) • Diverse Actuation System (DAS) • Hydrogen ignitors
Safety-Related Systems and Functions Credited in Focused PRA Sensitivity Study
• Passive Core Cooling System (PXS) – IRWST injection/containment recirculation – Core makeup tank (CMT) – Accumulator – Passive residual heat removal (PRHR) – Automatic depressurization • Passive Containment Cooling (PCS) • Containment Isolation • Class 1E DC and UPS System (IDS) • Protection and Safety Monitoring System (PMS) • Steam Generator Isolation

Table 2-2 PRA Results for Baseline and Focused PRA Sensitivity Study

	AP1000[1]	AP1000[2]
CDF, At-Power, Internal		
Baseline	2.4E-7	2.4E-7
Focused	7.4E-6	2.1E-6
CDF, Shutdown, Internal		
Baseline	1.2E-7	1.2E-7
Focused	1.2E-6	9.7E-7
CDF, Total Internal		
Baseline	3.6E-7	3.6E-7
Focused	8.6E-6	3.1E-6
Safety goal	1.0E-4	1.0E-4
LRF, At-Power, Internal		
Baseline	1.9E-8	1.9E-8
Focused	5.2E-6	4.3E-7
LRF, Shutdown, Internal		
Baseline	2.0E-8	2.0E-8
Focused	6.9E-7	3.8E-7
LRF, Total Internal		
Baseline	4.0E-8	3.9E-8
Focused	5.9E-6	7.7E-7
Safety goal	1.0E-6	1.0E-6

Notes:

1. Assumes NNS SSCs in Table 2-1 fail.
2. Assumes NNS SSCs in Table 2-1 fail, except for manual DAS controls listed in section 2.2.

Definitions:

N/A = not applicable

NNS = non-nuclear safety

3 PROBABILISTIC RISK ASSESSMENT INITIATING EVENT FREQUENCY EVALUATION

An evaluation was performed to study the importance of the nonsafety-related systems to the initiating event frequencies used for shutdown and at-power initiating event frequencies in the AP1000 PRA.

The initiating events identified in the PRA were reviewed for the impact of nonsafety-related system unavailability. The assessment of the importance of nonsafety-related SSCs on initiating event frequency is based on the specific PRA methodologies used to calculate the initiating event frequencies.

For evaluating the importance of the nonsafety-related SSC unavailability to the calculation of initiating event frequency, the baseline PRA initiating events were categorized by the PRA methodology used to calculate the initiating event frequencies. Eleven categories of initiating events were identified for at-power and shutdown conditions. A brief discussion of the initiating event frequency calculational methodology for each category is provided to assist in understanding the process used to determine the importance of nonsafety-related SSC reliability on the initiating event frequency. The specific categories are listed below along with the section of this report that evaluates the importance of the nonsafety-related SSCs:

- At-power initiating events

  3.1 – Main Steam Line Stuck Open Safety Valve
  3.2 – Reactor Coolant System Leak
  3.3 – Loss-of-Coolant Accidents
  3.4 – Secondary Side Breaks
  3.5 – Transients
  3.6 – Anticipated Transient Without Scram
  3.7 – Miscellaneous Special Initiators

- Shutdown initiating events

  3.8 – Shutdown Loss-of-Coolant Accident
  3.9 – Shutdown Loss of Offsite Power
  3.10 – Shutdown Loss of Decay Heat Removal
  3.11 – Reactor Coolant System Overdrain

The initiating events and the associated initiating event frequencies calculated in the baseline PRA are provided in Chapter 2 of the AP1000 PRA. As discussed in Chapter 2 of the AP1000 PRA, the initiating event frequencies were determined using several different methodologies.

The evaluation of the importance of the nonsafety-related SSC unavailability to the initiating event frequency requires identifying appropriate criteria for use in determining the importance of the nonsafety-related SSCs. The following three criteria were developed for use in the evaluation:

Criterion 1 Are nonsafety-related SSCs considered in the calculation of the initiating event frequency?

Criterion 2 Does the unavailability of the nonsafety-related SSCs significantly affect the calculation of the initiating event frequency?

Criterion 3 Does the initiating event significantly affect CDF and LRF for the PRA?

The criteria are applied to the individual initiating events in each of the initiating event categories. For each initiating event, if the response to any one of the three criteria is "No," then the unavailability of the nonsafety-related SSCs is not important to the calculation of initiating event frequency for the PRA. The discussions in sections 3.1 through 3.11 include the results from applying the screening criteria to the initiating events discussed in each section. Section 3.12 provides a summary of the results of the evaluation, and Table 3-1 shows the results of the criteria application. Figure 3-1 shows a diagram of the evaluation process.

The third screening criterion was developed for initiating events where nonsafety-related SSCs affect the calculation of the initiating event frequency, but the initiating event itself is not significant to the PRA from the perspective of its contribution to the CDF and the LRF. The rationale for this criterion is that a change in the nonsafety-related SSC unavailability can impact the calculated initiating event frequency, but the change does not have a significant effect on the CDF and LRF. For this screening criteria, individual initiating events with a contribution to CDF and LRF of less than approximately 10 percent are not considered to be significant.

AT-POWER INITIATING EVENTS

3.1 MAIN STEAM LINE STUCK OPEN SAFETY VALVE

A plant-specific calculation was performed to determine the initiating event frequency for spurious opening of the steam generator safety valves and power-operated relief valves. The steam generator system, including the steam generator safety valves and the power-operated relief valve block valves, are safety-related. The design of the steam generator power-operated relief valve is such that the valve itself and the closing function of the actuator are safety-related, while the valve actuator opening capability (required for this initiating event) and the required support functions (compressed air, plant control system, and dc power) are nonsafety-related. The initiating event frequency calculation implicitly includes the nonsafety-related component initiators that contribute to spurious actuation of the steam generator power-operated relief valve. Since this initiating event considers nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "Yes."

The initiating event frequency calculation considers the historical data for spurious opening of both the steam generator safety valves and the power-operated relief valve. The historical data reflects the difference in the number of safety valves per plant compared to the number of power-operated relief valves per plant. Based on a comparison of the contributions from each type of valve, the contribution from the relatively small population of power-operated relief valves is not significant when compared to the contribution from the larger population of safety valves in the historical data. Since nonsafety-related SSCs do not significantly affect the calculation of initiating event frequency, the response to Criterion 2 is "No." An additional consideration for this event is that increased unavailability of the associated nonsafety-related SSCs will reduce the reliability of the power-operated relief valves to open on demand and, therefore, reduce the initiating event frequency.

The response to Criterion 2 is "No." Therefore, the nonsafety-related SSCs associated with this event are not considered to be important with respect to their effect on this initiating event.

3.2 REACTOR COOLANT SYSTEM LEAK

For an RCS leak event, the initiating event frequency is derived from a review of historical data that identifies leaks that result in an RCS leak with an equivalent pipe diameter of less than 3/8-inch and the unavailability of the CVS to provide RCS makeup. The components considered in the portion of the RCS leak event frequency calculation related to RCS leakage are safety-related. The CVS and the associated support systems are nonsafety-related. Since this initiating event considers nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "Yes."

The effect of overall nonsafety-related system unavailability on this initiator results in a proportional change in the initiating event frequency. It is also possible to evaluate sensitivity to changes in unavailability of specific equipment and components modeled in the CVS fault tree. The initiating event frequency changes in proportion to the importance of the specific component to the overall nonsafety-related system unavailability. Based on a comparison of the probability of a leak initiator with the probability for unavailability of the CVS, the nonsafety-related SSC impact on the initiating event frequency is significant. Since the nonsafety-related SSCs significantly affect the calculation of initiating event frequency, the response to Criterion 2 is "Yes."

As shown in section 59 of the PRA, this initiating event contributes only 0.7 percent to the CDF and only 1.5 percent to the LRF. Since these contributions to CDF and LRF are well under the screening criteria, this initiating event does not significantly contribute to the CDF or LRF, the response to Criterion 3 is "No."

Therefore, the nonsafety-related CVS SSCs and other nonsafety-related SSCs (required for normal plant power operation) associated with this event are not considered to be important with respect to their effect on this initiating event.

3.3 LOSS-OF-COOLANT ACCIDENTS

For LOCA events, the initiators are caused by piping and valve leaks, breaks, and spurious opening of certain safety-related valves such as RCS safety valves or automatic depressurization system valves. The PRA methodology identifies the piping segments (or tube segments for tube rupture events) within the appropriate areas of the various systems and calculates the initiating event frequency based on a basic failure rate for these piping sections.

There are two nonsafety-related systems (RNS and CVS) identified in the LOCA events; however, all of the sections of these systems that could contain reactor coolant and potentially initiate a LOCA event use safety-related piping and components.

In addition, these piping sections have redundant safety-related isolation valves that are either normally closed during plant operation or automatically closed following LOCA events. For example, the CVS purification loop and discharge piping includes redundant letdown isolation valves and redundant

containment isolation valves to isolate leaks that initiate in this piping and to prevent leakage from lines that exit containment.

The piping sections of the nonsafety-related systems included in the initiating event frequency calculation are the same sections designed using safety-related piping as discussed previously.

Since these initiating events do not consider nonsafety-related SSCs in the calculation of the initiating event frequencies, the response to Criterion 1 is "No." Therefore, nonsafety-related SSCs are not considered to be important with respect to their effect on these initiating events.

For spurious ADS actuation events leading to a large LOCA event, the answer to the first criterion question is "Yes" since DAS is one of the means of spurious actuation. However, the answer to the second criteria question is "No" since the contribution of DAS to spurious ADS actuation is much less than that of PMS. Thus, spurious ADS actuation leading to a large LOCA is also dismissed due to the "No" response to Criterion 2.

As outlined in Chapter 2 of the PRA, the initiating event frequency for the interfacing system LOCA event is a result of the erroneous opening of RNS isolation valves. This is due to either hardware failure or operator error, in conjunction with the rupture of safety-related RNS components due to overpressurization. Since these components are safety-related and the operator errors that contribute to this initiating event have no relationship to nonsafety-related systems, the response to Criterion 1 is "No." Therefore, nonsafety-related SSCs are not considered to be important with respect to their effect on the interfacing system LOCA initiating event.

3.4 SECONDARY SIDE BREAKS

For the secondary side break events, the initiators are caused by pipe leaks and breaks. Similar to the calculation for LOCA events, the PRA methodology identifies the piping segments within the appropriate areas of the various secondary systems and calculates the initiating event frequency based on a basic failure rate for these piping sections.

The initiating event frequency calculation consists of a plant-specific analysis that includes pipe segments in several nonsafety-related systems that can be leak initiators for specific events.

In the AP1000 baseline PRA, two main steam line pipe break initiating events were identified. The following initiating events include piping segments in nonsafety-related systems, as identified below:

- Secondary side break – upstream of the main steam isolation valves or downstream of the main feedwater isolation valves

- Secondary side break – downstream of main steam isolation valves or upstream of the main feedwater isolation valves

For the two nonsafety-related systems identified for the secondary side break events listed above, the initiating event frequency calculation includes both safety-related and nonsafety-related piping sections.

Since these initiating events consider nonsafety-related SSCs in the calculation of the initiating event frequencies, the response to Criterion 1 is "Yes."

The initiating event frequencies for the main steam line break transient events are calculated considering only piping integrity for these nonsafety-related systems. Therefore, the operational unavailability of the nonsafety-related systems has no impact on the initiating event frequency. This is assuming that piping integrity is unchanged.

The integrity of this nonsafety-related piping directly affects the calculation of the initiating event frequencies. To provide conservative treatment of the nonsafety-related SSCs (piping) for these nonsafety-related systems, piping integrity is assumed to impact availability for screening against this criterion. Since nonsafety-related SSCs significantly affect the calculation of initiating event frequency, the response to Criterion 2 is "Yes."

As shown in section 59 of the PRA, the main steam line break initiating events contributes 0.4 percent to CDF and only 1.5 percent to the LRF. Since these contributions to CDF and LRF are well under the screening criteria, this initiating event does not significantly contribute to the CDF or LRF and the response to Criterion 3 is "No." Therefore, the nonsafety-related SSCs (required for normal plant power operation) associated with these events are not considered to be important with respect to their effect on these initiating events.

3.5 TRANSIENTS

The initiating event frequencies for the transient events are calculated using historical failure data. The historical data for applicable initiating events is sorted into categories for calculating the initiating event frequencies for the specific initiating events. In general, the initiating event frequency is determined based upon the number of initiating events per year from the historical data. Once the historical data used in the calculation of initiating event frequency for a specific event was identified, the historical data not applicable to the AP1000 design for a specific initiating event is not included in the initiating event frequency calculation.

For some events, the available historical database was used to calculate the initiating event frequency. These events include the following:

- Core power excursion
- Loss of RCS flow
- Loss of offsite power
- Loss of condenser
- Loss of main feedwater flow to both steam generators
- Spurious safeguards actuation

As described in Chapter 2 of the PRA, the loss of offsite power initiating event frequency is based on the frequency provided in Appendix A of the Advanced Light Water Reactor (ALWR) Utility Requirements Document (Volume III, ALWR Passive Plant, Chapter 1 Appendix A, PRA Key Assumptions and Groundrules, Electric Power Research Institute). The value provided in the ALWR Utility Requirements Document is based on historical data, which is also provided.

For other initiating events, some of the historical data was not applicable to the AP1000 design. For these events, the nonapplicable data was removed from the calculation of the initiating event frequencies. The events that included data inappropriate for the AP1000 include the following:

- Transient with main feedwater flow
  - Spurious reactor trip
  - Turbine trip
- Loss of main feedwater flow to one steam generator
- Loss of main feedwater flow to both steam generators
- Total loss of main feedwater flow
- Secondary to primary power mismatch

For example, the loss of main feedwater event data was removed to exclude events where a plant trip occurred following the loss of a single main feedwater pump. This is due to the AP1000 design that allows for continued plant operation following a loss of one main feedwater pump. For loss of main feedwater events and secondary-to-primary power mismatch events, an adjustment was made in calculating the initiating event frequencies to account for the lower number of steam generators in AP1000. Since AP1000 has two steam generators and the historical data includes data from plants that have more than two steam generators, an adjustment to the initiating event frequency is required to prevent calculation of an overly conservative initiating event frequency.

Several of the transient events have been grouped under similar transient event categories. These transients have been grouped for quantification purposes. This is possible since the plant response is identical for the group transients. For example, the spurious trip and turbine trip events are grouped under the transient with main feedwater category.

The initiating event frequencies for the seven initiating events listed above are impacted by the unavailability of various nonsafety-related SSCs. Chapter 2 of the PRA lists nonsafety-related SSCs and associated malfunctions, identified in the historical data and considered in the calculation of the AP1000 initiating event frequencies for these initiators. Since the seven initiating events consider nonsafety-related SSCs in the calculation of the initiating event frequencies, the response to Criterion 1 is "Yes."

The unavailability of the nonsafety-related SSCs impacts the number of events documented in the historical data and, therefore, contributes directly to the calculation of the initiating event frequencies. However, some of the associated nonsafety-related SSCs are more significant than others in the calculation of the initiating event frequencies. Since some nonsafety-related SSCs significantly affect the calculation of the initiating event frequencies, the response to Criterion 2 is "Yes."

As shown in section 59 of the PRA report, the CDF and LRF for these events are as follows:

	CDF (%)	LRF (%)
• Transient with main feedwater flow	1.4	7.5
• Core power excursion	0.7	0.5
• Loss of condenser	0.5	2.7
• Loss of offsite power	0.4	2.5
• Loss of main feedwater flow to both steam generators	0.4	1.7
• Loss of main feedwater flow to one steam generator	0.2	1.1
• Loss of RCS flow	0.0	0.1

As shown above, six of the seven initiating events discussed in this section have contributions to CDF and LRF that are well under the screening criteria. Since these six initiating events do not significantly contribute to the CDF or LRF, the response to Criterion 3 is "No." Therefore, the nonsafety-related SSCs associated with these events are not considered to be important with respect to the effect on these six initiating events.

As shown above, the CDF and LRF contributions for transient with main feedwater flow event do not exceed the screening criteria; however, the LRF contribution does not have so much margin to the screening criteria. As a result, this event is considered to significantly contribute to LRF. Therefore, the response to Criterion 3 is "Yes."

The responses to Criteria 1, 2, and 3 for the transient with main feedwater initiating event are "Yes." Therefore, the nonsafety-related SSCs required for normal at-power operation associated with this event are important with respect to the effect on this initiating event. Section 10 provides a list of important SSCs, the functions they perform, and the proposed regulatory oversight recommendations.

3.6 ANTICIPATED TRANSIENT WITHOUT SCRAM

As identified in Chapter 2 of the PRA, there are three ATWS initiating events considered in the CDF and LRF calculations for the PRA. The three initiating events are comprised of the following:

- ATWS precursor without main feedwater flow
- ATWS precursor with safeguards actuation
- ATWS precursor with main feedwater flow available

The calculation of the individual ATWS initiating event frequencies is outlined in Chapter 2. As can be seen from the ATWS events descriptions in subsection 2.2.4, the calculation of all three of the ATWS initiating event frequencies consider nonsafety-related SSCs. Since the ATWS initiating events consider nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "Yes."

The probability of an ATWS event is the combination of the probability of the initiating events as described in subsection 2.2.4 of the PRA and the probability of a failure of safety-related SSCs to insert control rods. The actual failure probability of the automatic and manual reactor trip is not included in the ATWS frequency calculation; however, automatic and manual reactor trip are modeled as top events in

the ATWS event trees, Chapter 4 of the AP1000 PRA report. Therefore, if either the automatic or manual reactor trip is successful, the event does not develop into an ATWS event. Since the failure of safety-related SSCs determines if an initiating event develops into an ATWS event, nonsafety-related SSCs do not significantly affect the calculation of the probability of an ATWS; the response to Criterion 2 is "No."

Since the response to Criterion 2 is "No," the nonsafety-related SSCs associated with this event are not considered to be important with respect to their effect on this initiating event.

3.7 MISCELLANEOUS SPECIAL INITIATORS

For several initiating events, plant-specific fault trees were developed and evaluated for the specified nonsafety-related systems to determine the initiating event frequencies for these events. These miscellaneous events are typically referred to as special initiators, and they include the following:

- Loss of CCS/service water
- Loss of compressed and instrument air

Since the plant response to the loss of service water or CCS is the same, the initiating event frequencies are combined under the same initiating event category.

Since these initiating events consider nonsafety-related SSCs in the calculation of the mitigating event frequencies, the response to Criterion 1 is "Yes."

The unavailability of these nonsafety-related systems completely determines the initiating event frequency of the associated special initiator. For example, if the overall CCS unavailability increases by a specified amount, the initiating event frequency directly increases by this same amount. Since nonsafety-related SSCs significantly affect the calculation of these initiating event frequencies, the response to Criterion 2 is "Yes."

As shown in section 59 of the PRA, these two events contribute 0.4 percent to CDF and only 1.2 percent to the LRF. Since these contributions to CDF and LRF are well under the screening criteria, this initiating event does not significantly contribute to the CDF or LRF and the response to Criterion 3 is "No."

Since the response to Criterion 3 is "No," the nonsafety-related SSCs (required for normal plant power operation) associated with these events are not considered to be important with respect to their effect on these four initiating events.

SHUTDOWN INITIATING EVENTS

3.8 SHUTDOWN LOSS-OF-COOLANT ACCIDENT

For the shutdown LOCA event, as with the at-power LOCA events, the initiators are caused by piping leaks and breaks, with one exception. As discussed in Chapter 54, the PRA methodology identifies the pipe segments and calculates the initiating event frequency based on a basic failure rate for these pipe segments. The shutdown evaluation considers a number of additional RNS pipe segments in containment

that are not included in the at-power calculation (almost three times as many pipe segments). For the shutdown LOCA event, the RNS is assumed to be the source of the LOCA. The RNS piping is safety-related. Therefore, no nonsafety-related SSCs are considered in the calculation of the initiating event frequency from piping breaks or leaks.

An additional mechanism that contributes to the initiating event frequency is included in the calculation of the initiating event frequency for shutdown LOCAs. The calculation includes the potential for inadvertent operator opening of the RNS discharge valve(s) to the IRWST. This mechanism reduces the RCS inventory by diverting flow from the shutdown cooling flowpath. This operator error in this initiating event mechanism has no relationship to nonsafety-related SSCs.

The piping sections for the nonsafety-related RNS included in the initiating event frequency calculation are designed using safety-related piping. The potential for the operator to erroneously initiate a loss of RCS inventory is not related to the unavailability of nonsafety-related SSCs. Since this initiating event does not consider nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "No." Therefore, nonsafety-related SSCs are not considered to be important with respect to their effect on this initiating event.

3.9 SHUTDOWN LOSS OF OFFSITE POWER

A calculation was completed to determine the initiating event frequency for the loss of offsite power during shutdown conditions. The calculation uses the initiating event frequency for this event from the historical data with an adjustment for the length of time spent in shutdown conditions. The calculation considers effects from onsite nonsafety-related systems, such as the transmission switchyard and the main ac power systems, as well as the offsite power system. Since this initiating event considers nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "Yes."

A review of the historical data used in the calculation of initiating event frequency for this event shows that the contribution from onsite nonsafety-related SSCs – such as transformers, high-voltage switchyard circuit breakers, or the main ac power circuit breakers – are significant to the calculation of the initiating event frequency. Since nonsafety-related SSCs significantly affect the calculation of initiating event frequency, the response to Criterion 2 is "Yes."

As seen from Table 55-4 of the PRA, the contributions to CDF for this event during RCS drained conditions is about 14.1 percent, which is well over the screening criteria. Since this initiating event contributes to the CDF, the response to Criterion 3 is "Yes."

The responses to Criteria 1, 2, and 3 for this initiating event are "Yes." Since the responses to all three criteria are "Yes," the nonsafety-related SSCs (required to provide offsite power during shutdown RCS drained conditions) associated with this event are important with respect to their effect on this initiating event. Section 10 provides a list of important SSCs, the functions they perform, and the proposed regulatory oversight recommendations.

3.10 SHUTDOWN LOSS OF DECAY HEAT REMOVAL

A plant-specific fault tree was developed and evaluated to determine the initiating event frequency for two initiating events that represent a loss of decay heat removal during shutdown conditions. The two initiating events include the loss of decay heat removal capability due to failure of the RNS and the loss of decay heat removal capability due to failure of the CCS or Service Water System (SWS). The evaluation for a loss of decay heat removal during shutdown is provided in Chapter 54 of the PRA report. This initiating event results from the loss of a nonsafety-related system normally used to provide decay heat removal during shutdown conditions. The nonsafety-related SSCs considered in this evaluation include the RNS, the CCS, and the SWS. Since this initiating event considers nonsafety-related SSCs in the calculation of the initiating event frequency, the response to Criterion 1 is "Yes."

The unavailability of these nonsafety-related systems significantly affects the initiating event frequency. Since nonsafety-related SSCs significantly affect the calculation of these initiating event frequencies, the response to Criterion 2 is "Yes."

As seen from Table 54-4 of the AP1000 PRA report, these events occurring during RCS drained conditions contribute 68.5 percent for loss of component cooling water/service water and 9.3 percent for loss of RNS to CDF. As a result, they are important contributors to the CDF. Since this initiating event contributes significantly to the CDF, the response to Criterion 3 is "Yes."

The responses to Criteria 1, 2, and 3 for this initiating event are "Yes." Since the responses to all three criteria are "Yes," the nonsafety-related SSCs (required for decay heat removal during plant shutdown conditions with reduced RCS inventory) associated with this event are considered to be important with respect to their effect on this initiating event. Section 10 provides a list of important SSCs, the functions they perform, and the proposed regulatory oversight recommendations.

3.11 REACTOR COOLANT SYSTEM OVERDRAIN

For the RCS overdrain event, two scenarios have been identified where this accident could occur. The first scenario is a combination of the failure of the hot-leg level instruments and operator failure to recognize that the hot-leg level instruments have failed. Scenario two is the combination of a failure of the valves CVS-V045 and CVS-V047 to close on the receipt of a closure signal, in conjunction with an operator failure to recognize that the valves have not closed and manually isolate the valves. The failure mechanisms for these two scenarios are detailed in Chapter 2 of the PRA.

The SSCs considered in the RCS overdrain event include the hot-leg level instruments, valves CVS-V045 and CVS-V047, and the PMS to actuate the components. Since these SSCs are safety-related and the operator errors that contribute to this initiating event have no relationship to nonsafety-related systems, the response to Criterion 1 is "No."

The response to Criterion 1 is "No." Therefore, nonsafety-related SSCs are not considered to be important with respect to their effect on this initiating event.

3.12 SUMMARY

The results of the screening criteria application for each initiating event category are provided in Table 3-1. Section 10 provides a list of important SSCs, the functions they perform, and the proposed regulatory oversight recommendations for nonsafety-related SSCs that impact the calculation of the baseline PRA initiating event frequencies, based on the initiating event criteria application.

Table 3-1 Initiating Event Criteria Application

Initiating Event Category	Criterion 1 Are nonsafety-related SSCs considered in the calculation of the initiating event frequency?	Criterion 2 Does the unavailability of the nonsafety-related SSCs significantly affect the calculation of the initiating event frequency?	Criterion 3 Does the initiating event significantly affect CDF and LRF for the baseline PRA?
3.1 Main steam line stuck open safety valve	Yes	No	N/A
3.2 RCS leak	Yes	Yes	No
3.3 LOCAs	No	N/A	N/A
3.4 Secondary side breaks	Yes	Yes	No
3.5 Transient with main feedwater flow	Yes	Yes	Yes
Other transients	Yes	Yes	No
3.6 ATWS	Yes	No	N/A
3.7 Miscellaneous special initiators	Yes	Yes	No
3.8 Shutdown LOCA	No	N/A	N/A
3.9 Shutdown loss of offsite power	Yes	Yes	Yes
3.10 Shutdown loss of decay heat removal	Yes	Yes	Yes
3.11 Shutdown RCS overdrain	No	N/A	N/A

N/A = not applicable

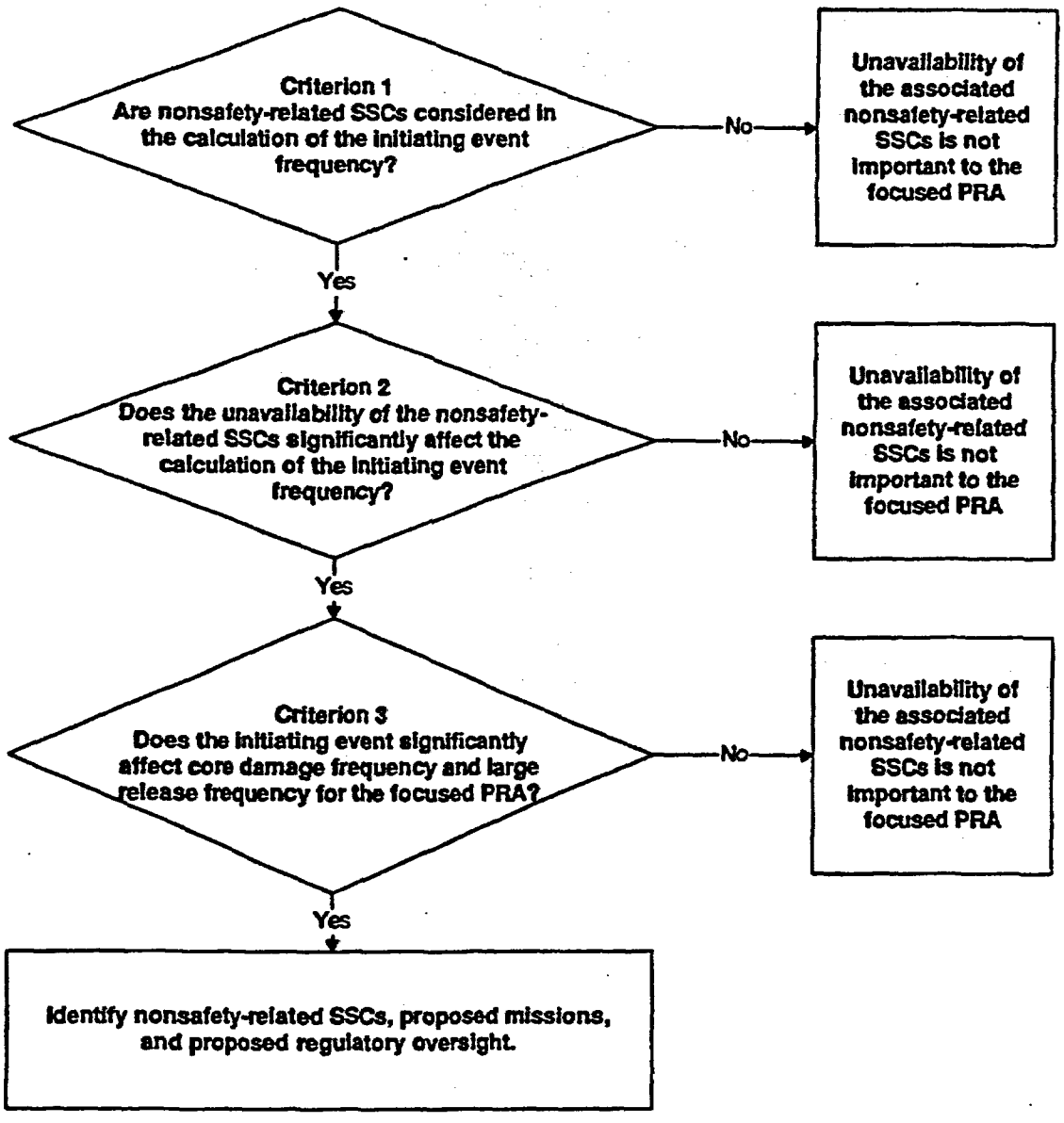

Figure 3-1 Evaluation of Impact of Nonsafety-Related Structures, Systems, and Components on Initiating Event Frequency

4 ANTICIPATED TRANSIENT WITHOUT SCRAM (10 CFR 50.62)

4.1 EVALUATION

The requirements for reduction of risks from ATWS are set forth in 10 CFR 50.62. The rule requires diverse actuation of auxiliary feedwater (for decay heat removal) and turbine trip. The AP1000 design includes a DAS, diverse from the PMS, that trips the turbine and actuates PRHR, to provide decay heat removal for AP1000. The DAS also provides reactor trip.

The DAS is nonsafety-related and powered by the non-Class 1E dc and uninterruptible power supply (UPS) system. A power supply must be provided to support the DAS functions. The non-class 1E dc and UPS system is the nonsafety-related system that supports the DAS functions needed to meet the requirements of 10 CFR 50.62.

Since the DAS relies upon power to actuate, the function of the non-class 1E dc and UPS system to provide the DAS with power is needed to meet the requirements of 10 CFR 50.62. The DAS is designed to function for at least 1 hour following loss of heating, ventilation, and air conditioning (HVAC). The DAS can perform its required functions (reactor trip, turbine trip, and PRHR actuation) before the point where environmental conditions degrade the DAS capabilities. Therefore, environmental control systems are not necessary to meet the requirements of 10 CFR 50.62.

4.2 CONCLUSION

The following nonsafety-related system functions are needed to meet the requirements of 10 CFR 50.62:

- DAS functions of reactor trip, turbine trip, and PRHR actuation functions during power operation
- Non-class 1E dc and UPS system support of the DAS and required component actuation associated with reactor trip, turbine trip, and PRHR actuation functions during power operation

The missions for these systems, along with the corresponding proposed regulatory oversight recommendations, are included in section 10 of this document.

5 LOSS OF ALL AC POWER (10 CFR 50.63)

5.1 EVALUATION

The requirements for addressing the capabilities to safely shut down a reactor following a loss of all ac power are set forth in 10 CFR 50.63.

The AP1000 design minimizes the potential risk contribution of station blackout by not requiring ac power sources for design basis events. Safety-related systems do not need nonsafety-related ac power sources to perform safety-related functions.

The AP1000 safety-related systems automatically establish and maintain safe shutdown conditions for the plant following design basis events, including an extended loss of ac power sources. The safety-related systems can maintain these safe shutdown conditions after design basis events, without operator action, following a loss of both onsite and offsite ac power sources. Therefore, no nonsafety-related SSCs are relied upon to establish and maintain safe shutdown conditions following a loss of all ac power for up to 72 hours. Section 6 provides an evaluation of the post-72-hour actions for an extended loss of ac power beyond 72 hours.

5.2 CONCLUSION

No installed nonsafety-related SSCs are relied upon to meet the requirements of 10 CFR 50.63.

6 POST-72-HOUR ACTIONS

6.1 EVALUATION

The AP1000 includes safety-related passive systems and equipment sufficient to automatically establish and maintain safe shutdown conditions for the plant following design basis events. This is assuming that the most limiting single failure occurs. The safety-related passive systems maintain safe shutdown conditions after an event without operator action, without onsite, and without offsite ac power sources.

The AP1000 includes nonsafety-related active systems and equipment designed to provide multiple levels of defense for a wide range of events. For the more probable events, these nonsafety-related systems automatically actuate to provide a first level of defense to reduce the likelihood of unnecessary actuation and operation of the safety-related passive systems. These nonsafety-related systems establish and maintain safe shutdown conditions for the plant following design basis events, provided that at least one of the standby nonsafety-related ac power sources is available.

Although event scenarios that result in an extended loss of the nonsafety-related systems, or both offsite and onsite ac power sources, for more than 72 hours are unlikely, this potential is considered in the AP1000 design.

The safety functions required following an extended loss of these nonsafety-related systems include the following:

- Core cooling, inventory, and reactivity control
- Containment cooling and ultimate heat sink
- Main control room habitability
- Post-accident monitoring
- Spent fuel pool cooling

For support of extended operation of the passive safety-related systems, the AP1000 includes both nonsafety-related onsite equipment and safety-related connections for use with transportable equipment and supplies to provide the following extended support actions:

- Provide electrical power to supply the post-accident and spent fuel pool monitoring instrumentation using the ancillary diesel generators or transportable, engine-driven ac generators that connect to safety-related electrical connections

- Provide makeup water to the passive containment cooling water storage tank to maintain external containment cooling water flow, using a PCS recirculation pump powered by an ancillary diesel generator or a transportable, engine-driven pump that connects to a safety-related makeup connection

- Provide open doors and ancillary fans for ventilation and cooling of the main control room, the instrumentation and control rooms, and the dc equipment rooms

- Provide makeup water to the spent fuel pool to maintain spent fuel cooling, using a PCS recirculation pump powered by an ancillary diesel generator or a transportable engine-driven pump that connects to a safety-related makeup connection.

These actions are accomplished by the site support personnel, in coordination with the main control room operators. These actions are performed separate from, but in parallel with, other actions taken by the plant operators to directly mitigate the consequences of an event.

6.2 CONCLUSION

In order to provide margin for events that may challenge the ability to secure offsite transportable equipment within 72 hours, the following nonsafety-related onsite equipment should be available:

- Ancillary diesel generator and ancillary diesel generator fuel oil storage tank
- PCS recirculation pump and ancillary PCS water storage tank
- Main control room ancillary fan
- Instrumentation room ancillary fan

The missions for this equipment, along with the corresponding proposed regulatory oversight recommendations, are included in section 10 of this document.

7 CONTAINMENT PERFORMANCE

7.1 EVALUATION

The SSCs relied upon to support containment performance assumptions in the baseline PRA were evaluated using the Modular Accident Analysis Program (MAAP) code as described in Chapter 44 of the AP1000 PRA report. The following containment performance criteria are identified in SECY 93-087 and used in the AP1000 PRA:

> The containment should maintain its role as a reliable, leak-tight barrier by ensuring that containment stresses do not exceed ASME service level C limits for a minimum period of 24 hours following the onset of core damage, and that following this 24-hour period the containment should continue to provide a barrier against the uncontrolled release of fission products.

The containment performance evaluation includes consideration for the following functions:

- RCS depressurization
- PXS injection
- Containment isolation
- Passive containment cooling
- Ex-vessel coolable geometry

The only nonsafety-related SSCs included in the evaluation of the containment integrity are the hydrogen igniters and the reactor vessel insulation.

The bounding evaluation performed in Chapter 41 of PRA for containment performance following hydrogen combustion shows that the AP1000 containment design is sufficient to meet the containment performance criteria without credit for the nonsafety-related hydrogen igniters. In addition, the AP1000 meets the safety margin basis. This examines the containment's ability to satisfy the structural requirements in 10 CFR 50.34(f) when subjected to the pressure and temperature loads associated with a LOCA, combined with the burning of hydrogen produced by the oxidation of 75 percent of the active cladding and without credit for the hydrogen igniters.

Water in the containment must be able to flow to the reactor vessel and steam (generated on the reactor vessel outside surface) must be vented away from the reactor vessel to support in-vessel retention of a damaged core. The AP1000 reactor vessel insulation is designed to allow this to occur.

7.2 CONCLUSION

The reactor vessel insulation design is required to support in-vessel retention.

Although not required to meet the containment performance functions, at least one hydrogen ignitor group should be available.

The missions for this equipment along with the corresponding proposed regulatory oversight recommendations are included in section 10 of this document.

8 ADVERSE SYSTEMS INTERACTION

8.1 EVALUATION

The potential adverse systems interactions considered here are those where nonsafety-related systems may adversely interact with the safety-related systems. The following three types of interactions have been addressed:

- Functional interactions
- Spatial interactions
- Human-intervention interactions

The AP1000 Adverse System Interactions Evaluation Report (WCAP-15992) summarizes the systematic and thorough approach used to evaluate the AP1000 for potential adverse system interactions. Potential adverse systems interactions, which reduce the capability or degrade the performance of the safety-related systems to perform their safety-related missions, are identified in this report.

8.2 CONCLUSION

The AP1000 Adverse System Interactions Evaluation Report documents that the AP1000 DCD and the AP1000 PRA have properly considered potential adverse system interactions. As a result, no nonsafety-related SSCs are captured by this evaluation.

9 SEISMIC CONSIDERATIONS

9.1 EVALUATION

The seismic margins analysis used to perform the AP1000 seismic evaluation does not credit nonsafety-related SSCs. SSCs relied upon to address design basis events are designed in accordance with the AP1000 seismic design criteria provided in section 3.7 of the Standard Safety Analysis Report (SSAR).

9.2 CONCLUSION

No nonsafety-related SSCs are relied upon to support the AP1000 seismic margins evaluation.

10 MISSION STATEMENTS AND PROPOSED REGULATORY OVERSIGHT RECOMMENDATIONS

Section 10.1 describes the nonsafety SSCs that were identified as RTNSS-important in Sections 2 through 9. Section 10.2 describes the RTNSS-important mission statements for these nonsafety SSCs. Section 10.3 describes the regulatory oversight recommendations for these nonsafety SSCs.

10.1 IMPORTANT NONSAFETY-RELATED STRUCTURES, SYSTEMS, AND COMPONENTS

The following are the nonsafety-related SSCs identified as important by the evaluations summarized in Sections 2 through 9 of this report.

10.1.1 Probabilistic Risk Assessment Event Mitigation

The following DAS manual controls were identified as important by this evaluation:

- Reactor trip
- PRHR HX and IRWST gutter valves
- CMT isolation valves
- ADS stages 1, 2, 3, 4
- IRWST injection isolation valves
- Containment recirculation isolation valves
- PCS water drain valves
- Containment isolation valves

10.1.2 Probabilistic Risk Assessment Initiating Event Frequency

Three initiating events are identified (in section 3) as having important, nonsafety-related SSCs. These events include transients with main feedwater available, shutdown loss of offsite power, and shutdown loss of decay heat removal.

- Transients with main feedwater available

  The evaluation of the at-power turbine trip/spurious reactor trip and loss of main feedwater transient events identifies several nonsafety-related secondary plant systems whose continuous operation during power production prevents plant trips. These nonsafety-related systems, therefore, impact the at-power turbine trip/spurious reactor trip and loss of main feedwater transient initiating event frequencies for the baseline PRA. These nonsafety-related systems include the following:

  - Main steam system

  - Main feedwater system

- Condensate system
- Main turbine
- Main turbine control and diagnostics system
- Plant control system portions that control main steam, main feedwater (including steam generator water level control subsystem), condensate, and main turbine whose malfunction can cause a reactor trip

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides an evaluation of the need for additional regulatory oversight based on the impact on the baseline PRA initiating event frequencies.

- Shutdown loss of offsite power/loss of decay heat removal

The evaluation of the shutdown loss of offsite power and loss of decay heat removal events identifies several nonsafety-related SSCs whose continuous operation during shutdown, RCS open conditions prevents a loss of shutdown decay heat removal. These nonsafety-related systems, therefore, impact the shutdown loss of offsite power and loss of decay heat removal initiating event frequencies for the baseline PRA.

The following nonsafety-related SSCs are identified as important for these two shutdown, RCS open initiating events:

- Offsite power system (only portions of the system needed to provide electrical power to onsite equipment required to support decay heat removal operation during RCS open conditions)
- Onsite standby power system (only need diesel generators as a backup source of electrical power to support decay heat removal operation during RCS open conditions)
- RNS (only portions of the system needed to provide shutdown decay heat removal during RCS open conditions)
- CCS (only portions of the system needed to support RNS shutdown decay heat removal operation during RCS open conditions)
- SWS (only portions of the system needed to support CCS system shutdown decay heat removal operation during RCS open conditions)

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides an evaluation of the need for additional regulatory oversight based on the impact on the baseline PRA initiating event frequencies.

10.1.3 Probabilistic Risk Assessment Uncertainty

The following nonsafety-related SSCs are identified as important:

- DAS ATWS and ESF actuation
- RNS injection
- Onsite AC power supplies
- Hydrogen ignitors

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides the proposed regulatory oversight recommendations for these systems.

10.1.4 Anticipated Transient Without Scram (10 CFR 50.62)

The following nonsafety-related SSCs are identified as important:

- DAS (only portions of the system needed to provide reactor trip, turbine trip, and PRHR actuation functions during power operation)

- Non-class 1E DC and UPS system (only portions of the system needed to support the DAS and required actuation components to provide reactor trip, turbine trip, and PRHR actuation functions during power operation)

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides the proposed regulatory oversight recommendations for these systems.

10.1.5 Loss of All AC Power (10 CFR 50.63)

No nonsafety-related SSCs are identified as important.

10.1.6 Post-72-Hour Actions

The following nonsafety-related SSCs are identified as important:

- PCS ancillary water makeup for containment cooling and spent fuel pool cooling
- MCR ancillary cooling
- Instrumentation room ancillary cooling
- Onsite AC ancillary power supply (to supply post-accident monitoring and above functions)

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides the proposed regulatory oversight recommendations for these systems.

10.1.7 Containment Performance

The following nonsafety-related SSC is identified as important: reactor vessel insulation (to support in-vessel retention).

Section 10.2 provides the missions for these nonsafety-related systems. Section 10.3 provides the proposed regulatory oversight recommendations for these systems.

10.1.8 Adverse Systems Interaction

No nonsafety-related SSCs are identified as important.

10.1.9 Seismic Considerations

No nonsafety-related SSCs are identified as important.

10.2 MISSION STATEMENTS

This section provides the mission statements for the nonsafety-related SSCs identified as important in the evaluations summarized in sections 2 through 9. The mission statements are grouped by type of system (instrumentation, plant, and electrical systems).

10.2.1 Instrumentation Systems

The instrumentation systems are as follows:

- DAS Manual Actuations (Focused PRA)

  The DAS provides the capability to manually actuate reactor trip and ESF functions during at-power and shutdown MODEs.

- DAS Automatic Reactor Trip (ATWS)

  The DAS provides the capability to automatically actuate reactor and turbine trip and initiate PRHR under conditions indicative of an ATWS during power operation.

- DAS Automatic Actuation of Passive Safety Features (ESF)

  The DAS provides the capability to automatically actuate passive safety-related features during at-power and shutdown MODEs.

10.2.2 Plant Systems

The plant systems are as follows:

- Miscellaneous secondary plant systems

  Continuous operation of the following nonsafety-related secondary plant systems during power production prevents plant trips:

  - Main steam system
  - Main feedwater system

- Condensate system
- Main turbine
- Main turbine control and diagnostics system
- Plant control system portions that control main steam, main feedwater (including steam generator water level control subsystem), condensate, and main turbine whose malfunction can cause a reactor trip

- RNS Low-Pressure RCS Injection

  The RNS provides low-pressure RCS injection following ADS actuation during at-power and shutdown conditions.

- RNS Shutdown Cooling

  The RNS provides shutdown decay heat removal during RCS open shutdown conditions.

- CCS

  The CCS provides cooling to support RNS shutdown decay heat removal operation during RCS open shutdown conditions. The CCS also provides cooling to support RNS injection operation following ADS actuation during at-power and shutdown conditions.

- SWS

  The SWS provides cooling to support CCS shutdown decay heat removal operation during RCS open shutdown conditions. The SWS also provides cooling to support RNS injection operation following ADS actuation during at-power and shutdown conditions.

- PCS water and spent fuel pool makeup (long-term shutdown)

  The PCS recirculation pumps provide the capability to transfer water from the PCS ancillary water storage tank to the PCS water storage tank and the spent fuel pool to support post-72-hour operation of passive safety-related SSCs. This capability is required when the decay heat of the core is sufficient to require PCS water evaporative cooling. The safety-related PCS water storage tank and the spent fuel pit provide at least 72 hours of water supply. The ancillary water storage tank provides additional water to support PCS and SFP operation from 3 days to 7 days.

- MCR cooling

  The MCR ancillary room fans provide cooling of the MCR to support post-72-hour MCR habitability during all modes of plant operation.

- Instrumentation room cooling

  The instrumentation room fans provide cooling of the 1E instrumentation rooms to support post-72-hour post-accident monitoring during all modes of plant operation.

- Hydrogen ignitors

  The hydrogen ignitors prevent combustion of hydrogen that may cause failure of the containment following a core melt with failure of all ADS stage 4 valves.

- Reactor vessel insulation

  The reactor vessel insulation supports in-vessel retention of a molten core during a severe accident by allowing water from the containment to remove heat from the reactor vessel outer surface.

10.2.3 Electrical Systems

The electrical systems are as follows:

- Onsite AC power supply

  The onsite standby power system provides a backup source of electrical power to onsite equipment needed to provide PMS actuation and to support RNS operation during at-power and shutdown conditions following a loss of offsite power.

- AC power supplies

  The offsite power system provides electrical power to onsite equipment needed to support decay heat removal operation during RCS open shutdown conditions.

- AC power supply

  The ancillary diesel generators provide power to support post-72- hour operation following at-power and shutdown events.

- Non-class 1E DC and UPS system (DAS)

  The non-class 1E DC and UPS system provides electrical power to the DAS and actuation components to actuate reactor and turbine trip and initiate PRHR under conditions indicative of an ATWS during power operation.

10.3 PROPOSED REGULATORY OVERSIGHT RECOMMENDATIONS

The proposed regulatory oversight recommendations are grouped in the same manner as the mission statements (by system type). Table 10-1 lists the nonsafety-related SSCs that have short-term availability controls. Table 10-2 contains the short-term availability controls.

10.3.1 Instrumentation Systems

The instrumentation systems are as follows:

- DAS (PRA Event Mitigation)

  A description of the following DAS manual controls is included in DCD subsection 7.7.1.11:

  - Reactor trip
  - PRHR HX and IRWST gutter valves (AOV)
  - CMT isolation valves (AOV)
  - ADS stages 1, 2, 3 (MOV), and stage 4 (squib)
  - IRWST injection isolation valves (squib)
  - Containment recirculation isolation valves (squib)
  - PCS water drain valves (AOV and MOV)
  - Containment isolation valves (AOV)
  - Hydrogen ignitors

  The AP1000 D-RAP includes the DAS in DCD Table 17.4-1. The inspection, tests, analyses, and acceptance criteria (ITAACs) are provided in subsection 2.5.1.

  Table 10-3 provides recommendations for DAS Technical Specifications covering these manual controls.

- DAS (ATWS)

  A description of the DAS is included in DCD subsection 7.7.1.11. The AP1000 D-RAP includes the DAS in DCD Table 17.4-1. ITAACs are provided in subsection 2.5.1.

  The quality assurance guidance provided in Generic Letter 85-06 is applicable to the DAS because of the ATWS mitigation functions (DCD subsection 7.7.1.11).

  Table 10-2 (item 1.1) provides recommendations for DAS short-term availability controls covering the ATWS function.

- DAS (EFS)

  A description of the DAS is included in DCD subsection 7.7.1.11. The AP1000 D-RAP includes the DAS in DCD Table 17.4-1. ITAACs are provided in subsection 2.5.1.

Table 10-2 (item 1.2) provides recommendations for DAS short-term availability controls covering the ESF actuation function.

10.3.2 Plant Systems

The plant systems are as follows:

- Reactor trip initiating event systems

  For these initiating events, the impact of nonsafety-related SSCs on the baseline PRA initiating event frequencies is identified as important. There are several factors that must be considered in evaluating the potential benefit of additional regulatory oversight to the initiating event frequencies calculated in the baseline PRA. Therefore, these factors must be considered in identifying missions for these nonsafety-related systems and developing proposed additional regulatory oversight based on these missions. The two initiating events are the following:

  - Turbine trip/spurious reactor trip
  - Loss of main feedwater

  For this discussion, the turbine trip/spurious reactor trip and loss of main feedwater transients can be grouped together as they were in the transient initiating event frequency evaluation in section 3.5.

  The responses to the three criteria for these initiating events indicate that some of the associated nonsafety-related SSCs are significant to the calculation of the initiating event frequencies and these initiating events affect the baseline PRA results. However, there are other considerations related to the nonsafety-related SSCs that contribute to the calculation of these initiating events that must be considered in deciding upon the benefit of additional regulatory oversight for these SSCs.

  The nonsafety-related SSCs contributing to the historical data for these two events in current plants are also nonsafety-related systems and perform essentially the same functions for the AP1000. These nonsafety-related systems include the following:

  - Main steam system
  - Main feedwater system
  - Condensate system
  - Main turbine
  - Main turbine control and diagnostics system
  - Plant control system portions that control main steam, main feedwater (including steam generator water level control subsystem), condensate, and main turbine whose malfunction can cause a reactor trip

The AP1000 nonsafety-related systems include various design features and improvements that help to increase system reliability and availability. There is currently regulatory oversight in the design for these nonsafety-related systems and the associated design improvements, based on the descriptions of the various systems provided in the AP1000 DCD. Examples of these design improvements and the DCD subsection that describes the specific AP1000 design features are provided below:

- Digital steam generator water level system (7.7)
- Motor-driven main feedwater pumps (10.4.7.2.2)
- Improved main feedwater regulating valve throttling control features (10.4.7.2.2)
- Elimination of main feedwater bypass control valves (10.4.7.2.2)
- No plant trip following the loss of one main feedwater pump (10.4.7.1.2)
- Full load rejection capability (10.4.4)
- Digital turbine electrohydraulic control system (10.2.2.3)

Although the nonsafety-related SSCs affect the initiating event frequencies for these two transients, there are several considerations in evaluating the need for and benefit from additional regulatory oversight for the associated nonsafety-related SSCs.

As discussed previously, the AP1000 systems, including the nonsafety-related systems listed previously, contain numerous design improvements that incorporate current regulatory oversight provided by the NRC to address various plant safety issues. The nonsafety-related systems that impact these two initiating events are required to continuously operate to support normal plant power operation. Therefore, there is strong incentive to establish and maintain reliable system performance. By providing more fault-tolerant system designs that increase plant reliability and availability, the design improvements also directly increase plant safety by reducing the potential for plant transients or trips that could present challenges to the plant.

The PRA benefit from these design improvements is not fully reflected from the perspective of the initiating event frequency calculation. As discussed in section 3.5, the accepted PRA methodology for calculating the initiating event frequencies for these two transient events is to use the available historical data for these events because the historical data is applicable to the AP1000. In calculating the initiating event frequency, it is possible to adjust the calculated initiating event frequency for some design improvements. For example, the calculation can ignore historical events where the loss of one main feedwater pump caused a plant trip. However, there is no attempt to adjust the historical data to compensate for improvements such as increased main feedwater pump or main feedwater control valve reliability. Either the events in the historical data for a component failure are included or they are not included, without consideration of whether the AP1000 component is more reliable. The calculation includes events where the loss of two or three main feedwater pumps causes a plant trip, and these events are not adjusted to account for increased AP1000 main feedwater pump reliability.

Based on this PRA methodology, the AP1000 design improvements are not fully credited in the calculation of the initiating event frequencies for these two events. The increased reliability of the AP1000 systems, when compared to the same systems in current plants, results in a conservative calculation of initiating event frequency for the AP1000 PRA. This historical data,

which conservatively bounds the calculation of initiating event frequency for these events, is based upon the current level of regulatory oversight for similar nonsafety-related SSCs in current plants.

Therefore, additional regulatory oversight for the AP1000 nonsafety-related SSCs that impact these two initiating events, beyond that provided via the DCD design details and via existing operational controls on current plants, will not provide significant benefit in reducing either the initiating event frequency, CDF, or LRF. In addition, it is not meaningful to consider additional regulatory oversight that is intended to increase the reliability of nonsafety-related systems that are normally in standby operation to nonsafety-related systems that are required to operate during power production.

The current level of regulatory oversight, including the DCD design oversight, is sufficient to ensure that the changes in unavailabilities of the nonsafety-related SSCs that impact these two specific initiating events are conservatively bounded from the perspective of calculating the baseline PRA initiating event frequency, and the resulting CDF and LRF.

Therefore, from the perspective of initiating event frequencies for the baseline PRA, the evaluation for these two initiators identify no nonsafety-related SSCs where additional regulatory oversight would significantly reduce the associated initiating event frequencies, the CDF, and the LRF. No proposed regulatory oversight recommendations have been identified for these nonsafety-related SSCs.

- Shutdown loss of offsite power

The shutdown loss of offsite power is significant only from the perspective of CDF and LRF during shutdowns with the RCS open conditions. This initiating event is not important during any of the other shutdown conditions considered in the shutdown PRA and discussed in Chapter 54 of the AP1000 PRA report.

Therefore, the missions developed for these nonsafety-related SSCs as a result of this initiating event, and any associated additional regulatory oversight recommendations, are only applicable during RCS open shutdown conditions, which represent a small percentage of the overall time spent in plant shutdown.

The responses to the three criteria for this initiating event indicate that the associated nonsafety-related SSCs are significant to the calculation of the initiating event frequency and this initiating event affects the baseline PRA results.

This initiating event is impacted by the loss of electrical power from the offsite grid sources, which is independent of onsite nonsafety-related SSCs. The initiating event is also impacted by nonsafety-related SSCs, such as the transmission switchyard system, which is site-specific and not part of the AP1000 design as described in the DCD or modeled in the PRA report. However, the onsite nonsafety-related SSCs contributing to the historical data for this event in current plants

are also nonsafety-related systems and perform essentially the same functions for the AP1000. These nonsafety-related systems include the following:

- Offsite power system equipment, including the main step-up, unit auxiliary, and reserve auxiliary transformers

- Main ac power system equipment, including the offsite power supply circuit breakers to the onsite switchgear buses

The nonsafety-related SSCs identified above are required to be in continuous operation to support shutdown plant operations during reduced RCS inventory conditions. These nonsafety-related SSCs provide electrical power to the onsite ac power system. The design and operation of these nonsafety-related SSCs are described in Chapter 8 of the AP1000 DCD.

Additionally, the operation of these nonsafety-related SSCs during RCS open shutdown operations follows industry guidelines and practices, which minimize the potential for, and enhance mitigation of, this event.

Even though not specifically required for the evaluation of initiating event frequency impact, additional regulatory oversight recommendations are also proposed for the nonsafety-related diesel-generators of the onsite standby power system. This initiating event frequency evaluation considers only nonsafety-related SSCs that impact the probability of an event occurring. From this perspective, where the failure of a site transformer can cause a loss of offsite power event, failure of a nonsafety-related diesel-generator does not initiate a loss of offsite power and availability of the diesel-generators does not prevent a loss of offsite power. Diesel-generator unavailability does impact the plant response and mitigation of this event. However, mitigation impact is not the intent of this evaluation.

In developing the proposed regulatory oversight recommendations for this event, the need for short-term availability control of the offsite power sources can benefit from credit for availability of the diesel-generators. The proposed oversight recommendations are not onerous, considering the normal plant actions expected in preparing for RCS open shutdown operations. In addition, the proposed oversight enhances plant safety during these conditions and provides flexibility by allowing for preventive or corrective maintenance that may need to be performed while in RCS open shutdown conditions, such as during special plant evolutions that are required over the lifetime of the plant.

- Shutdown loss of decay heat removal

As with the shutdown loss of offsite power, the shutdown loss of decay heat removal is significant only from the perspective of CDF and LRF during shutdowns with RCS open conditions. This initiating event is not important during any of the other shutdown conditions considered in the shutdown PRA and discussed in Chapter 54 of the AP1000 PRA report.

Therefore, the missions developed for these nonsafety-related SSCs as a result of this initiating event, and any associated additional regulatory oversight recommendations, are applicable only during RCS open shutdown conditions, which represent a small percentage of the overall time spent in plant shutdown.

The responses to three criteria for this initiating event indicate that the associated nonsafety-related SSCs are significant to the calculation of the initiating event frequencies and these initiating events affect the baseline PRA results.

This initiating event is impacted by the loss of nonsafety-related SSCs that are used to provide core decay heat removal – the RNS and its support systems.

The AP1000 includes a number of design features and improvements that help to improve plant safety by increasing shutdown decay heat removal reliability and availability. There is currently regulatory oversight in the design for these nonsafety-related systems and the associated design improvements, based on the descriptions of the various systems provided in the AP1000 DCD. A discussion of these design features and specific design improvements to support shutdown decay heat removal is included in subsection 5.4.7 of the AP1000 DCD.

There is also regulatory oversight in the operation of the shutdown decay heat removal systems through industry documents such as Generic Letters 87-12 and 88-17. Subsection 1.9.5.1 of the DCD provides the AP1000 response to the SECY-90-016 issue of midloop operation, which references the guidance provided in the generic letters.

Examples of these design improvements, which are discussed in subsection 5.4.7 and subsection 1.9.5.1 of the AP1000 DCD, include the following:

- Loop piping offset
- Hot-leg level instrumentation
- Self-venting residual heat removal pump suction line
- No residual heat removal system throttling required during midloop operation
- Capability for full RNS flow with saturated fluid conditions

The nonsafety-related systems identified above are required to be in continuous operation to support shutdown core decay heat removal during reduced RCS inventory conditions. The nonsafety-related RNS and its nonsafety-related support systems are normally available and fully operational to support the plant cooldown before entering RCS open shutdown maintenance conditions. In addition, these nonsafety-related systems are required to be available before initiating reduced RCS inventory operations during a plant shutdown. Planned maintenance for these systems will not be scheduled during RCS open shutdown conditions.

Additionally, the operation of these nonsafety-related SSCs during RCS open shutdown operations follow industry guidelines and practices, which minimize the potential for, and enhance mitigation of, this event.

- RNS

  A description of the RNS is included in DCD subsection 5.4.7. The AP1000 D-RAP includes the RNS in DCD Table 17.4-1. ITAACs are provided in subsection 2.3.6.

  Table 10-2 (item 2.2) provides recommendations for RNS short-term availability controls.

- CCS

  A description of the CCS is included in DCD subsection 9.2.2. The AP1000 D-RAP includes the CCS in DCD Table 17.4-1. ITAACs are provided in subsection 2.3.1.

  Table 10-2 (item 2.3) provides recommendations for CCS short-term availability controls.

- SWS

  A description of the SWS is included in DCD subsection 9.2.1. The AP1000 D-RAP includes the SWS in DCD Table 17.4-1. ITAACs are provided in subsection 2.3.8.

  Table 10-2 (item 2.4) provides recommendations for SWS short-term availability controls.

- PCS and spent fuel pool water makeup (long-term shutdown)

  Makeup to the PCS water supply and spent fuel pool post-72 hours is provided by the PCS recirculation pumps taking suction from the PCS ancillary water storage tank. A description of this arrangement is provided in DCD subsections 6.2.2 and 9.1.3. ITAACs are provided in DCD Tier 1 subsections 2.2.2 and 2.3.7.

  This equipment should be available following seismic and high wind events that may make procurement of offsite equipment more difficult. Therefore, as a minimum, the supports for this equipment are Seismic Category II as shown in DCD Table 3.2-3. In addition, the ancillary water storage tank (which is located outdoors) is designed and analyzed for Seismic II criteria and for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles (DCD subsection 6.2.2). Table 10-2 (item 2.5) provides recommendations for PCS water makeup short-term availability controls.

- MCR cooling (long-term shutdown)

  MCR cooling post-72 hours is provided by opening doors and using the MCR ancillary fans. A description of this cooling capability is provided in DCD subsection 9.4.1. ITAACs are provided in subsection 2.7.1.

  This equipment should be available following seismic and high wind events that may make procurement of offsite equipment more difficult. Therefore, as a minimum, the supports for this equipment are Seismic Category II as shown in DCD Table 3.2-3. In addition, this equipment is located in the auxiliary building, which is a Seismic Category I structure. This provides more

than adequate protection for Seismic II criteria and for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles (DCD subsection 9.4.1). Table 10-2 (item 2.6) provides recommendations for MCR fan short-term availability controls.

- Instrumentation room cooling (long-term shutdown)

  Instrumentation room cooling post-72 hours is provided by opening doors and using the instrumentation room ancillary fans. A description of this cooling capability is provided in DCD subsection 9.4.1. ITAACs are provided in subsection 2.7.1.

  This equipment should be available following seismic and high wind events that may make procurement of offsite equipment more difficult. Therefore, as a minimum, the supports for this equipment are Seismic Category II as shown in DCD Table 3.2-3. In addition, this equipment is located in the auxiliary building, which is a Seismic Category I structure. This provides more than adequate protection for Seismic II criteria and for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles (DCD subsection 9.4.1). Table 10-2 (item 2.7) provides recommendations for instrumentation room fan short-term availability controls.

- Hydrogen ignitors

  A description of the hydrogen ignitors is provided in DCD subsection 6.2.4. The AP1000 D-RAP includes the hydrogen ignitors in DCD Table 17.4-1. ITAACs are provided in subsection 2.3.9.

  Table 10-2 (item 2.8) provides recommendations for hydrogen ignitors short-term availability controls.

- Reactor vessel insulation

  A description of the features of the reactor vessel insulation that provide in-vessel retention of a molten core are described in DCD subsection 5.3.5. ITAACs are provided in subsection 2.2.3. Short-term availability controls are unnecessary for this passive component.

10.3.3 Electrical Systems

The electrical system are as follows:

- AC power supply system

  A description of the onsite power system is included in DCD subsection 8.3. The AP1000 D-RAP includes the onsite standby power system in DCD Table 17.4-1. ITAACs are provided in subsection 2.6.4.

  Table 10-2 (item 3.1) provides recommendations for onsite power system short-term availability controls.

- AC power supplies (RCS open)

  A description of the offsite power system is included in DCD subsection 8.2. A description of the main AC power system is included in DCD subsection 8.3.1.

  Table 10-2 (item 3.2) provides recommendations for AC power supply short-term availability controls.

- AC power supply (long-term shutdown)

  The ancillary diesel generators provide power for post-accident monitoring, PCS water makeup (recirculation pumps), MCR cooling (MCR ancillary fans), and instrumentation room cooling (instrumentation room ancillary fans). A description of the ancillary diesel generators is included in DCD subsection 8.3.1. The AP1000 D-RAP includes the ancillary diesel generators in DCD Table 17.4-1. ITAACs are provided in subsection 2.6.1.

  This equipment should be available following seismic and high wind events, which may make procurement of offsite equipment more difficult. Therefore, as a minimum, the supports for this equipment are Seismic Category II as shown in DCD Table 3.2-3. In addition, this equipment is located in a portion of the Annex Building that is a Seismic II structure. Features of this structure that protect the function of this equipment are designed and analyzed for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles (DCD subsection 8.3.1).

  Table 10-2 (item 3.3) provides recommendations for the ancillary diesel generator short-term availability controls.

- AC power supply (DAS)

  The non-class 1E dc and UPS system provides power to the DAS. A description of the non-class 1E dc and UPS system is included in DCD subsection 8.3.2. ITAACs are provided in subsection 2.6.2.

  The quality assurance guidance provided in Generic Letter 85-06 is applicable to the non-class 1E dc and UPS system because of the ATWS mitigation functions (DCD subsection 8.3.2.1.2).

  Table 10-2 (item 3.4) provides recommendations for non-class 1E dc and UPS system short-term availability controls.

Table 10-1 List of Investment Protection Short-Term Availability Controls

Structures, Systems, and Components	Number Trains [a]	MODES Operations [b]
1.0 Instrumentation Systems		
1.1 DAS ATWS mitigation	2	1
1.2 ESF actuation	2	1,2,3,4,5,6 (3)
2.0 Plant Systems		
2.1 RNS	1	1,2,3
2.2 RNS – RCS open	2	5,6 (2,3)
2.3 CCS – RCS open	2	5,6 (2,3)
2.4 SWS – RCS open	2	5,6 (2,3)
2.5 PCS and spent fuel pool water makeup – long-term shutdown	1	1,2,3,4,5,6
2.6 MCR cooling – long-term shutdown	1	1,2,3,4,5,6
2.7 I&C room cooling – long-term shutdown	1	1,2,3,4,5,6
2.8 Hydrogen ignitors	1	1,2,5,6 (2,3)
3.0 Electrical Power Systems		
3.1 AC power supplies	1	1,2,3,4,5
3.2 AC power supplies – RCS open	(1)	5,6 (2,3)
3.3 AC power supplies – long-term shutdown	1	1,2,3,4,5,6
3.4 DC power supplies – DAS	2	1,2,3,4,5,6 (3)

Alpha Notes:

(a) Refers to the number of trains covered by the availability controls.

(b) Refers to the MODES of plant operation where the availability controls apply.

Notes:

(1) Two of three AC power supplies (two standby diesel generators and one offsite power supply).

(2) MODE 5 with RCS open.

(3) MODE 6 with upper internals in place and cavity level less than full.

Table 10-2 Investment Protection Short-Term Availability Controls

1.0 Instrumentation Systems

1.1 Diverse Actuation System (DAS) ATWS Mitigation

OPERABILITY: DAS ATWS mitigation function listed in Table 1.1-1 should be operable.

APPLICABILITY: MODE 1

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. DAS ATWS Function with one or more required channels inoperable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore required channels to operable status.	14 days
B. Required Action and associated Completion Time of Condition A not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

1.0 Instrumentation Systems

1.1 Diverse Actuation System (DAS) ATWS Mitigation

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	1.1.1	Perform CHANNEL CHECK on each required channel.	30 hours
SR	1.1.2	Perform CHANNEL OPERATIONAL TEST on each required channel.	92 days
SR	1.1.3	Perform CHANNEL CALIBRATION on each required channel.	24 months
SR	1.1.4	Verify that the MG set field breakers open on demand.	24 months

Table 1.1-1 DAS ATWS Functions

DAS Function	Initiating Signal	Number Installed	Channels Required	Setpoint
Rod Drive MG Set Trip, Turbine Trip, and PRHR HX Actuation	SG Wide Range Level	2 per SG	1 per SG	> [55,000 lb]

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

1.0 Instrumentation Systems

1.1 DAS ATWS Mitigation

BASES:

The DAS ATWS mitigation function of reactor trip, turbine trip, and PRHR heat exchanger (PRHR HX) actuation should be available to provide ATWS mitigation capability. This function is important based on 10 CFR 50.62 (ATWS Rule) and because it provides margin in the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to actuate.

The DAS uses a two out of two logic to actuate automatic functions. When a required channel is unavailable the automatic DAS function is unavailable. DCD subsection 7.7.1.11 provides additional information. The DAS channels listed in Table 1.1-1 should be available.

Automated operator aids may be used to facilitate performance of the CHANNEL CHECK. An automated tester may be used to facilitate performance of the CHANNEL OPERATIONAL TEST.

The DAS ATWS mitigation function should be available during MODE 1 when ATWS is a limiting event. Planned maintenance affecting this DAS function should be performed MODES 3, 4, 5, and 6; these MODES are selected because the reactor is tripped in these MODES and ATWS cannot occur.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

1.0 Instrumentation Systems

1.2 DAS Engineering Safeguards Features Actuation (ESFA)

OPERABILITY: DAS ESFA functions listed in Table 1.2-1 should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. DAS ESFA Functions with one or more required channels inoperable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore required channels to operable status.	14 days
B. Required Action and associated Completion Time of Condition A not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

1.0 Instrumentation Systems

1.2 DAS Engineering Safeguards Features Actuation (ESFA)

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	1.2.1	Perform CHANNEL CHECK on each required CHANNEL.	30 hours
SR	1.2.2	Perform CHANNEL OPERATIONAL TEST on each required CHANNEL.	92 days
SR	1.2.3	Perform CHANNEL CALIBRATION on each required CHANNEL.	24 months

Table 1.2-1 DAS ESFA Functions

DAS Function	Initiating Signal	Number Installed	Channels Required	Setpoint
PRHR HX Actuation	SG Wide Level or	2 per SG	1 per SG	> [55,000 lb]
	HL Temp	1 per HL	1 per HL	< [625]F
CMT Actuation and RCP trip	Pzr Level	2	2	> [7]%
Passive Cont. Cooling and Selected Cont. Isolation Actuation	Cont. Temp	2	2	< [200]F

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

1.0 Instrumentation Systems

1.2 DAS ESFA

BASES:

The DAS ESFA functions listed in Table 1.2-1 should be available to provide accident mitigation capability. This function is important because it provides margin in the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to actuate.

The DAS uses a two out of two logic to actuate automatic functions. When a required channel is unavailable, the automatic DAS function is unavailable. DCD section 7.7.1.11 provides additional information. The DAS channels listed in Table 1.2-1 should be available.

Automated operator aids may be used to facilitate performance of the CHANNEL CHECK. An automated tester may be used to facilitate performance of the CHANNEL OPERATIONAL TEST.

The DAS ESFA mitigation functions should be available during MODES 1, 2, 3, 4, 5, and 6 when accident mitigation is beneficial to the PRA results. The DAS ESFA should be available in MODE 6 with upper internals in place or cavity level less than full. Planned maintenance affecting these DAS functions should be performed in MODE 6 when the refueling cavity is full; this MODE is selected because requiring DAS ESFA is not anticipated in this MODE.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.1 Normal Residual Heat Removal System (RNS)

OPERABILITY: One train of RNS injection should be operable.

APPLICABILITY: MODES 1, 2, and 3

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required train not operable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore one train to operable status	14 days
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.1 Normal Residual Heat Removal System (RNS)

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.1.1	Verify that one RNS pump develops a differential head of [330] feet on recirculation flow	92 days
SR	2.1.2	Verify that the following valves stroke open RNS V011RNS Discharge Cont. Isolation RNS V022RNS Suction Header Cont. Isolation RNS V023RNS Suction from IRWST Isolation RNS V055RNS Suction from Cask Loading Pit	92 days

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.1 RNS

BASES:

The RNS injection function provides a nonsafety-related means of injecting cask loading pit (CLP) water into the RCS following ADS actuations. The RNS injection function is important because it provides margin in the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

One train of RNS injection includes one RNS pump and the line from the CLP to the RCS. One valve in the line between the CLP and the RCS is normally closed and needs to be opened to allow injection. Later on, the RNS suction is switched from the CLP to the IRWST. Two valves in the IRWST line are normally closed and must be opened to allow recirculation. This equipment does not normally operate during MODES 1, 2, and 3. DCD subsection 5.4.7 contains additional information on the RNS.

The RNS injection function should be available during MODES 1, 2, and 3 because decay heat is higher and the need for ADS is greater.

Planned maintenance on redundant RNS SSCs should be performed during MODES 1, 2, and 3. Such maintenance should be performed on an RNS SSC not required to be available. The bases for this recommendation is that the RNS is more risk-important during shutdown MODES when it is normally operating than during other MODES when it only provides a backup to PXS injection.

Planned maintenance on nonredundant RNS valves (such as V011, V022, V023, and V055) should be performed to minimize the impact on their RNS injection and their containment isolation capability. Nonpressure boundary maintenance should be performed during MODE 5 with a visible pressurizer level or MODE 6 with the refueling cavity full. In these MODES, these valves need to be open, but they do not need to be able to close. Containment closure, which is required in these MODES, can be satisfied by one normally open operable valve. Pressure boundary maintenance cannot be performed during MODES when the RNS is used to cool the core, therefore such maintenance should be performed during MODES 1, 2, and 3. Since these valves are also containment isolation valves, maintenance that renders the valves inoperable requires that the containment isolation valve located in series with the inoperable valve has to closed and de-activated. The basis for this recommendation is that the RNS is more risk-important during shutdown MODES when it is normally operating than during other MODES when it only provides a backup to PXS injection. In addition, it is not possible to perform pressure boundary maintenance of these valves during RNS operation.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.2 Normal Residual Heat Removal System (RNS) – RCS Open

OPERABILITY: Both RNS pumps should be operable for RCS cooling.

APPLICABILITY: MODE 5 with RCS pressure boundary open,
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One pump not operable.	A.1 Initiate actions to increase the water inventory above the core.	12 hours
	AND	
	A.2 Remove plant from applicable MODES	72 hours
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

2.0 Plant Systems

2.2 Normal Residual Heat Removal System (RNS) – RCS Open

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.2.1	Verify that one RNS pump is in operation and that each RNS pump operating individually circulates reactor coolant at a flow > [900] gpm OR Verify that both RNS pumps are in operation and circulating reactor coolant at a flow > [1800] gpm	Within 1 day prior to entering the MODES of applicability

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.2 RNS – RCS Open

BASES:

The RNS cooling function provides a nonsafety-related means to normally cool the RCS during shutdown operations (MODES 4, 5, and 6). This RNS cooling function is important during conditions when the RCS pressure boundary is open and the refueling cavity is not flooded because it reduces the probability of an initiating event due to loss of RNS cooling and because it provides margin in the PRA sensitivity performed. This is assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The RCS is considered open when its pressure boundary is not intact. The RCS is also considered open if there is no visible level in the pressurizer. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The RNS cooling of the RCS involves the RNS suction line from the RCS HL, the two RNS pumps, and the RNS discharge line returning to the RCS through the DVI lines. The valves located in these lines should be open prior to the plant entering reduced inventory conditions. One of the RNS pumps has to be operating; the other pump may be operating or may be in standby. Standby includes the capability of being able to be placed into operation from the MCR. DCD subsection 5.4.7 contains additional information on the RNS.

Both RNS pumps should be available during the MODES of applicability when the loss of RNS cooling is risk-important. If both RNS pumps are not available, the plant should not enter these conditions. If the plant has entered reduced inventory conditions, then the plant should take action to restore full system operation or leave the MODES of applicability. If the plant has not restored full system operation or left the MODES of applicability within 12 hours, then actions need to be initiated to increase the RCS water level to either 20-percent pressurizer level or to a full refueling cavity.

Planned maintenance affecting this RNS cooling function should be performed in MODES 1, 2, and 3 when the RNS is not normally operating. The basis for this recommendation is that the RNS is more risk-important during shutdown MODES, especially during the MODES of applicability conditions, than during other MODES when it only provides a backup to PXS injection.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.3 Component Cooling Water System (CCS) – RCS Open

OPERABILITY: Both CCS pumps should be operable for RNS cooling.

APPLICABILITY: MODE 5 with RCS pressure boundary open,
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One pump not operable.	A.1 Initiate actions to increase the water inventory above the core.	12 hours
	AND	
	A.2 Remove plant from applicable MODES.	72 hours
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

2.0 Plant Systems

2.3 Component Cooling Water System (CCS) – RCS Open

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 2.3.1	Verify that one CCS pump is in operation and each CCS pump operating individually provides a CCS flow through one RNS heat exchanger > [2820] gpm. OR Verify that both CCS pumps are in operation and the CCS flow through each RNS heat exchanger is > [2820] gpm.	Within 1 day prior to entering the MODES of applicability

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.3 CCS – RCS Open

BASES:

The CCS cooling of the RNS HXs provides a nonsafety-related means to normally cool the RCS during shutdown operations (MODES 4, 5, and 6). This RNS cooling function is important because it reduces the probability of an initiating event due to loss of RNS cooling and because it provides margin in the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The RCS is considered open when its pressure boundary is not intact. The RCS is also considered open if there is no visible level in the pressurizer. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The CCS cooling of the RNS involves two CCS pumps and HXs and the CCS line to the RNS HXs. The valves around the CCS pumps and HXs and in the lines to the RNS HXs should be open prior to the plant entering these conditions. One of the CCS pumps and its HX has to be operating. One of the lines to a RNS HX also has to be open. The other CCS pump and HX may be operating or may be in standby. Standby includes the capability of being able to be placed into operation from the MCR. DCD subsection 9.2.2 contains additional information on the CCS.

Both CCS pumps should be available during the MODES of applicability when the loss of RNS cooling is risk-important. If both CCS pumps are not available, the plant should not enter these conditions. If the plant has entered these conditions, then the plant should take action to restore both CCS pumps or to leave these conditions. If the plant has not restored full system operation or left the MODES of applicability within 12 hours, then actions need to be initiated to increase the RCS water level to either 20-percent pressurizer level or to a full refueling cavity.

Planned maintenance affecting this CCS cooling function should be performed in MODES 1, 2, and 3 when the CCS is not supporting RNS operation. The basis for this recommendation is that the CCS is more risk-important during shutdown MODES, especially during the MODES of applicability conditions than during other MODES.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.4 Service Water System (SWS) – RCS Open

OPERABILITY: Both SWS pumps and cooling tower fans should be operable for CCS cooling.

APPLICABILITY: MODE 5 with RCS pressure boundary open,
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One pump or fan not operable.	A.1 Initiate actions to increase the water inventory above the core.	12 hours
	AND	
	A.2 Remove plant from applicable MODES.	72 hours
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.4 Service Water System (SWS) – RCS Open

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.4.1	Verify that one SWS pump is operating and that each SWS pump operating individually provides a SWS flow > [8600] gpm	Within 1 day prior to entering the MODES of applicability
SR	2.4.2	Operate each cooling tower fan for > 15 min	Within 1 day prior to entering the MODES of applicability

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.4 SWS – RCS Open

BASES:

The SWS cooling of the CCS HXs provides a nonsafety-related means to normally cool the RNS HX, which cools the RCS during shutdown operations (MODES 4, 5, and 6). This RNS cooling function is important because it reduces the probability of an initiating event due to loss of RNS cooling and because it provides margin in the PRA sensitivity performed. This is assuming no credit for nonsafety-related SSCs to mitigate shutdown events. The RCS is considered open when its pressure boundary is not intact. The RCS is also considered open if there is no visible level in the pressurizer. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The SWS cooling of the CCS HXs involves two SWS pumps and cooling tower fans and the SWS line to the RNS HXs. The valves in the SWS lines should be open prior to the plant entering these conditions. One of the SWS pumps and its cooling tower fan has to be operating. The other SWS pump and cooling tower fan may be operating or may be in standby. Standby includes the capability of being able to be placed into operation from the MCR. DCD subsection 9.2.1 contains additional information on the SWS.

Both SWS pumps and cooling tower fans should be available during the MODES of applicability when the loss of RNS cooling is risk-important. If both SWS pumps and cooling tower fans are not available, the plant should not enter these conditions. If the plant has entered these conditions, then the plant should take action to restore both SWS pumps/fans or to leave these conditions. If the plant has not restored full system operation or left the MODES of applicability within 12 hours, then actions need to be initiated to increase the RCS water level to either 20-percent pressurizer level or to a full refueling cavity.

Planned maintenance affecting this SWS cooling function should be performed in MODES when the SWS is not supporting RNS operation; that is, during MODES 1, 2, and 3. The basis for this recommendation is that the SWS is more risk-important during shutdown MODES, especially during the MODES of applicability conditions than during other MODES.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.5 Passive Containment System Water Storage Tank (PCCWST) and Spent Fuel Pool Makeup – Long-Term Shutdown

OPERABILITY: Long-term makeup to the PCCWST and the Spent Fuel Pool should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Water volume in PCS ancillary tank less than limit.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore volume to within limits.	14 days
B. One required PCS recirculation pump not operable.	B.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	B.2 Restore pump to operable status.	14 days

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

C.	Required Action and associated Completion Time of Condition A, B not met.	C.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
		AND	
		C.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.5.1	Verify water volume in the PCS ancillary tank is > [725,000] gal.	31 days
SR	2.5.2	Record that the required PCS recirculation pump provides recirculation of the PCCWST at > [100] gpm.	92 days
SR	2.5.3	Verify that each PCS recirculation pump transfers > [100] gpm from the PCS ancillary tank to the PCCWST. During this test, each PCS recirculation pump will be powered from an ancillary diesel.	10 years
SR	2.5.4	Verify that each PCS recirculation pump transfers > [100] gpm from the PCS ancillary tank to the spent fuel pool. During this test, each PCS recirculation pump will be powered from an ancillary diesel.	10 years

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

2.0 Plant Systems

2.5 PCCWST and Spent Fuel Pool Makeup – Long Term Shutdown

BASES:

The PCS recirculation pumps provide long-term shutdown support by transferring water from the PCS ancillary tank to the PCCWST and the spent fuel pool. The specified PCS ancillary water tank volume is sufficient to maintain PCS and spent fuel pool cooling during the 3- to 7-day time period following an accident. After 7 days, water brought in from offsite allows the PCCWST to continue to provide PCS cooling and makeup to the spent fuel pit. This PCCWST makeup function is important because it supports long-term shutdown operation. A minimum availability of 90 percent is assumed for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The PCCWST makeup function involves the use of one PCS recirculation pump, the PCS ancillary tank and the lines connecting the PCS ancillary tank with the PCCWST and spent fuel pool. One PCS recirculation pump normally operates to recirculate the PCCWST. DCD subsections 6.2.2 and 9.1.3 contain additional information on the PCCWST and spent fuel pool makeup function.

The PCCWST makeup function should be available during MODES of operation when PCS and spent fuel pool cooling is required; one PCS recirculation pump and PCS ancillary tank should be available during all MODES.

Planned maintenance should be performed on the redundant pump (that is, the pump not required to be available). Planned maintenance affecting the PCS ancillary tank that requires less than 72 hours to perform can be performed in any MODE of operation. Planned maintenance requiring more than 72 hours should be performed in MODES 5 or 6 when the calculated core decay heat is < 9 MWt. The basis for this recommendation is that the long-term PCS makeup for containment cooling is not required in this condition, and in most cases, the PCCWST can provide the required makeup to the spent fuel pool.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.6 Main Control Room (MCR) Cooling – Long-Term Shutdown

OPERABILITY: Long-term cooling of the MCR should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required MCR ancillary fans not operable.	A.1 Notify [chief nuclear officer] or [on-call alternate]. AND A.2 Restore one fan to operable status	72 hours 14 days
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE. AND B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 day 1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

2.0 Plant Systems

2.6 Main Control Room (MCR) Cooling – Long-Term Shutdown

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.6.1	Operate required MCR ancillary fan for > 15 min	92 days
SR	2.6.2	Verify that each MCR ancillary fan can provide a flow of air into the MCR for >15 min. During this test, the MCR ancillary fans will be powered from the ancillary diesels.	10 years

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.6 MCR Cooling – Long-Term Shutdown

BASES:

The MCR ancillary fans provide long-term shutdown support by cooling the MCR. For the first 3 days after an accident, the emergency HVAC system (VES) together with the passive heat sinks in the MCR provide cooling of the MCR. After 3 days, the MCR ancillary fans can be used to circulate ambient air through the MCR to provide cooling. The long-term MCR cooling function should be available during all MODES of operation. This long-term MCR cooling function is important because it supports long-term shutdown operation. A minimum availability of 90 percent is assumed for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The long-term MCR cooling function involves the use of an MCR ancillary fan. During SR 2.6.1, the fan will be run to verify that it operates without providing flow to the MCR. During SR 2.6.2, each fan will be connected to the MCR and operated such that it provides flow to the MCR. DCD subsection 9.4.1 contains additional information on the long-term MCR cooling function.

One MCR ancillary fan should be available during all MODES of plant operation. Planned maintenance should be performed on the redundant MCR ancillary fan (that is, the fan not required to be available) during MODES 3 or 4, MODE 5 with a visible pressurizer level, or MODE 6 with the refueling cavity full; these MODES are selected because the reactor is tripped in these MODES and the risk of core damage is low.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.7 I&C Room Cooling – Long-Term Shutdown

OPERABILITY: Long-term cooling of I&C rooms B & C should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required I&C room ancillary fan not operable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore one fan to operable status.	14 days
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

2.0 Plant Systems

2.7 I&C Room Cooling – Long-Term Shutdown

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.7.1	Operate required I&C room ancillary fan for > 15 min.	92 days
SR	2.7.2	Verify that each I&C room ancillary fan can provide a flow of air into an I&C room for >15 min. During this test, the I&C room ancillary fans will be powered from an ancillary diesel.	10 years

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.7 I&C Room Cooling – Long-Term Shutdown

BASES:

The I&C room ancillary fans provide long-term shutdown support by cooling I&C rooms B & C which, contain post-accident instrument processing equipment. For the first 3 days after an accident, the passive heat sinks in the I&C rooms provide cooling. After 3 days, the I&C room ancillary fans can be used to circulate ambient air through the I&C room to provide cooling. The long-term I&C room cooling function should be available during all MODES of operation. This long-term I&C room cooling function is important because it supports long-term shutdown operation. A minimum availability of 90 percent is assumed for this function during the MODES of applicability. This is considering both maintenance unavailability and failures to operate.

The long-term I&C room cooling function involves the use of two I&C room ancillary fans; each fan is associated with one I&C room (B or C). During SR 2.6.1, the required fan will be run to verify that it operates without providing flow to the I&C room. During SR 2.6.2, each fan will be connected to its associated I&C room and operated such that flow is provided to the I&C room. DCD subsection 9.4.1 contains additional information on the long-term I&C room cooling function.

One I&C room ancillary fan should be available during all MODES of plant operation. Planned maintenance should be performed on the redundant I&C room ancillary fan (that is, the fan not required to be available) during MODES 3 or 4, MODE 5 with a visible pressurizer level, or MODE 6 with the refueling cavity full; these MODES are selected because the reactor is tripped in these MODES and the risk of core damage is low.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.8 Hydrogen Ignitors

OPERABILITY: Hydrogen ignitors should be operable in accordance with Table 2.8-1.

APPLICABILITY: MODE 1, 2,
MODE 5 with RCS pressure boundary open,
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more required hydrogen ignitor inoperable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore required ignitors to operable status.	14 days
B. Required Action and associated Completion Time of Condition A not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.8 Hydrogen Ignitors

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	2.8.1	Energize each required hydrogen ignitor, and verify the surface temperature is > [1700]°F.	Each refueling outage

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

Table 2.8-1 Hydrogen Ignitors

Location	Hydrogen Ignitors Group 1	Hydrogen Ignitors Group 2	Number Available[1]
- Reactor Cavity	(2)	(2)	na
- Loop Compartment 01	12,13	11,14	3 of 4
- Loop Compartment 02	5,8	6,7	3 of 4
- Pressurizer Compartment	49,60	50,59	3 of 4
- Tunnel connecting Loop Compartments	1,3,31	2,4,30	5 of 6
- Southeast Valve Room & Southeast Accumulator Room	21	20	2 of 2
- East Valve Room, Northeast Accumulator Room, & Northeast Valve Room	18	17,19	(3)
- North CVS Equipment Room	34	33	2 of 2
- Lower Compartment Area (CMT and Valve Area)	22,27,28,29,31, 32	23,24,25,26,30	10 of 11
- IRWST	9,35,37	10,36,38	5 of 6
- IRWST inlet	16	15	2 of 2
- Refueling Cavity	55,58	56,57	3 of 4
- Upper Compartment			
- Lower Region	39,42,43,44,47	40,41,45,46,47	9 of 10
- Mid-Region	51,54	52,53	2 of 4
- Upper Region	61,63	62,64	2 of 4

Notes:

(1) In each location, the minimum number of ignitors that should be available are defined in this column.

(2) Ignitors in this location are shared with other locations.

(3) Ignitor 18 and either 17 or 19 should be available.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

2.0 Plant Systems

2.8 Hydrogen Ignitors

BASES:

The hydrogen ignitors should be available to provide the capability of burning hydrogen generated during severe accidents to prevent failure of the containment due to hydrogen detonation. These hydrogen ignitors are required by 10 CFR 50.34 to limit the buildup of hydrogen to less than 10 percent. This is assuming that 100 percent of the active zircaloy fuel cladding is oxidized.

This function is also important because it provides margin in the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The ignitors are distributed in the containment to limit the buildup of hydrogen in local areas. Two groups of ignitors are provided in each area; one of which is sufficient to limit the buildup of hydrogen. When an ignitor is energized, the ignitor surface heats up to ≥[1700]°F. This temperature is sufficient to ignite hydrogen in the vicinity of the ignitor when the lower flammability limit is reached. DCD subsection 6.2.4 provides additional information.

The hydrogen ignitor function should be available during MODES 1 and 2 when core decay heat is high, during MODE 5 when the RCS pressure boundary is open, and during MODE 6 when the refueling cavity is not full. Planned maintenance should be performed on hydrogen ignitors when they are not required to meet this availability control. Table 2.8-1 indicates the minimum number of hydrogen ignitors that should be available.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.1 AC Power Supplies

OPERABILITY: One standby diesel generator should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, and 5

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Fuel volume in one required standby diesel fuel tank less than limit.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore volume to within limits.	14 days
B. One required fuel transfer pump or standby diesel generator not operable.	B.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	B.2 Restore pump and diesel generator to operable status.	14 days

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

C.	Required Action and associated Completion Time not met.	C.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability and schedule for restoration to OPERABLE. AND C.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 day 1 month

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	3.1.1	Verify that the fuel oil volume in the required standby diesel generator fuel tank is > [50,000] gal.	31 days
SR	3.1.2	Record that the required fuel oil transfer pump provides a recirculation flow of > [8] gpm.	92 days
SR	3.1.3	Verify that the required standby diesel generator starts and operates at > [4000] kw for > 1 hour. This test may utilize diesel engine prelube prior to starting and a warmup period prior to loading.	92 days
SR	3.1.4	Verify that each standby diesel generator starts and operates at > [4000] kw for > 24 hours. This test may utilize diesel engine prelube prior to starting and a warmup period prior to loading. Both diesel generators will be operated at the same time during this test.	10 years

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.1 AC Power Supplies

BASES:

AC power is required to power the RNS and to provide a nonsafety-related means of supplying power to the safety-related PMS for actuation and post-accident monitoring. The RNS provides a nonsafety-related means to inject water into the RCS following ADS actuations in MODES 1, 2, 3, and 4 (when steam generators cool the RCS). This AC power supply function is important because it adds margin to the PRA sensitivity performed assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability. This is considering both maintenance unavailability and failures to operate.

Two standby diesel generators are provided. Each standby diesel generator has its own fuel oil transfer pump and fuel oil tank. The volume of fuel oil required is that volume above the connection to the fuel oil transfer pump. DCD subsection 8.3.1 contains additional information.

This AC power supply function should be available during MODES 1, 2, 3, 4, and 5 when RNS injection and PMS actuation are more risk-important. Planned maintenance should be performed on redundant AC power supply SSCs during MODES 1, 2, and 3 when the RNS is not normally in operation. The bases for this recommendation is that the AC power is more risk-important during shutdown MODES, especially when the RCS is open as defined in availability control 2.2, than during other MODES.

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

3.0 Electrical Power Systems

3.2 AC Power Supplies – RCS Open

OPERABILITY: Two AC power supplies should be operable to support RNS operation.

APPLICABILITY: MODE 5 with RCS pressure boundary open,
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required AC power supply not operable.	A.1 Initiate actions to increase the water inventory above the core.	12 hours
	AND	
	A.2 Remove plant from applicable MODES.	72 hours
B. Required Action and associated Completion Time not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.2 AC Power Supplies – RCS Open

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
SR 3.2.1 Verify that the required number of AC power supplies are operable.	Within 1 day prior to entering the MODES of applicability

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.2 AC Power Supplies – RCS Open

BASES:

AC power is required to power the RNS and its required support systems (CCS and SWS); the RNS provides a nonsafety-related means to normally cool the RCS during shutdown operations. This RNS cooling function is important when the RCS pressure boundary is open and the refueling cavity is not flooded because it reduces the probability of an initiating event due to loss of RNS cooling during these conditions and because it provides margin in the PRA sensitivity performed. This is assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The RCS is considered open when its pressure boundary is not intact. The RCS is also considered open if there is no visible level in the pressurizer. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

Two AC power supplies, one offsite and one onsite supply, should be available as follows:

- Offsite power through the transmission switchyard and either the main step-up transformer/unit auxiliary transformer or the reserve auxiliary transformer supply from the transmission switchyard
- Onsite power from one of the two standby diesel generators

DCD subsection 8.3.1 contains additional information on the standby diesel generators. DCD section 8.2 contains information on the offsite AC power supply.

One offsite and one onsite AC power supply should be available during the MODES of applicability when the loss of RNS cooling is important. If both of these AC power supplies are not available, the plant should not enter these conditions. If the plant has already entered these conditions, then the plant should take action to restore this AC power supply function or to leave these conditions. If the plant has not restored full system operation or left the MODES of applicability within 12 hours, then actions need to be initiated to increase the RCS water level to either 20 percent pressurizer level or to a full refueling cavity.

Planned maintenance should not be performed on required AC power supply SSCs. Planned maintenance affecting the standby diesel generators should be performed in MODES 1, 2, and 3 when the RNS is not normally in operation. Planned maintenance of the other AC power supply should be performed in MODES 2, 3, or MODE 6 with the refueling cavity full. The basis for this recommendation is that the AC power is more risk-important during shutdown MODES, especially during the MODES of applicability conditions, than during other MODES.

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.3 AC Power Supplies – Long-Term Shutdown

OPERABILITY: One ancillary diesel generator should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Fuel volume in ancillary diesel fuel tank less than limit.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore volume to within limits.	14 days
B. One required ancillary diesel generator not operable.	B.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	B.2 Restore one diesel generator to operable status.	14 days

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

C. Required Action and associated Completion Time not met.	C.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE. AND C.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 day 1 month

SURVEILLANCE REQUIREMENTS

SURVEILLANCE			FREQUENCY
SR	3.3.1	Verify fuel volume in the ancillary fuel tank is >[600] gal.	31 days
SR	3.3.2	Verify that the required diesel generator starts and operates for >1 hour connected to a test load > [35] kw. This test may utilize diesel engine warmup period prior to loading.	92 days
SR	3.3.3	Verify that each diesel generator starts and operates for 4 hours while providing power to the regulating transformer, an ancillary control room fan, an ancillary I&C room fan, and a PCCWST recirculation pump that it will power in a long-term post-accident condition. Test loads will be applied to the output of the regulating transformers that represent the loads required for post-accident monitoring and control room lighting. This test may use diesel engine warmup prior to loading. Both diesel generators will be operated at the same time during this test.	10 years

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.3 AC Power Supplies – Long-Term Shutdown

BASES:

The ancillary diesel generators provide long term power supplies for post accident monitoring, MCR and I&C room cooling, PCS and spent fuel water makeup. For the first three days after an accident the 1E batteries provide power for post accident monitoring. Passive heat sinks provide cooling of the MCR and the I&C rooms. The initial water supply in the PCCWST provides for at least 3 days of PCS cooling. The initial water volume in the spent fuel pit normally provides for 3 days of spent fuel cooling. In some events the PCCWST and ancillary PCCWST are used to supplement the spent fuel pit. A minimum availability of 90 percent is assumed for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

After 3 days, ancillary diesel generators can be used to power the MCR and I&C room ancillary fans, the PCS recirculation pumps, and MCR lighting. In this time frame, the PCCWST provides water makeup to both the PCS and the spent fuel pit. An ancillary generator should be available during all MODES of operation. This long-term AC power supply function is important because it supports long-term shutdown operation.

The long-term AC power supply function involves the use of two ancillary diesel generators and an ancillary diesel generator fuel oil storage tank. The specified ancillary fuel oil storage tank volume is based on operation of both ancillary diesel-generators for 4 days. DCD subsection 8.3.1 contains additional information on the long-term AC power supply function.

One ancillary diesel generator and the ancillary diesel generator fuel oil storage tank should be available during all MODES of plant operation. Planned maintenance should be performed on the redundant ancillary diesel generator. Planned maintenance affecting the ancillary diesel generator or fuel tank that requires less than 72 hours to perform can be performed in any MODE of operation. Planned maintenance requiring more than 72 hours should be performed in MODE 6 with the refueling cavity full. The basis for this recommendation is that core decay heat is low and the risk of core damage is low in these MODES, the inventory of the refueling cavity results in slow response of the plant to accidents.

Table 10-2 (cont.) Investment Protection Short-Term Availability Controls

3.0 Electrical Power Systems

3.4 Non Class 1E DC and UPS System (EDS)

OPERABILITY: Power for DAS automatic actuation functions listed in 1.1 and 1.2 should be operable.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and
MODE 6 with upper internals in place or cavity level less than full

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Power to DAS Function inoperable.	A.1 Notify [chief nuclear officer] or [on-call alternate].	72 hours
	AND	
	A.2 Restore power supply to DAS to operable status.	14 days
B. Required Action and associated Completion Time of Condition A not met.	B.1 Submit report to [chief nuclear officer] or [on-call alternate] detailing interim compensatory measures, cause for inoperability, and schedule for restoration to OPERABLE.	1 day
	AND	
	B.2 Document in plant records the justification for the actions taken to restore the function to OPERABLE.	1 month

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.4 Non Class 1E DC and UPS System (EDS)

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
SR 3.4.1 Verify power supply voltage at each DAS cabinet is 120 volts ± 5%	92 days

Table 10-2 Investment Protection Short-Term Availability Controls (cont.)

3.0 Electrical Power Systems

3.4 Non Class 1E DC and UPS System (EDS)

BASES:

The EDS function of providing power to DAS to support ATWS mitigation is important based on 10 CFR 50.62 (ATWS Rule) and to support ESFA is important based on providing margin in the PRA sensitivity performed. This is assuming no credit for nonsafety-related SSCs to mitigate at-power and shutdown events. The margin provided in the PRA study assumes a minimum availability of 90 percent for this function during the MODES of applicability, considering both maintenance unavailability and failures to operate.

The DAS uses a two out of two logic to actuate automatic functions. EDS power must be available to the DAS sensors, DAS actuation, and the devices that control the actuated components. Power may be provided by EDS to DAS by non-1E batteries through non-1E inverters. Other means of providing power to DAS include the spare battery through a non-1E inverter or non-1E regulating transformers.

The EDS support of the DAS ATWS mitigation function is required during MODE 1 when ATWS is a limiting event and during MODES 1, 2, 3, 4, 5, and 6 when ESFA is important. The DAS ESFA is required in MODE 6 with upper internals in place or cavity level less than full. Planned maintenance should be performed on the redundant supplies of EDS power (that is, power supplies not required to be available) during MODE 6 with the cavity full.

10.4 DIVERSE ACTUATION SYSTEM MANUAL CONTROL TECHNICAL SPECIFICATION

As discussed in section 2.2, the CDF and LRF resulting from an AP1000 PRA sensitivity study were higher than the results of the AP600 focused PRA. This result is caused by not having all events lose offsite AC power upon reactor trip. As a result, the PMS is required to actuate passive safety features, such as the control rods, PRHR heat exchanger, and containment isolation. These sensitivity studies indicate that the LRF will be above the safety goal. By crediting the manual DAS controls, the LRF as well as the CDF, are reduced such that the PRA safety goals are met.

Since the DAS manual controls are credited to meet the LRF safety goal, it was concluded that these DAS manual controls should be included in the AP1000 Technical Specifications. Table 10-3 contains a draft of the DAS manual control Technical Specification.

Table 10-3 Technical Specifications

3.3 Instrumentation

3.3.5 Diverse Actuation System (DAS) Manual Controls

LCO 335 The DAS manual controls for each function in Table 3.3.5-1 shall be OPERABLE.

APPLICABILITY: According to Table 3.3.5-1

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more manual DAS controls inoperable.	A.1 Restore DAS manual controls to OPERABLE status.	30 days
B. Completion Time of Required Action A not met for inoperable DAS manual reactor trip control.	B.1 Perform SR 3.3.1.5. AND B.2 Restore all controls to OPERABLE status.	Once per 31 days on a STAGGERED TEST BASIS Prior to entering MODE 2 following next MODE 5 entry.
C. Completion Time of Required Action A not met for inoperable DAS manual actuation control other than reactor trip.	C.1 Perform SR 3.3.2.2. AND C.2 Restore all controls to OPERABLE status.	Once per 31 days on a STAGGERED TEST BASIS Prior to entering MODE 2 following next MODE 5 entry

Table 10-3 Technical Specifications (cont.)		
D. Completion Time of Required Action B not met. OR Completion Time of Required Action C not met.	D.1 Be in MODE 3. AND D.2 Be in MODE 5.	6 hours 36 hours
SURVEILLANCE REQUIREMENTS		
SURVEILLANCE		FREQUENCY
SR 3.3.5.1	----------NOTE---------- Verification of setpoint not required. ---------- Perform TRIP ACTUATING DEVICE OPERATIONAL TEST (TADOT).	 24 months

Table 10-3 Technical Specifications (cont.)

Table 3.3.5-1
DAS Manual Controls

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CONTROLS
1. Reactor Trip Manual Controls	1,2	2 switches
2. PRHR HX control and IRWST gutter control valves	1,2,3,4,5(a)	2 switches
3. CMT isolation valves	1,2,3,4,5(a)	2 switches
4. ADS stage 1 valves	1,2,3,4,5(a)	2 switches
5. ADS stage 2 valves	1,2,3,4,5(a)	2 switches
6. ADS stage 3 valves	1,2,3,4,5(a)	2 switches
7. ADS stage 4 valves	1,2,3,4,5,6(c)	2 switches
8. IRWST injection squib valves	1,2,3,4,5,6	2 switches
9. Containment recirc. valves	1,2,3,4,5,6	2 switches
10. Passive Containment Cooling Drain valves	1,2,3,4,5(b),6(b)	2 switches
11. Selected containment isolation valves	1,2,3,4,5,6	2 switches

(a) With RCS pressure boundary intact

(b) With the calculated reactor decay heat > 9.0 MWt

(c) In MODE 6 with reactor internals in place

Table 10-3 Technical Specifications (cont.)

B 3.3 Instrumentation

B 3.3.5 Diverse Actuation System (DAS) Manual Controls

BASES:

BACKGROUND

The Diverse Actuation System (DAS) manual controls provide non-Class 1E backup controls in case of common-mode failure of the Protection and Safety Monitoring System (PMS) automatic and manual actuations evaluated in the AP1000 PRA. These DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 analyses.

The specific DAS controls were selected based on PRA risk importance as discussed in Reference 1. As noted in Reference 1, electrical power for these controls and instrument indications need not be covered by Technical Specifications. The rational is that these controls use the same nonsafety-related power supply used by the plant control system. This power is required to be available to support normal operation of the plant. With offsite power available, there are several sources to provide this power including AC power to non-Class 1E battery chargers, AC power to rectifiers, and non-Class 1E batteries. As a result, with offsite power available it is very likely that power will be available for these DAS controls. If offsite power is not available, then there is still the likelihood that the non-1E batteries or the non-1E diesel generators will be available. Even if these sources are unavailable, the desired actions will occur without operator action for the more probable events. The rods will insert automatically on loss of offsite power. The passive residual heat removal heat exchanger (PRHR HX), core makeup tanks (CMT), passive containment cooling system (PCS), and containment isolation features are initiated by operation of fail-safe, air-operated valves. If all offsite and onsite AC power is lost, the instrument air system will depressurize by the time these functions are needed in the 1-hour time frame.

Instrument readouts are expected to be available even in case of complete failure of the PMS due to common cause failure. These instruments include both DAS and PLS instruments. As discussed above, it is expected that AC power will be available to power the instruments. Even if the operators have no instrument indications, they are expected to actuate the controls most likely to be needed (PRHR HX, CMT, PCS, and containment isolation). If all AC power fails, then the rods will drop and the air-operated valves will go to their fail-safe positions.

The DAS uses equipment from sensor output to the final actuated device that is diverse from the PMS to automatically initiate a reactor trip, or to manually actuate the identified safety-related equipment. DCD Section 7.7.1.11 (Ref. 2) provides a description of the DAS.

Table 10-3 (cont.) Technical Specifications	
APPLICABLE SAFETY ANALYSIS	The DAS manual controls are required to provide a diverse capability to manually trip the reactor and actuate the specified safety-related equipment, based on risk importance in the AP1000 PRA. The DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 safety analyses. The AP1000 PRA, Appendix A, provides additional information, including the thermal and hydraulic analyses of success sequences used in the PRA. The DAS manual controls satisfy Criterion 4 of 10 CFR 50.36(c)(2)(ii).
LCO	The DAS LCO provides the requirements for the OPERABILITY of the DAS manual trip and actuation controls necessary to place the reactor in a shutdown condition and to remove decay heat in the event that the PMS automatic actuation and manual controls are inoperable.
APPLICABILITY	The DAS manual controls are required to be OPERABLE in the MODES specified in Table 3.3.5-1. The manual DAS reactor trip control is required to be OPERABLE in MODES 1 and 2 to mitigate the effects of an ATWS event occurring during power operation. The other manual DAS actuation controls are required to be available in the plant MODES specified, based on the need for operator action to actuate the specified components during events that may occur in these various plant conditions, as identified in the AP1000 PRA.
ACTIONS	<u>A.1</u> Condition A applies when one or more DAS manual controls are inoperable. The Required Action A.1 to restore the inoperable DAS manual control(s) to OPERABLE status within 30 days is reasonable because the DAS is a separate and diverse non-safety backup system for the manual reactor trip and manual safety-related equipment actuation controls. The 30-day Completion Time allows sufficient time to repair an inoperable manual DAS control but ensures the control is repaired to provide backup protection. <u>B.1 and B.2</u> Condition B applies when Required Action A cannot be completed for the DAS manual reactor trip control within the required completion time of 30 days. Required Action B.1 requires SR 3.3.1.5, "Perform TADOT" for the reactor trip breakers, to be performed once per 31 days, instead of once every 92 days. Condition A of Example 1.3-6 illustrates the use of the Completion Time for Required Action B.1. The initial performance of SR 3.3.1.5 on the first division (since it is performed on a STAGGERED TEST BASIS) must be completed within 31 days of entering Condition B. The normal surveillance test frequency requirements for SR 3.3.1.5 must still be satisfied while performing SR 3.3.1.5 for Required Action B.1. The predominant failure requiring

Table 10-3 (cont.) Technical Specifications	
ACTIONS (continued)	the DAS manual reactor trip control is common-mode failure of the reactor trip breakers. This change in surveillance frequency for testing the reactor trip breakers increases the likelihood that a common-mode failure of the reactor trip breakers would be detected while the DAS manual reactor trip control is inoperable. This reduces the likelihood that a diverse manual reactor trip is required. It is not required to perform a TADOT for the manual actuation control. The manual reactor trip control is very simple, highly reliable, and does not use software in the circuitry. Although the DAS manual controls are non-Class 1E, they have been shown to be PRA risk important as discussed in Reference 1. The impact of an inoperable DAS manual control is compensated for by increasing the reactor trip breaker surveillance frequency from once every 92 days to once every 31 days. Action B.2 requires that the inoperable DAS manual reactor trip control be restored to OPERABLE status prior to entering MODE 2 following any plant shutdown to MODE 5 while the control is inoperable. This ACTION is provided to ensure that all DAS manual controls are restored to OPERABLE status following the next plant shutdown. <u>C.1 and C.2</u> Condition C applies when Required Action A cannot be completed for any DAS manual actuation control (other than reactor trip) within the required completion time of 30 days. Required Action C.1 requires SR 3.3.2.2, "Perform ACTUATION LOGIC TEST," to be performed once per 31 days, instead of once every 92 days. Condition A of Example 1.3-6 illustrates the use of the Completion Time for Required Action C.1. The initial performance of SR 3.3.2.2 on the first division (since it is performed on a STAGGERED TEST BASIS) must be completed within 31 days of entering Condition C. The normal surveillance test frequency requirements for SR 3.3.2.2 must still be satisfied while performing SR 3.3.2.2 for Required Action C.1. The predominant failure requiring the DAS manual actuation control is common-mode failure of the PMS actuation logic software or hardware. This change in surveillance frequency for actuation logic testing increases the likelihood that a common-mode failure of the PMS actuation logic from either cause would be detected while any DAS manual actuation control is inoperable. This reduces the likelihood that a diverse component actuation is required. It is not required to perform a TADOT for the manual actuation control device since the manual actuation control devices are very simple and highly reliable. Although the DAS manual controls are non-Class 1E, they have been shown to be PRA risk important as discussed in Reference 1. The impact of an inoperable DAS manual control is compensated for by increasing the automatic actuation surveillance frequency from once every 92 days to once every 31 days. Action C.2 requires that the inoperable DAS manual actuation control(s) be restored to OPERABLE status prior to entering MODE 2 following any plant shutdown to MODE 5 while the control is inoperable. This ACTION is provided to ensure that all DAS manual controls are restored to OPERABLE status following the next plant shutdown.

Table 10-3 (cont.) Technical Specifications	
ACTIONS (continued)	D.1 and D.2 Condition D is entered if the Required Action associated with Condition B or C is not met within the required Completion Time. Required Actions D.1 and D.2 ensure that the plant is placed in a condition where the probability and consequences of an event are minimized. The allowed Completion Times are reasonable based on plant operating experience, for reaching the required plant conditions from full power conditions in an orderly manner, without challenging plant systems.
SURVEILLANCE REQUIREMENTS	SR 3.3.5.1 SR 3.3.5.1 is the performance of a TADOT of the DAS manual trip and actuation controls for the specified safety-related equipment. This TADOT is performed every 24 months. The Frequency is based on the known reliability of the DAS functions and has been shown to be acceptable through operating experience. The SR is modified by a Note that excludes verification of the setpoints from the TADOT. The functions have no setpoints associated with them.
REFERENCES	1. WCAP-15985, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," November 2002. 2. DCD, Section 7.7.1.11