Westinghouse

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

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

Direct tel: 412-374-6306
Direct fax: 412-374-5005
e-mail: sterdia@westinghouse.com

Your ref: Project Number 740
Our ref: DCP/NRC2020

October 10, 2007

Subject: AP1000 COL Standard Technical Report Submittal of APP-GW-GLR-080 (TR 80)

In support of Combined License application pre-application activities, Westinghouse is submitting AP1000 Standard Combined License Technical Report Number 80. The primary purpose of Technical Report 80 is to describe changes to the AP1000 Instrumentation & Control systems and the AP1000 Design Control Document (DCD). This report contains both changes incorporated in Revision 16 and changes to Revision 16 of the DCD. This report is submitted as part of the NuStart Bellefonte COL Project (NRC Project Number 740). The information included in this report is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification.

The purpose for submittal of this report was explained in a March 8, 2006 letter from NuStart to the NRC.

Pursuant to 10 CFR 50.30(b), APP-GW-GLR-080, Revision 0, "Mark-up of AP1000 Design Control Document Chapter 7," Technical Report Number 80, is submitted as Enclosure 1 under the attached Oath of Affirmation.

It is expected that when the NRC review of Technical Report Number 80 is complete, Technical Report 80 will be considered approved generically for all COL applicants referencing the AP1000 Design Certification.

Questions or requests for additional information related to content and preparation of this report should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Westinghouse requests the NRC to provide a schedule for review of the technical report within two weeks of its submittal.

00265psa.doc

D063
D079
NRO

Very truly yours,

A. Sterdis, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Attachment

1. "Oath of Affirmation," dated October 10, 2007

/Enclosure

1. APP-GW-GLR-080, Revision 0, "Mark-up of AP1000 Design Control Document Chapter 7," Technical Report Number 80

cc:	D. Jaffe	-	U.S. NRC	1E	1A
	E. McKenna	-	U.S. NRC	1E	1A
	G. Curtis	-	TVA	1E	1A
	P. Hastings	-	Duke Power	1E	1A
	C. Ionescu	-	Progress Energy	1E	1A
	A. Monroe	-	SCANA	1E	1A
	M. Moran	-	Florida Power & Light	1E	1A
	C. Pierce	-	Southern Company	1E	1A
	E. Schmiech	-	Westinghouse	1E	1A
	G. Zinke	-	NuStart/Entergy	1E	1A
	J. Ewald	-	Westinghouse	1E	1A

ATTACHMENT 1

"Oath of Affirmation"

ATTACHMENT 1

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

In the Matter of:)

NuStart Bellefonte COL Project)

NRC Project Number 740)

APPLICATION FOR REVIEW OF
"AP1000 GENERAL COMBINED LICENSE INFORMATION"
FOR COL APPLICATION PRE-APPLICATION REVIEW

W. E. Cummins, being duly sworn, states that he is Vice President, Regulatory Affairs & Standardization, for Westinghouse Electric Company; that he is authorized on the part of said company to sign and file with the Nuclear Regulatory Commission this document; that all statements made and matters set forth therein are true and correct to the best of his knowledge, information and belief.

W. E. Cummins
Vice President
Regulatory Affairs & Standardization

Subscribed and sworn to
before me this 10th day
of October 2007.

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Patricia S. Aston, Notary Public
Murrysville Boro, Westmoreland County
My Commission Expires July 11, 2011
Member, Pennsylvania Association of Notaries

Notary

ENCLOSURE 1

APP-GW-GLR-080, Revision 0

"Mark-up of AP1000 Design Control Document Chapter 7"

Technical Report 80

AP1000 DOCUMENT COVER SHEET

TDC: ________ Permanent File: ________ APY: ________

RFS#: ________ RFS ITEM #: ________

AP1000 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
APP-GW-GLR-080	0	Page 1 of ~~186~~ 183	W - McGinnis

ALTERNATE DOCUMENT NUMBER: TR 80 — WORK BREAKDOWN #:

ORIGINATING ORGANIZATION: Westinghouse

TITLE: Mark-up of AP1000 Design Control Document Chapter 7

ATTACHMENTS: N/A CALCULATION/ANALYSIS REFERENCE: N/A	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: APP-GW-GEE-163,-067,-184,-229,-088,-156,-080,-054.

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
APP-GW-GLR-080 r0.doc	Word	

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

Class 3 Documents being transmitted to the NRC require the following two review signatures in lieu of a Form 36.

LEGAL REVIEW T. J. WHITE	SIGNATURE/DATE T. J. White 10-8-07
PATENT REVIEW D. E. EKEROTH	SIGNATURE/DATE Douglas E Ekeroth 10/8/07

☐ 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.

ORIGINATOR J. G. Ewald	SIGNATURE/DATE John G. Ewald 10/8/07	
REVIEWERS N/A	SIGNATURE/DATE	
VERIFIER M. A. Gasparovic	SIGNATURE/DATE Michael Gasparovic 10/8/07	VERIFICATION METHOD Page by Page Review
AP1000 RESPONSIBLE MANAGER C.A. McGinnis	SIGNATURE* CA McGinnis	APPROVAL DATE 10-8-07

* 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.

WESTINGHOUSE NON-PROPRIETARY CLASS 3

APP-GW-GLR-080
Revision 0

October 2007

AP1000 Standard Combined License Technical Report

Title: Mark-up of AP1000 Design Control Document Chapter 7

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

TABLE OF CONTENTS

II.14 ADDITION OF DELAY TIMERS FOR ENABLING THE SOURCE RANGE REACTOR TRIP AND FLUX DOUBLING SIGNAL

II.15 RT/ESF ACCURACIES AND RESPONSE TIMES CORRECTIONS

II.16 CORRECT CHAPTER 7 TECHNICAL SPECIFICATION REFERENCE

II.17 CORRECT CORE MAKEUP TANK ACTUATION SIGNALS

II.18 TRIPPING OF PRESSURIZER HEATERS

II.19 CORRECT DESCRIPTION FOR PERMISSIVE P-19

II.20 MINOR TECHNICAL CHANGES TO TABLE 7.3-1

II.21 CVS LETDOWN ISOLATION LOGIC MODIFICATIONS

II.22 REACTOR TRIP BREAKER STATUS INPUTS TO P-3 AND P-4 LOGIC

II.23 DELETION OF DIVISION TRIP STATUS BETWEEN DIVISIONS

II.24 LOW TCOLD AND HIGH STEAM PRESSURE NEGATIVE RATE ESF ACTUATION LOGIC MODIFICATIONS

II.25 DELETION OF REDUNDANT AUTOMATIC SAFEGUARDS REACTOR TRIP

II.26 CORE MAKEUP TANK LEVEL INPUT TO ADS LOGIC MODIFICATIONS

II.27 CMT AND PRHR ISOLATION VALVE LOGIC CHANGES

II.28 EDITORIAL CHANGES AND CLARIFICATIONS

II.29 CLARIFICATION OF REMOTE SHUTDOWN WORKSTATION REDUNDANCY

II.30 CONTROL SYSTEM FUNCTIONAL MODIFICATIONS

II.33 POST-ACCIDENT MONITORING SYSTEM TABLE CHANGES

II.34 DAS PLATFORM TECHNOLOGY AND REMOTE INDICATION CHANGES

PART B - CHANGES TO BE INCORPORATED IN NEXT DCD REVISION

II. TECHNICAL DESCRIPTIONS AND JUSTIFICATIONS

II.1 DESIGN COMPLETION

II.2 ELIMINATION OF CONTROL ROOM MULTIPLEXER

II.7 LOW REACTOR COOLANT FLOW REACTOR TRIP LOGIC MODIFICATIONS

II.8 OVERTEMPERATURE/OVERPOWER ΔT REACTOR TRIP MODIFICATIONS

II.9 FLUX DOUBLING/BORON DILUTION MODIFICATIONS

II.12 REMOVAL OF LOW-2 RCS HOT LEG SIGNAL FROM IRWST INJECTION LOGIC

II.13 CREATION OF NEW PERMISSIVE P-3 FOR SAFEGUARDS ACTUATION BLOCK

II.14 ADDITION OF DELAY TIMERS FOR ENABLING THE SOURCE RANGE REACTOR TRIP AND FLUX DOUBLING SIGNAL

II.15 RT/ESF ACCURACIES AND RESPONSE TIMES CORRECTIONS

II.28 EDITORIAL CHANGES AND CLARIFICATIONS

II.31 CORRECTION TO CMT LEVEL INSTRUMENT RANGE

II.32 INSTRUMENTATION AND CONTROL DESIGN CHANGE

II.33 POST-ACCIDENT MONITORING SYSTEM TABLE CHANGES

III. REGULATORY IMPACT

SUMMARY

Brief Description of the change (what is being changed and why):

This technical report describes changes to the AP1000 I&C systems and the AP1000 Design Control Document.

Changes and clarifications to the discussion and representation of the Protection and Safety Monitoring System in the AP1000 Design Control Document are identified. Modifications have been made to Tier 1 Sections 2.5.1 and 2.5.2 and Tier 2 Table 1-1, Chapter 3, Chapter 4, Chapter 7, Chapter 9, Chapter 14, Chapter 15, Chapter 16 (Technical Specifications and Bases) and Chapter 19 in order to refine and better illustrate the approach taken in the AP1000 design.

Common Q has been identified as the protection system platform and reflects the current state of design completion.

Modifications have been made to correct the logic and text found in Chapter 7 of the DCD and the revised Figure 7.2-1 diagrams, the Digital Enhancement of Overtemperature and Overpower ΔT Reactor Trips and the Flux Doubling/Boron Dilution Protection function and various corrections and additions resulting from ongoing functional and hardware design activities.

Part A provides the additions and changes that are included in AP1000 DCD Revision 16. For those additions and changes that are addressed in other AP1000 Technical Reports, a cross-reference to the appropriate report is provided. Part A is structured such that each impacted section includes a description, technical justification, regulatory basis and DCD markup. The DCD markups provided in Part A are markups of the DCD Revision 15 section.

Part B provides the additions and changes that will be included in a future AP1000 DCD Revision. For those additions and changes that are addressed in other AP1000 Technical Reports, a cross-reference to the appropriate report is provided. Part B is structured such that each impacted section includes a description, technical justification, regulatory basis and DCD markup. The DCD markups provided in Part B are markups of the DCD Revision 16 section.

Section III provides the formal documentation of the regulatory assessment

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

I. APPLICABILITY DETERMINATION

This evaluation is prepared to document if the changes described above are a departure from Tier 2 information of the AP1000 Design Control Document (DCD) that may be included in plant specific FSARs without prior NRC approval.

A.	Does the proposed change include a change to:		
	1. Tier 1 of the AP1000 Design Control Document APP-GW-GL-700	☐ NO ☒ YES	(If YES prepare a report for NRC review of the changes)
	2. Tier 2* of the AP1000 Design Control Document, APP-GW-GL-700	☐ NO ☒ YES	(If YES prepare a report for NRC review of the changes)
	3. Technical Specification in Chapter 16 of the AP1000 Design Control Document, APP-GW-GL-700	☐ NO ☒ YES	(If YES prepare a report for NRC review of the changes)
B.	Does the proposed change involve:		
	1. Closure of a Combined License Information Item identified in the AP1000 Design Control Document, APP-GW-GL-700	☒ NO ☐ YES	(If YES prepare a COL item closure report for NRC review.)
	2. Completion of an ITAAC item identified in Tier 1 of the AP1000 Design Control Document, APP-GW-GL-700	☐ NO ☒ YES	(If YES prepare an ITAAC completion report for NRC review.)

PART A – CHANGES INCORPORATED IN REVISION 16 OF THE DCD

II. TECHNICAL DESCRIPTIONS AND JUSTIFICATIONS

II.1 DESIGN COMPLETION

The design of the AP1000 instrumentation and control systems have progressed and additional details can be added to the DCD to describe these systems. The changes listed below identify Common Q as the platform to be used for the Protection and Safety Monitoring System, describe the Common Q implementation, and identify the latest design process documents that are being used for this design.

Revisions to both Tier 1 and Tier 2 are proposed to describe the design and reflect the current status of the design process.

The Tier 1 changes propose deleting item 11a in section 2.5.2 Design Description and item 11a in Table 2.5.2-8 because this item has been completed and audited by the NRC in October 2006.

The Tier 2 changes upgrade the references to the current design practices and reference WCAP-16675 (TR-89) for design description rather than duplicating this material in the DCD.

Tier 1 Changes

Section 2.5.2 is revised as shown to eliminate the "Design requirements phase" because this item has been completed and audited by the NRC in October. This change does not affect conformance to regulatory requirements and guidance.

2.5.2 Protection and Safety Monitoring System

Design Description

11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:

a) System definition phase 2006.

Deleted: <#>Design requirements phase, may be referred to as conceptual or project definition phase¶

b) Hardware and software development phase, consisting of hardware and software design and implementation

c) System integration and test phase

d) Installation phase

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Table 2.5.2-8 is revised as shown to eliminate the "Design requirements phase" because this item has been completed and audited by the NRC in October 2006. This change does not affect conformance to regulatory requirements and guidance.

Table 2.5.2-8 (cont.)
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages: a) System definition phase b) Hardware and software development phase, consisting of hardware and software design and implementation c) System integration and test phase d) Installation phase	Inspection will be performed of the process used to design the hardware and software.	A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following: a) Specification of functional requirements. b) Documentation and review of hardware and software. c) Performance of system tests and the documentation of system test results. d) Performance of installation tests and inspections.

Deleted: a) Design requirements phase, may be referred to as conceptual or project definition phase¶
Deleted: b
Deleted: a) Establishment of plans and methodologies.¶
Deleted: b
Deleted: c
Deleted: c
Deleted: d
Deleted: d
Deleted: e
Deleted: e

Tier 2 Changes

DCD Table 1-1 is revised as shown. The changes are as follows:

1. Remove the reference to WCAP-13383 which is AP600 specific.

2. Change the reference for the Common Qualified Platform Topical Report from CENPD-396-P, Rev. 01 to WCAP-16097-P-A, Rev. 0. The new reference is the latest Nuclear Regulatory Commission accepted version. The Common Q Platform was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML011690170 (Reference 7), and ML0305507760 (Reference 8).

3. Change the reference for the Software Program Manual from CE-CES-195 Rev. 01 to WCAP-16096-NP-A 01A. The new reference is the latest Nuclear Regulatory Commission accepted version. The Software Program Manual was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML0305507760 (Reference 8), and ML042730580 (Reference 9).

4. Remove the reference to WCAP-15927 which is a lower-level process document. All commitments to regulatory requirements and guidance are made in WCAP-16096-NP-A, Rev. 0. The lower-level process is now available in NABU-DP-00014-GEN (Reference 20 in this section of the DCD).

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

These changes do not affect conformance to regulatory requirements and guidance.

Table 1-1 (Cont.)
Index of AP1000 Tier 2 Information Requiring NRC Approval for Change

Item	Expiration at First Full Power	Tier 2 Reference
WCAP-14605, "Westinghouse Setpoint Methodology for Protection Systems, AP600," Rev 0	Yes	Chapter 7 Table 1.6-1
WCAP-16097-P-A, "Common Qualified Platform", Rev 0	Yes	Chapter 7 Table 1.6-1
WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," Rev 01A	Yes	Chapter 7 Table 1.6-1
Verification and Validation	Yes	7.1.2.14
Hard-wired DAS manual actuation	No	7.7.1.11

Deleted: WCAP-13383, "AP600 Instrumentation and Control Hardware & Software Design, Verification & Validation Process Report," Rev 1.

Deleted: Yes

Deleted: Chapter 7 Table 1.6-1

Deleted: CENPD-396-P, Rev. 01

Deleted: CE-CES-195

Deleted: WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Rev 0

Deleted: Yes

Deleted: Chapter 7 Table 1.6-1

The List of Figures in DCD Chapter 7 is revised as shown to delete figures that are no longer referenced from the text. The associated text changes are described elsewhere in this document.

LIST OF FIGURES

The third paragraph of section 7.1 is revised as shown to remove the option to implement the protection and safety monitoring system using the Westinghouse Eagle product line.

This change does not affect conformance to regulatory requirements and guidance.

DCD Chapter 7 for the AP1000 has been written to describe the protection system hardware utilizing the Common Qualified Platform (Common Q) described in References 8 and 13 (which include the NRC SER). The I&C functional requirements of the AP600, which has received Design Certification, have been retained to the maximum extent compatible with the Common Q hardware and software.

Deleted: permit

Deleted: use of either the Eagle

Deleted: described in the AP600 DCD or

Deleted: and accepted in References 11, 14, and 16

Deleted: and the Eagle hardware and software

Section 7.1.2 and its subsections are revised as shown.

The content of several subsections is deleted and replaced with a reference to WCAP-16675 (TR-89) (Reference 10) which provides a more detailed description of the current Common Q protection system design. The most significant changes in the system include:

1) Replace the bi-directional gateway between the protection and safety monitoring system (PMS) and the data display and processing system (DDS) with a uni-directional gateway.

2) Eliminate manual system level safety functions [engineered safety features (ESF) system level actuations, blocks and resets, and reactor trip] from the plant control system (PLS).

3) Use "discrete" signals via the remote I/O bus and the component interface module (CIM) for non-safety control of safety components from the PLS, in place of the bi-directional gateway.

4) Eliminate component level control of safety components with "onerous" consequences from the PLS.

5) Eliminate the PMS control room multiplexers. (See the discussion in section II.C.)

Changes one through four are made to more easily demonstrate compliance with IEEE-603 and IEEE 7-4.3.2. Change five is made to reduce heat and noise in the main control room since the multiplexers are not required for the Common Q implementation. These changes do not adversely affect conformance to regulatory requirements and guidance.

Subsection 7.1.2 is revised to remove references related to the Westinghouse Eagle product line, to update the Common Q references to the latest version accepted by the Nuclear Regulatory Commission, to map the development phase names used in various documents, and to document that the conceptual phase is complete. This change does not affect conformance to regulatory requirements and guidance.

7.1.2 Protection and Safety Monitoring System

Reference 19, Section 2.1 provides an overview description of the protection and safety monitoring system.

7.1.2.1 Plant Protection Subsystems

Reference 19, Section 2.2 describes the plant protection subsystems.

7.1.2.1.1 Reactor Trip Functions

Reference 19, Section 1.1 describes the reactor trip functions.

7.1.2.1.2 Reactor Trip Switchgear Interface

Reference 19, Section 2.2.3.1.1 describes the reactor trip switchgear interface.

7.1.2.1.3 Manual Reactor Trip

Reference 19, Section 2.2.3.1.3 describes the manual reactor trip.

7.1.2.2 Engineered Safety Features Coincidence Logic

Reference 19, Section 2.2.3.2.1 describes the Engineered Safety Features Coincidence Logic.

7.1.2.3 Engineered Safety Features Actuation Subsystems

Reference 19, Section 2.2.3.2.2 describes the Engineered Safety Features Actuation Subsystems.

7.1.2.4 Reactor Trip Switchgear

Reference 19, Section 2.2.3.1.1 describes the reactor trip switchgear.

7.1.2.5 Qualified Data Processing Subsystems

Reference 19, Section 4.2 describes the Qualified Data Processing Subsystem (QDPS).

7.1.2.8 Communication Functions

Reference 19, Section 3 describes the communication functions.

7.1.2.9 Fault Tolerance, Maintenance, Test, and Bypass

Reference 19, Section 7 describes the fault tolerance features and Section 6 describes the maintenance, test and bypass features of the protection and safety monitoring system.

Deleted: The protection and safety monitoring system is illustrated in Figure 7.1-2. The functions of the protection and safety monitoring system are implemented in separate processor-based subsystems. Each subsystem is located on an independent computer bus to prevent propagation of failures and to enhance availability. In most cases, each subsystem is implemented in a separate card chassis. Subsystem independence is maintained through the use of the following:¶ ... [1]

Deleted: The plant protection subsystems contain the necessary equipment to perform the following functions:¶ <#>Permit acquisition and analysi ... [2]

Deleted: The reactor trip functions are performed in two subsystems per division for accident protection. The primary function of the reactor trip subsystems is to process input data and provide ... [3]

Deleted: The final stage of the reactor trip coincidence logic provides the signal to energize the undervoltage trip attachment on each of the two division reactor trip switchgear breakers. L ... [4]

Deleted: A manual reactor trip can be accomplished from the main control room by redundant momentary switches. The switches directly interrupt the power from the voting logic, actuating the ... [5]

Deleted: The ESF logic functions are also performed in two subsystems per division for more reliable accident mitigation. The primary functions of the ESF coincidence logic are to proc ... [6]

Deleted: The ESF actuation subsystems provide a distributed interface between the plant operator and the nonmodulating safety-related plant components. Nonmodulating control relates to t ... [7]

Deleted: The reactor trip switchgear is used to initiate reactor shutdown. The reactor trip switchgear connects the electrical motive power, supplied from motor-generator sets, to the rod co ... [8]

Deleted: The Qualified Data Processing Subsystem (QDPS), a subsystem of the PMS, provides safety-related display of selected parameters in the control room.¶ The QDPS subsystems are a redun ... [9]

Deleted: The communication functions provide information from the plant protection subsystem, the ESF coincidence logic, the ESF actuation subsystems, and the QDPS subsy ... [10]

Deleted: The protection and safety monitoring system provides a high degree of reliability and fault tolerance. This capability is demonstrated by the following design features:¶ ... [11]

7.1.2.11 Test Subsystem

Reference 19, Section 6 describes the test subsystem.

7.1.2.14 Verification and Validation

[*Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program are provided in WCAP-16096-NP-A (Reference 9).*]* **WCAP-16096-NP-A defines a software development process consistent with the appropriate industry standards.**

7.1.2.14.1 Design Process

[*WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:*

- *Conceptual phase (may also be referred to as design requirements phase)*
- *Requirements phase (may also be referred to as system definition phase)*
- *Design phase (may also be referred to as hardware and software development phase)*
- *Implementation phase (may also be referred to as hardware and software development phase)*
- *Test phase (may also be referred to as system integration and test phase)*
- *Installation and checkout phase (may also be referred to as installation phase)*]*

The conceptual phase (design requirements phase) has been completed for AP1000.

[*WCAP-16096-NP-A (Reference 9), NABU-DP-00014-GEN (Reference 20), and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.*]*

Deleted: The test subsystem provides a means of testing the operation of the protection and safety monitoring system and verifying that the plant protection system setpoints are within the system requirements. Each redundant subsystem is tested individually.¶
Testing from the sensor inputs of the protection and safety monitoring system through to the actuated equipment is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power would upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down.¶
Each division of the protection and safety monitoring system is furnished with a test subsystem. The test subsystem provides for verification of the accuracy of setpoints and other constants, and verification that proper signals appear at other locations in the system.¶
Verification of the signal processing algorithms is made by exercising ... [12]

Deleted: *either WCAP-13383 (Reference 3) or CE-CES-195*

Deleted: **WCAP-13383 is an AP600 reference. CE-CES-195 is a Common Q document. The**

Deleted: **is**

Deleted: **following**

Deleted: **:¶ ANSI/IEEE ANS-7-4.3.2-1993; "IEEE Standard Criteria for Digital** ... [13]

Deleted: *WCAP-13383 provides a planned design process for hardware and software development during the* ... [14]

Deleted: <#>¶

Deleted: *15927*

Deleted: *10*

Deleted: *. a Common Q document. also*

Deleted: *hardware and*

Deleted: *similar*

Deleted: *System definition*

Deleted: *Software d*

Deleted: *<#>Hardware design phase¶ Software i*

Deleted: *<#>Hardware implementation phase¶ System integration*

Deleted: *Depending on the protection and safety monitoring system hardware used for AP1000. either WCAP-13383 or*

Deleted: *15927*

The references are revised as shown for consistency with the text changes described elsewhere in this document.

1. Delete the reference to WCAP-13382, which is AP600 specific and describes the Eagle product line.

2. Delete the reference to WCAP-13383, which is AP600 specific and related to the Eagle product line.

3. Delete the reference to WCAP-14080 and WCAP 14081 which are AP600 specific.

4. Change the reference for the Software Program Manual from CE-CES-195 Rev. 01 to WCAP-16096-NP-A 01A. The new reference is the latest Nuclear Regulatory Commission accepted version. The Software Program Manual was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML0305507760 (Reference 8), and ML042730580 (Reference 9).

5. Change the reference for the Common Qualified Platform Topical Report from CENPD-396-P, Rev. 01 to WCAP-16097-P-A, Rev. 0. The new reference is the latest Nuclear Regulatory Commission accepted version. The Common Q Platform was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML011690170 (Reference 7), and ML0305507760 (Reference 8).

6. Remove the reference to WCAP-15927 which is a lower-level process document. All commitments to regulatory requirements and guidance are made in WCAP-16096-NP-A, Rev. 0. The lower-level process is now available in NABU-DP-00014-GEN (Reference 20 which was added in this section of the DCD).

7. Delete the references to ML003740165, ML011690170, and ML030550776. These Nuclear Regulatory Commission acceptance letters are included in the documents they refer to.

8. Add the reference to WCAP-16361 which is an AP1000 technical report that has been separately submitted to the Nuclear Regulatory Commission.

9. Add the reference to APP-GW-GLR-017 which is an AP1000 technical report that has been separately submitted to the Nuclear Regulatory Commission.

10. Add the reference to WCAP-16675 which is an AP1000 technical report that has been separately submitted to the Nuclear Regulatory Commission.

7.1.7 References

1. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

2. Deleted.

3. Deleted.

4. Deleted.

[5. *WCAP-14605 (Proprietary) and WCAP-14606 (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996.*]*

6. 10 CFR 21, "Reporting of Defects and Noncompliance."

7. WCAP-15775, Revision 2, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," March 2003.

[8. *WCAP-16097-P-A, (Proprietary)and WCAP-16097-NP-A, (Non-Proprietary), Revision 0, "Common Qualified Platform," May 2003.*]*

[9. *WCAP-16096-NP-A, Rev. 01A, "Software Program Manual for Common Q Systems," January 2004.*]*

10. *Deleted.*

11. Deleted.

12. WCAP-15776, "Safety Criteria for the AP1000 Instrument and Control Systems," April 2002.

13. WCAP-16097-P-A (Proprietary) and WCAP-16096-NP-A (Non-Proprietary), Appendix 4, "Common Qualified Platform Integrated Solution," May 2003.

14. Deleted.

15. Deleted.

16. Deleted.

17. WCAP16361-P (Proprietary) and WCAP-16361-NP (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006.

18. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC Items," Westinghouse Electric Company LLC.

Deleted: WCAP-13382 (Proprietary) and WCAP-13391 (Non-Proprietary), "AP600 Instrumentation and Control Hardware Description," May 1992

Deleted: [

Deleted: *WCAP-13383, Revision 1 (Non-Proprietary), "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," June 1996.*]*

Deleted: WCAP-14080 (Proprietary) and WCAP-14081 (Non-Proprietary), "AP600 Instrumentation and Control Software Architecture and Operation Description," June 1994

Deleted: *CENPD-396-P*

Deleted: *Rev.01*

Deleted: *May 2000 and WCAP-16097-NP-A, (Non-Proprietary)*

Deleted: *CE-CES-195*

Deleted: *May 26, 2000*

Deleted: [

Deleted: *WCAP-15927, Rev. 0, "Design Process for AP1000 Common Q Safety Systems," August 2002.*]*

Deleted: ML003740165, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 01 (TAC No. MA1677)," August 11, 2000

Deleted: CENPD-396-P

Deleted: Rev. 02 (Proprietary),

Deleted: April 2001 and WCAP-16097-NP-A, Appendix 4 (Non-Proprietary),

Deleted: ML011690170, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1 (TAC No. MB0780)," June 22, 2001

Deleted: IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Deleted: ML0305507760, "Acceptance of the Changes to Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Closeout of Category 2 Open Items (TAC No. MB2553)," February 24, 2003

19. WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), AP1000 Protection and Safety Monitoring System Architecture Technical Report," February 2007.

20. NAMB-DP-00014-GEN, Rev. 1 (Proprietary), "Design Process for Common Q Safety Systems," March 2006.

21. Westinghouse Electric Company Quality Management System (QMS), Rev. 5 (Non-Proprietary), October 1, 2002.

Figure 7.1-1 is revised to show the overall I&C Architecture consistent with the textual changes described elsewhere in this document. Figures 7.1-2 through 7.1-11 are deleted because the text that references them has been deleted or they are redundant to figure 7.1-1.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

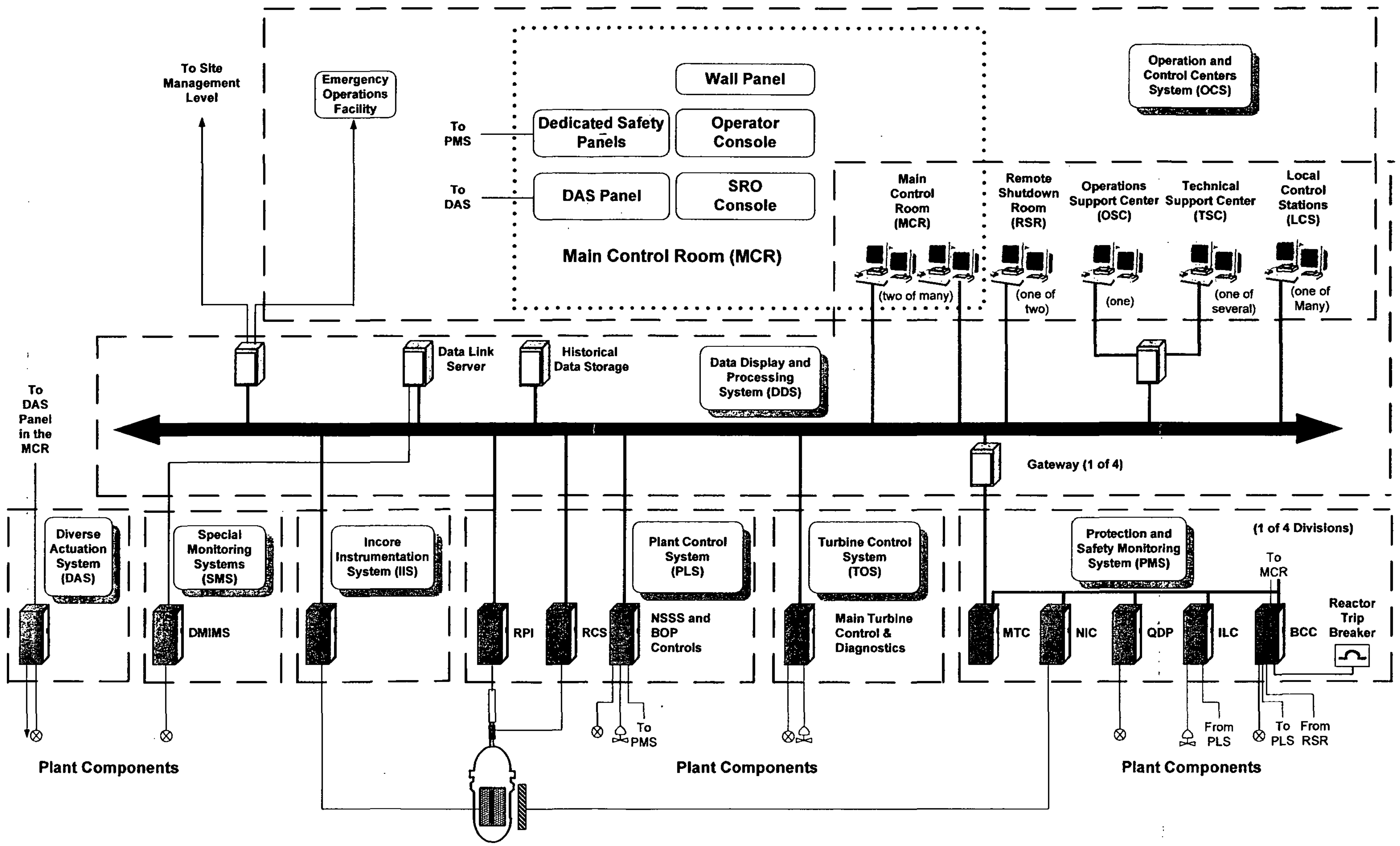

Figure 7.1-1

Instrumentation and Control Architecture

Section 7.2.4 is revised as shown to change the reference for the Common Qualified Platform Digital Plant Protection System Topical Report from CENPD-396-P, Rev. 1 to WCAP-16097-P-A, Rev. 0 and WCAP-16097-NP-A, Rev. 0. The new reference is the latest Nuclear Regulatory Commission accepted version. The Common Q Platform was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML011690170 (Reference 7), and ML0305507760 (Reference 8).

This change does not affect conformance to regulatory requirements and guidance.

7.2.4 References

3. WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Appendix 3, Rev. 0, "Common Qualified Platform, Digital Plant Protection System," May 2003.

Deleted: CENPD-396-P

Deleted: 1

Deleted: 2000

II.2 REMOVAL OF NON-SAFETY PERMISSIVE P-17 FROM THE PROTECTION SYSTEM:

Permissive P-17 is not used in the PMS and is not credited in the Chapter 15 Accident Analysis. It will be developed in the PLS and be used as part of that system's Automatic Rod Withdrawal Block function and therefore will be removed from Tier 1 Table 2.5.2-6 and Tier 2 Subsection 7.2.1.1.11. This item is also addressed as part of the Figure 7.2-1, Sheet 4 changes above. This change also requires that part of Table 7.2-3 (Sheet 2 of 2) be corrected and an abridged version is included after the Subsection 7.2.1.1.11 changes.

Tier 1 Changes

TABLE 2.5.2-6 PMS BLOCKS
Reactor Trip Functions: Source Range High Neutron Flux Reactor Trip Intermediate Range High Neutron Flux Reactor Trip Power Range High Neutron Flux (Low Setpoint) Trip Reactor Coolant Pump High Bearing Water Temperature Trip Pressurizer Low Pressure Trip Pressurizer High Water Level Trip Low Reactor Coolant Flow Trip Low Reactor Coolant Pump Speed Trip High Steam Generator Water Level Trip Engineered Safety Features: Automatic Safeguards Containment Isolation Main Feedwater Isolation Reactor Coolant Pump Trip Core Makeup Tank Injection Turbine Trip Steam Line Isolation Startup Feedwater Isolation Block of Boron Dilution Chemical and Volume Control System Isolation Steam Dump Block Auxiliary Spray and Letdown Purification Line Isolation Passive Residual Heat Removal Heat Exchanger Alignment Normal Residual Heat Removal System Isolation

Deleted: Plant Control System Blocks (Nonsafety-related):

Automatic Rod Withdrawal

Document Number: APP-GW-GLR-080 Revision Number: 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Tier 2 Changes

7.2.1.1.11 Reactor Trip System Interlocks

Table 7.2-3 (Sheet 2 of 2)

REACTOR TRIP PERMISSIVES AND INTERLOCKS

Designation	Derivation	Function
•		

Deleted: **Automatic Rod Withdrawal Block** ¶
An automatic rod withdrawal block occurs on a power range negative flux rate below the P-17 setpoint to block the remaining rods that are not inserted by the rapid power reduction system. Figure 7.2-1, sheet 4, shows this block function. This interlock is generated by the protection and safety monitoring system and forwarded to the plant control system for implementation.

Deleted: ¶

Deleted: P-17(1) ... [15]

Deleted: Note:¶
1. This interlock does not meet the July 1993 Final Policy Statement on Technical Specification Improvements criteria and is not included in the Technical Specifications.

II.3 ELIMINATION OF CONTROL ROOM MULTIPLEXER

Section 7.1.2.6 is revised as shown to eliminate the protection and safety monitoring system control room multiplexers. In the Common Q implementation, control room multiplexers are not needed and add an extra level of complexity. Additionally, the multiplexers add heat and noise to the control room. The control room multiplexers were used in the Eagle architecture to provide the discrete digital inputs needed for the dedicated switches in the control room. Common Q does not require these devices so they are eliminated in the Common Q implementation

This change does not affect conformance to regulatory requirements and guidance.

7.1.2.6 Main Control Room Multiplexers

The protection and safety monitoring system does not use multiplexers to provide a signal path between the protection system equipment and the main control room. Each division's safety/QDPS display communicates with the protection system equipment via that division's communications network as shown in Figure 2-2 of Reference 19.

Deleted: The protection and safety monitoring system contains redundant multiplexers to provide a signal path from the protection channels to safety operator modules in the main control room. One redundant main control room multiplexer is associated with each of the four safety divisions. The multiplexers provide for transmission of component-level manual actuation signals from the main control room to the ESF actuation subsystems. The multiplexers also provide for transmission of component status information from the ESF actuation subsystems to the main control room.¶
The multiplexers communicate with soft control devices or operator interface modules in the main control room. Subsection 7.1.3.3 provides additional discussion of the operation of the soft control devices. The transfer of control from the main control room to the remote shutdown workstation is accomplished using transfer switches as described in subsection 7.4.3.¶
Various "handshaking" signals are implemented for requests and responses between the soft controls and the multiplexers to verify the receipt and the validity of the messages.

II.4 CYBER-SECURITY

Section 7.1 is modified as shown to add a reference to APP-GW-GLR-104 (TR-104) which describes the AP1000 cyber-security implementation. Previous revisions of the DCD did not explicitly address cyber-security. These changes do not adversely affect conformance to regulatory requirements and guidance.

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network. To meet cyber security concerns, the real-time data highway will be separated into security levels as described in Reference 22.

The following sub-section is added at the end of section 7.1.1 to address cyber security requirements.

Cyber Security

Reference 22 describes the cyber security implementation for AP1000.

Reference 22 is added to Section 7.1.7.

---

22. APP-GW-GLR-104, "AP1000 Cyber Security Implementation," May 2007.

II.5 REVISION TO TABLES 7.5-1, 7.5-5, 7.5-6, 7.5-7, AND 7.5-9 FOR CONSISTENT NAMING OF RCS WIDE RANGE PRESSURE

Tables 7.5-1, 7.5-5, 7.5-6, 7.5-7 and 7.5-9 use the variable name "RCS pressure." The correct title is "RCS wide range pressure." Tables 7.5-1, 7.5-5, 7.5-6, 7.5-7 and 7.5-9 are revised as shown below. This is an editorial change and does not affect the functional design or conformance to regulatory requirements and guidance.

Additionally, the description of the subcooling calculation in Note 6 to Table 7.5-1 is not correct. Note 6 is revised as shown.

Table 7.5-1 (Sheet 1 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
RCS wide range pressure	0-3300 psig	B1, B2, D2, C1, F2	Harsh	Yes	3 (Note 4)	1E	Yes	Located inside containment

Table 7.5-1 (Sheet 12 of 12)

POST-ACCIDENT MONITORING SYSTEM

Notes:

1. Total flow measurement is obtained from the sum of four branch flow devices.
2. The same information is available in the technical support center via the monitor bus. Information available on the qualified data processing system is also available at the remote shutdown workstation.
3. Noble gas: 10^{-7} to 10^{5} μCi/cc
   Particulate: 10^{-12} to 10^{-7} μCi/cc
   Iodines: 10^{-11} to 10^{-6} μCi/cc
4. The number of instruments required after stable plant conditions is two. A third channel is available through temporary connections to resolve information ambiguity if necessary (See subsection 7.5.4).
5. Noble gas: 10^{-7} to 10^{-2} μCi/cc
   Particulate: 10^{-12} to 10^{-7} μCi/cc
   Iodines: 10^{-11} to 10^{-5} μCi/cc
6. Degree of subcooling is calculated from RCS wide range pressure and core exit temperature.
7. This instrument is not required after 24 hours.
8. Two steam line pressure instruments per SG are located inside containment, and are qualified for a harsh environment. Two steam line pressure instruments per SG are located outside containment (not in MSIV compartment), and are qualified for a mild environment.
9. MCR supply air radiation monitoring is not required after MCR has been isolated.
10. This instrument is only required when non-safety power is available.
11. This instrument is not required if non-Class 1E UPS power is not available.
12. These devices are backup verification to qualified system status parameters. These devices are purchased to perform in their anticipated service environments for the plant conditions for which they must function.

Deleted: pressurizer

Deleted: RCS hot leg

Table 7.5-5

SUMMARY OF TYPE B VARIABLES

Function Monitored	Variable	Type/Category
Reactivity Control	Neutron flux	B1
	Control rod position	B3
Reactor Coolant System Integrity	RCS wide range pressure	B1
	RCS wide range T_{hot}	B1
	RCS wide range T_{cold}	B1
	Containment water level	B1
	Containment pressure	B1
Reactor Coolant Inventory Control	Pressurizer level	B1
	Pressurizer reference leg temperature	B1
	Pressurizer pressure	B1
	Reactor vessel - hot leg water level	B3
Reactor Core Cooling	Core exit temperature	B1
	RCS subcooling	B1
	RCS wide range T_{hot}	B2
	RCS wide range T_{cold}	B2
	RCS wide range pressure	B2
	Reactor vessel - hot leg water level	B2

Table 7.5-6

SUMMARY OF TYPE C VARIABLES

Function Monitored	Variable	Type/Category
Incore Fuel Clad	Core exit temperature	C1
RCS Boundary	RCS wide range pressure	C1
	Containment pressure	C2
	Containment water level	C1
	Containment area high range radiation	C1
	Turbine island vent discharge radiation level	C2
	Steam generator blowdown discharge radiation level	C2
	Steam generator blowdown brine radiation level	C2
	Main steam line radiation level	C2

Table 7.5-7 (Sheet 1 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Type/Category
Reactivity Control System	Reactor trip breaker status	D2
	Control rod position	D3
Pressurizer Level and Pressure Control	Pressurizer safety valve status	D2
	Pressurizer level	D2
	RCS wide range pressure	D2
	Pressurizer pressure	D2
	Reference leg temperature	D2

Table 7.5-9 (Sheet 1 of 4)

SUMMARY OF TYPE F VARIABLES

Variable	Type/Category
Monitoring for preplanned manual nonsafety-related system actions	
RCS wide range pressure	F2
RCS wide range T_{hot}	F2
RCS wide range T_{cold}	F2

II.6 MANUAL PASSIVE CONTAINMENT COOLING DIVISION ASSIGNMENT MODIFICATIONS

The changes to Table 7.3-3 are being made to correct the Division assignments for the Manual passive containment cooling actuations #1 and #2. These manual controls actuate passive containment cooling as well as containment isolation and therefore must also be connected to Division D. This change is shown in the abridged copy of Table 7.3-3 (Sheet 1 of 2) below.

Table 7.3-3 (Sheet 1 of 2)

SYSTEM-LEVEL MANUAL INPUT TO THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Manual Control	**To Divisions**				**Figure 7.2-1 Sheet**
Manual passive containment cooling actuation #1	A	B	C	D	13
Manual passive containment cooling actuation #2	A	B	C	D	13
Manual passive containment isolation actuation #1	A	B	C	D	13
Manual passive containment isolation actuation #2	A	B	C	D	13

II.7 LOW REACTOR COOLANT FLOW REACTOR TRIP LOGIC MODIFICATIONS

AP1000 is not licensed for N-1 Loop Operation and therefore the PMS is not required to account for this requirement as part of its design. This change affects Subsection 7.2.1.1.3, Table 7.2-2 (Sheet 1 of 2), Table 7.2-3 (Sheet 1 of 2), Technical Specification, Bases Section B 3.3.1, B 3.4.4, Section 3.3.1, Table 3.3.1-1 (Pages 2, 3 & 4 of 5), Table 15.0-4a (Sheet 1 of 2), Table 15.0-6 (Sheet 3 of 4), Subsection 15.3.1.1, 15.3.2.1 and Figure 7.2-1, Sheet 5. In all of these locations references to the P-8 permissive that permits operation at reduced power with a reactor coolant pump out of service have been removed. Additionally in table 7.2-2 (Sheet 1 of 2) "Pressurizer High Water Level Trip" has been changed to "High-3 Pressurizer Water Level Trip" to keep the labeling of that function consistent throughout the DCD.

In addition, the logic for the function shown in Figure 7.2-1, Sheet 5 is revised to so that the reactor will trip when either low flow signal channels in 2 out of the 4 divisions are true coincident with the P-10A signal. The existing logic does not segregate the hot leg signals across the divisions, thereby increasing the chance of an inadvertent reactor trip. For example, it would trip the reactor if one division monitoring one hot leg tripped and another division monitoring the other hot leg tripped at the same time. This is inconsistent with traditional design practice that only will trip the reactor if two or more divisions monitoring the same hot leg are tripped. The existing logic creates an increased likelihood of inadvertent reactor trips, thereby increasing the likelihood of challenges to safety systems. The revised design is consistent with the accident analysis as discussed in DCD Chapter 15.

The same changes are made for the High Reactor Coolant Pump Bearing Water Temperature Reactor Trip logic.

7.2.1.1.3 Core Heat Removal Trips

Reactor Trip on Low Reactor Coolant Flow

This trip protects against departure from nucleate boiling in the event of low reactor coolant flow. Flow in each hot leg is measured at the hot leg elbow. The trip on low flow in the hot legs is automatically blocked when reactor power is below the P-10 permissive setpoint. This enhances reliability by preventing unnecessary reactor trips. The trip function is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 5 shows the logic for this trip. The development of permissive P-10 and P-8 are shown in Figure 7.2-1, sheet 4.

Reactor Coolant Pump Bearing Water Temperature Trip

This trip is an anticipatory trip based on the expectation of a complete loss of reactor coolant flow if cooling water is lost to the reactor coolant pumps. This trip occurs before the reactor coolant pumps are tripped on the same measurement.

The reactor trip on high reactor coolant pump bearing water temperature in any single reactor coolant pump is automatically blocked when reactor power is below the P-10 permissive setpoint. This enhances reliability by preventing unnecessary reactor trips. The trip is automatically reset when reactor power is above the P-10 setpoint.

Deleted: either hot leg is automatically blocked when reactor power is below the P-8 permissive setpoint, and the trip on low flow in

Deleted: both

Deleted: two

Deleted: s

Deleted: are

Deleted: P-8 and

Deleted: s

Deleted: 8

Deleted: and the trip on high reactor coolant pump bearing water temperature in multiple pumps is automatically blocked when reactor power is below the P-10 permissive setpoint.

Deleted: two parts of the

Deleted: are

Deleted: P-8 and

Deleted: s

Table 7.2-2 (Sheet 1 of 2)

REACTOR TRIPS

Reactor Trip(1)	No. of Channels	Division Trip Logic	Bypass Logic	Permissives and Interlocks (See Table 7.2-3)
Source Range High Neutron Flux Reactor Trip	4	2/4	Yes(2)	P-6, P-10
Intermediate Range High Neutron Flux Reactor Trip	4	2/4	Yes(2)	P-10
Power Range High Neutron Flux (Low Setpoint) Trip	4	2/4	Yes(2)	P-10
Power Range High Neutron Flux (High Setpoint) Trip	4	2/4	Yes(2)	----
High Positive Flux Rate Trip	4	2/4	Yes(2)	----
Reactor Coolant Pump Bearing Water	16 (4/pump)	2/4 in any single pump	Yes(2)	P-10
Overtemperature ΔT	4 (2/loop)	2/4	Yes(2)	----
Overpower ΔT	4 (2/loop)	2/4	Yes(2)	----
Pressurizer Low Pressure Trip	4	2/4	Yes(2)	P-10
Pressurizer High Pressure Trip	4	2/4	Yes(2)	----
High-3 Pressurizer Water Level Trip	4	2/4	Yes(2)	P-10
Low Reactor Coolant Flow	8 (4/hot leg)	2/4 in either hot leg	Yes(2)	P-10
Reactor Coolant Pump Underspeed	4 (1/pump)	2/4	Yes(2)	P-10
Low Steam Generator Water Level	4/steam generator	2/4 in any steam generator	Yes(2)	----

Deleted: 8
Deleted: P-10
Deleted: 2/4 in 2/4 pumps
Deleted: Yes(2)
Deleted: High
Deleted: 8
Deleted: 2/4 in both legs
Deleted: Yes(2)
Deleted: P-10

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Table 7.2-3 (Sheet 1 of 2)

REACTOR TRIP PERMISSIVES AND INTERLOCKS

Designation	Derivation	Function
P-6	Intermediate range neutron flux above setpoint	Allows manual block of source range reactor trip
$\overline{\text{P-6}}$	Intermediate range neutron flux below setpoint	Automatically resets source range reactor trip
P-10	Power range nuclear power above setpoint	(a) Allows manual block of power range (low setpoint) reactor trip (b) Allows manual block of intermediate range reactor trip (c) Automatically blocks source range reactor trip (back-up to P-6) (d) Allows reactor trip on low coolant flow or reactor coolant pump high bearing water temperature in any single loop (e) Allows reactor trip on low reactor coolant pump speed (f) Allows reactor trip on high pressurizer water level (g) Allows reactor trip on low pressurizer pressure
P-10	Power range nuclear power below setpoint	(a) Prevents the block of power range (low setpoint) reactor trip (b) Prevents the block of intermediate range reactor trip (c) Permits manual reset of each source range channel reactor trip (d) Blocks reactor trip on low coolant flow or reactor coolant pump high bearing water temperature in any single loop (e) Blocks reactor trip on low reactor coolant pump speed (f) Blocks reactor trip on high pressurizer water level (g) Blocks reactor trip on low pressurizer pressure

Deleted: P-8 ... [16]
Deleted: multiple
Deleted: s
Deleted: multiple
Deleted: s

B 3.3.1 Reactor Trip System (RTS) Instrumentation

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

10. Reactor Coolant Flow – Low

a. Reactor Coolant Flow

The Reactor Coolant Flow – Low trip Function ensures that protection is provided against violating

the DNBR limit due to low flow in one or more RCS cold legs. Above the P-10 setpoint, a loss of flow in any RCS cold leg will actuate a reactor trip. Each RCS cold leg has four flow detectors to monitor flow. The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any event that results in a harsh environment.

The LCO requires four Reactor Coolant Flow – Low channels per cold leg to be OPERABLE in MODE 1 above P-10. Four OPERABLE channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 above the P-10 setpoint, when a loss of flow in one RCS cold leg could result in DNB conditions in the core, the Reactor Coolant Flow – Low trip must be OPERABLE.

Deleted: – Low (Single Cold Leg)
Deleted: (Single Cold Leg)
Deleted: 8
Deleted: 8
Deleted: 8
Deleted: (Single Cold Leg)
Deleted: In MODE 1 below the P-8 setpoint, a loss of flow in two or more cold legs is required to actuate a reactor trip (Function 10.b) because of the lower power level and the greater margin to the design limit DNBR.
Deleted: b. Reactor Coolant Flow – Low (Two Cold Legs)¶
Deleted: The Reactor Coolant Flow – Low
Deleted: (Two Cold Legs)
Deleted: trip Function ensures that protection is provided against violating the DNBR limit due to low flow in two or more RCS cold legs. Above the P-10 setpoint
Deleted: and below the P-8 setpoint
Deleted: , a loss of flow in two or more cold legs will initiate a reactor trip. Each cold leg has four flow detectors to monitor flow. The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any event that results in a harsh environment.
Deleted: The LCO requires four Reactor Coolant Flow – Low channels per cold leg to be OPERABLE in MODE 1 above P-10
Deleted: and below P-8
Deleted: . Four OPERABLE channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.
Deleted: In MODE 1 above the P-10 setpoint
Deleted: and below the P-8 setpoint
Deleted: , the Reactor Coolant Flow – Low
Deleted: (Two Cold Legs)
Deleted: trip must be OPERABLE. Below the P-10 setpoint, all re ... [17]
Deleted: distributions could occur that would cause a DNB conc ... [18]
Deleted: Above the P-8 setpoint, a loss of flow in any one cold le ... [19]

11. Reactor Coolant Pump (RCP) Bearing Water Temperature – High

    a. RCP Bearing Water Temperature – High

    The RCP Bearing Water Temperature – High reactor trip Function ensures that protection is provided against violating the DNBR limit due to a loss of flow in one RCS cold leg. Above the P-10 setpoint, high bearing water temperature in any RCP will initiate a reactor trip. The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any event that results in a harsh environment.

    The LCO requires four RCP Bearing Water Temperature – High channels per RCP to be OPERABLE in MODE 1 above P-10. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

    In MODE 1 above the P-10 setpoint, when a loss of flow in any RCS cold leg could result in DNB conditions in the core, the RCP Bearing Water Temperature – High trip must be OPERABLE.

Deleted: (Single Pump)

Deleted: (Single Pump)

Deleted: 8

Deleted: 8

Deleted: 8

Deleted: (Single Pump)

Deleted: In MODE 1 below the P-8 setpoint, a loss of flow in two or more cold legs is required to actuate a reactor trip because of the lower power level and the greater margin to the design limit DNBR.

Deleted: b. RCP Bearing Water Temperature – High (Two Pumps)¶

Deleted: The RCP Bearing Water Temperature – High

Deleted: (Two Pumps)

Deleted: reactor trip Function ensures that protection is provided against violating the DNBR limit due to a loss of flow in two or more RCS cold legs. Above the P-10 setpoint

Deleted: and below the P-8 setpoint

Deleted: , a high bearing water temperature in two or more RCPs will initiate a reactor trip. The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any event that results in a harsh environment.

Deleted: The LCO requires four RCP Bearing Water Temperature – High channels per RCP to be OPERABLE in MODE 1 above P-10

Deleted: and below P-8

Deleted: . Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

Deleted: In MODE 1 above the P-10 setpoint

Deleted: and below the P-8 setpoint

Deleted: , the RCP Bearing Water Temperature – High

Deleted: (Two Pumps)

Deleted: trip must be OPERABLE. Below the P-10 setpoint, all reactor trips on loss of flow are automatically blocked since no conceivable power distributions could occur that would cause a DNB concern at this low power level. Above the P-10 ... [20]

Deleted: Above the P-8 setpoint, a loss of flow in any one cold le ... [21]

16. Reactor Trip System Interlocks

Comment: Deleted b. Power Range Neutron Flux, P-8

b. Power Range Neutron Flux, P-10

Deleted: c

The Power Range Neutron Flux, P-10 interlock is actuated at approximately 10% power as determined by the respective PMS power-range detector. The LCO requirement for the P-10 interlock ensures that the following functions are performed:

- (1) on increasing power, the P-10 interlock automatically enables reactor trips on the following Functions:

  Pressurizer Pressure – Low,

  Pressurizer Water Level – High 3,

  Reactor Coolant Flow – Low,

  Deleted: (Both Hot Legs)

  RCP Bearing Water Temperature – High, and

  Deleted: (Two Pumps)

  RCP Speed – Low.

  These reactor trips are only required when operating above the P-10 setpoint (approximately 10% power). These reactor trips provide protection against violating the

  DNBR limit. Below the P-10 setpoint, the RCS is capable of providing sufficient natural circulation without any RCP running.

- (2) on increasing power, the P-10 interlock allows the operator to manually block the Intermediate Range Neutron Flux reactor trip.

- (3) on increasing power, the P-10 interlock allows the operator to manually block the Power Range Neutron Flux – Low Setpoint reactor trip.

- (4) on increasing power, the P-10 interlock automatically provides a backup block signal to the Source Range Neutron Flux reactor trip and also to de-energize the PMS source range detectors.

- (5) on decreasing power, the P-10 interlock automatically blocks reactor trips on the following Functions:

  Pressurizer Pressure – Low,

  Pressurizer Water Level – High 3,

  Reactor Coolant Flow – Low,

  RCP Bearing Water Temperature – High, and

  RCP Speed – Low.

- (6) on decreasing power, the P-10 interlock automatically enables the Power Range Neutron Flux – Low reactor trip and the Intermediate Range Neutron Flux reactor trip (and rod stop).

Deleted: (Two Cold Legs)

Deleted: (Two Pumps)

The LCO requires four channels of Power Range Neutron Flux, P-10 interlock to be OPERABLE in MODE 1 or 2.

In MODE 1, when the reactor is at power, the Power Range Neutron Flux, P-10 interlock must be OPERABLE. This Function must be OPERABLE in MODE 2 to ensure that core protection is provided during a startup or shutdown by the Power Range Neutron Flux – Low Setpoint and Intermediate

Range Neutron Flux reactor trips. In MODE 3, 4, 5, or 6, this Function does not have to be OPERABLE because the reactor is not at power and the Source Range Neutron Flux reactor trip provides core protection.

c. Pressurizer Pressure, P-11

Deleted: d

With pressurizer pressure channels less than the P-11 setpoint, the operator can manually block the Steam Generator Narrow Range Water Level – High 2 reactor Trip. This allows rod testing with the steam generators in cold wet layup. With pressurizer pressure channels > P-11 setpoint, the Steam Generator Narrow Range Water Level – High 2 reactor Trip is automatically enabled. The operator can also enable these actuations by use of the respective manual reset.

L.1.1, L.1.2, and L.2

Condition L is applicable to the Reactor Coolant Flow – Low (Single Cold Leg) and RCP Bearing Water Temperature – High (Single Pump) reactor trip Functions.

With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within [6] hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the

single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The [6] hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference [7].

If Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE. A Completion Time of an additional 4 hours is allowed to reduce power < P-10. Allowance of this time interval takes into consideration the redundant capability provided by the remaining two redundant OPERABLE channels and the low probability of occurrence of an event during this period that may require the protection afforded by this Function.

Deleted: 8

Deleted: O.1, O.2.1, O.2.2, and O.3¶
Condition O applies to the P-8 interlock. With one or two channels inoperable, the associated interlock must be verified to be in its required state for the existing plant condition within 1 hour, or the Functions associated with inoperable interlocks placed in a bypassed or tripped condition within [7] hours, or the unit must be placed in MODE 2 within 13 hours. Verifying the interlock manually accomplishes the interlock condition.

Deleted: If one interlock channel is inoperable, the associated Function(s) must be placed in a bypass or trip condition within [7] hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.)

Deleted: If two interlock channels are inoperable, one channel of the associated Function(s) must be bypassed and one channel of the associated Function(s) must be tripped. In this state, the logic becomes one-out-of-two, while still meeting the single failure criterion. The [7] hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference [7].

Deleted: If placing the associated Functions in bypass or trip is impractical, for instance as the result of other channels in bypass or trip, the Completion Time of an additional 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power in an orderly manner and without challenging plant systems.

B 3.4.4 RCS Loops

BASES

ACTIONS

A.1

If the requirements of the LCO are not met while in MODE 1 or 2, the Required Action is to reduce power and bring the plant to MODE 3 with the reactor trip breakers open. This lowers power level and thus reduces the core heat removal needs and minimizes the possibility of violating DNB limits.

Condition A is modified by a Note which requires completion of Required Action A.1 whenever the Condition is entered. This ensures that no attempt is made to restart a pump with the reactor trip breakers closed, thus precluding events which are unanalyzed.

When all four reactor coolant pumps are operating, a loss of a single reactor coolant pump above power level P-10 will result in an automatic reactor trip.

Deleted: 8

Deleted: When three reactor coolant pumps are operating, a loss of a single reactor coolant pump above power level P-10 will result in an automatic reactor trip.

The Completion Time of 6 hours is reasonable to allow for an orderly transition to MODE 3. The applicable safety analyses described above bound Design Basis Accidents (DBA) initiated with three reactor coolant pumps operating at power levels below P-10.

Deleted: 8

Deleted: , and with two reactor coolant pumps at power levels below P-10.

3.3.1 Reactor Trip System (RTS) Instrumentation

ACTIONS

L. One or two channels inoperable.	L.1.1	Place one inoperable channel in bypass or trip.	[6] hours
	AND		
	L.1.2	With two channels inoperable, place one channel in bypass and one channel in trip.	[6] hours
	OR		
	L.2	Reduce THERMAL POWER to < P-10.	10 hours

Deleted: 8

TABLE 3.3.1-1 (PAGE 2 OF 5)
REACTOR TRIP SYSTEM INSTRUMENTATION

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
6. Overtemperature ΔT	1,2	4	E	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.4 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11	Refer to Note 1 (Page 3.3.1-16)	Refer to Note 1 (Page 3.3.1-16)
7. Overpower ΔT	1,2	4	E	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11	Refer to Note 2 (Page 3.3.1-16)	Refer to Note 2 (Page 3.3.1-16)
8. Pressurizer Pressure a. Low Setpoint	1(f)	4	K	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11		≥ [1785] psig
b. High Setpoint	1,2	4	E	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11		≤ [2445] psig
9. Pressurizer Water Level – High 3	1(f)	4	K	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8		≤ [80]%*
10. Reactor Coolant Flow – Low	1(f)	4 per hot leg	L	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11		≥ [87]%(i)

(f) Above the P-10 (Power Range Neutron Flux) interlock.

(i) Percent of thermal design flow.

Deleted: a. Single Hot Leg [... [22]]

Deleted: ¶
(g) Above the P-8 (Power Range Neutron Flux) interlock.¶
(h) Above the P-10 (Power Range Neutron Flux) interlock and below the P-8 (Power Range Neutron Flux) interlock.

TABLE 3.3.1-1 (PAGE 3 OF 5)
REACTOR TRIP SYSTEM INSTRUMENTATION

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
11. Reactor Coolant Pump (RCP) Bearing Water Temperature – High	1(f)	4 per RCP	L	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8		≥ [230]°F*
12. RCP Speed – Low	1(f)	4	K	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8		≥ [90]%
13. Steam Generator (SG) Narrow Range Water Level – Low	1,2	4 per SG	E	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11		≥ [95,000] lbm
14. Steam Generator (SG) Narrow Range Water Level – High 2	1,2(k)	4 per SG	E	SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8 SR 3.3.1.11		≤ [100]%
15. Safeguards Actuation Input from Engineered Safety Feature Actuation System						
a. Manual	1,2	2	B	SR 3.3.1.10	N/A	N/A
b. Automatic	1,2	4	M	SR 3.3.1.6	N/A	N/A

(f) Above the P-10 (Power Range Neutron Flux) interlock.

(k) Above the P-11 (Pressurizer Pressure) interlock.

Deleted: a. Single Pump

Deleted: 1(g)

Deleted: 4 per RCP

Deleted: L

Deleted: SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8

Deleted: ≥ [320]°F*

Deleted: b. Two Pumps

Deleted: 1(h)

Deleted: 4 per RCP

Deleted: K

Deleted: SR 3.3.1.1 SR 3.3.1.6 SR 3.3.1.8

Deleted: ≥ [320]°F*

Deleted: ¶
(g) Above the P-8 (Power Range Neutron Flux) interlock.¶
(h) Above the P-10 (Power Range Neutron Flux) interlock and below the P-8 (Power Range Neutron Flux) interlock.

TABLE 3.3.1-1 (PAGE 4 OF 5)
REACTOR TRIP SYSTEM INSTRUMENTATION

FUNCTION	APPLICABLE MODES OR SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
16. Reactor Trip System Interlocks						
a. Intermediate Range Neutron Flux, P-6	2	4	N	SR 3.3.1.6 SR 3.3.1.9		≥ [1E-10] amps
b. Power Range Neutron Flux, P-10	1,2	4	N	SR 3.3.1.6 SR 3.3.1.9		[10]% RTP
c. Pressurizer Pressure, P-11	1,2	4	N	SR 3.3.1.6 SR 3.3.1.9		≤ [1970] psig
17. Reactor Trip Breakers	1,2 $3^{(i)},4^{(i)},5^{(i)}$	4 divisions with 2 RTBs per division	P,Q	SR 3.3.1.5	N/A	N/A
18. Reactor Trip Breaker (RTB) Undervoltage and Shunt Trip Mechanisms	1,2 $3^{(i)},4^{(i)},5^{(i)}$	1 each per RTB mechanism	P,Q	SR 3.3.1.5	N/A	N/A
19. Automatic Trip Logic	1,2 $3^{(i)},4^{(i)},5^{(i)}$	4 divisions 4 divisions	M R	SR 3.3.1.6 SR 3.3.1.6	N/A N/A	N/A N/A
20. ADS Stages 1, 2, and 3 Actuation input from engineered safety feature actuation system						
a. Manual	1,2 $3^{(i)},4^{(i)},5^{(i)}$	2 switch sets 2 switch sets	B B	SR 3.3.1.10 SR 3.3.1.10	N/A N/A	N/A N/A
b. Automatic	1,2 $3^{(i)},4^{(i)},5^{(i)}$	4 4	M R	SR 3.3.1.6 SR 3.3.1.6	N/A N/A	N/A N/A
21. Core Makeup Tank Actuation input from engineered safety feature actuation system						
a. Manual	1,2 $3^{(i)},4^{(i)},5^{(i)}$	2 switch sets 2 switch sets	B B	SR 3.3.1.10 SR 3.3.1.10	N/A N/A	N/A N/A
b. Automatic	1,2 $3^{(i)},4^{(i)},5^{(i)}$	4 4	M R	SR 3.3.1.6 SR 3.3.1.6	N/A N/A	N/A N/A

Deleted: b. . Power Range Neutron Flux, P-8 [... [23]

Deleted: d

15.3.1.1 Identification of Causes and Accident Description

A partial loss of coolant flow accident can result from a mechanical or an electrical failure of a reactor coolant pump or from a fault in the power supply to the pump or pumps. If the reactor is at power at the time of the event, the immediate effect of the loss of coolant flow is a rapid increase in the coolant temperature.

Normal power for the pumps is supplied through four buses connected to the generator. When a generator trip occurs, the buses are supplied from offsite power. The pumps continue to operate.

A partial loss of coolant flow is classified as a Condition II incident (a fault of moderate frequency), as defined in subsection 15.0.1.

Protection against this event is provided by the low primary coolant flow reactor trip signal, which is actuated by two-out-of-four low-flow signals. Above permissive P10, low flow in either hot leg actuates a reactor trip (see Section 7.2.

As specified in GDC 17 of 10 CFR Part 50, Appendix A, the effects of a loss of offsite power are considered in evaluating partial loss of forced reactor coolant flow transients. As discussed in subsection 15.0.14, the loss of offsite power is considered to be a potential consequence of the event due to disruption of the electrical grid following a turbine trip during the event. A delay of 3 seconds is assumed between the turbine trip and the loss of offsite power. In addition, turbine trip occurs 5.0 seconds following a reactor trip condition being reached. This delay on turbine trip is a feature of the AP1000 reactor trip system. The primary effect of the loss of offsite power is to cause the remaining operating reactor coolant pumps to coast down.

Deleted: 8

Deleted:). Between approximately 10-percent power (permissive P10) and the power level corresponding to permissive P8, low flow in both hot leg actuates a reactor trip

Deleted: and the power level corresponding to permissive P8

Deleted: , low flow in both hot leg actuates a reactor trip

15.3.2.1 Identification of Causes and Accident Description

A complete loss of flow accident may result from a simultaneous loss of electrical supplies to the reactor coolant pumps. If the reactor is at power at the time of the accident, the immediate effect of a loss of coolant flow is a rapid increase in the coolant temperature.

Electric power for the reactor coolant pumps is supplied through buses, connected to the generator through the unit auxiliary transformers. When a generator trip occurs, the buses receive power from external power lines and the pumps continue to supply coolant flow to the core.

A complete loss of flow accident is a Condition III event (an infrequent fault), as defined in subsection 15.0.1. The following signals provide protection against this event:

- Reactor coolant pump underspeed
- Low reactor coolant loop flow

The reactor trip on reactor coolant pump underspeed protects against conditions that can cause a loss of voltage to the reactor coolant pumps. This function is blocked below approximately 10-percent power (permissive P10).

The reactor trip on reactor coolant pump underspeed is also provided to trip the reactor for an underfrequency condition resulting from frequency disturbances on the power grid. If the maximum grid frequency decay rate is less than approximately 5 hertz per second, this trip protects the core from underfrequency events. WCAP-8424, Revision 1 (Reference 3), provides analyses of grid frequency disturbances and the resulting protection requirements that are applicable to the AP1000.

The reactor trip on low primary coolant loop flow is provided to protect against loss of flow conditions that affect only one or two reactor coolant loop cold legs. This function is generated by two-out-of-four low-flow signals per reactor coolant loop hot leg. Above permissive P10, low flow in either hot leg actuates a reactor trip. If the maximum grid frequency decay rate is less than approximately 2.5 hertz per second, this trip function also protects the core from this underfrequency event. This effect is described in WCAP-8424, Revision 1 (Reference 3).

Deleted: 8

Deleted: Between approximately 10-percent power (permissive P10) and the power level corresponding to permissive P8, low flow in both reactor coolant hot legs actuates a reactor trip.

Deleted: and the power level corresponding to permissive P8

Deleted: , low flow in both reactor coolant hot legs actuates a reactor trip.

II.8 OVERTEMPERATURE/OVERPOWER ΔT REACTOR TRIP MODIFICATIONS

The OTDT and OPDT reactor trips protect the core against DNB and excessive kw/ft. Their original formulas were selected for analog equipment requiring simple (and inexact) approximations for core limits and the core power calculation. In addition, hot leg streaming occurrs in the hot leg of pressurized water reactor systems. While the streaming effects on hot leg temperature measurement can be accounted for by RTD calibration at the beginning of the fuel cycle, recalibration to address changes in temperature streaming during fuel cycle operation are difficult. The use of modern computer based equipment permits much more exact formulas for the OTDT and OPDT reactor trip functions to be implemented. It also permits a simple recalibration of the measured core power as often as desired to minimize the effects of hot leg temperature streaming on the core power measurement. The result is a substantial reduction in the uncertainty of both the calculated reactor thermal power and the allowable power based on the measured reactor operating conditions.

The changes can be considered in two parts:

1. More accurate and more easily monitorable ΔT power signal.

   This change converts the linear ΔT approximation of thermal power to a true thermal power signal by calculating enthalpy at the measured hot and cold leg temperatures and pressure, and cold leg density at the cold leg temperature and pressure, and applying thermodynamic equations for thermal power (based on constant cold leg volumetric flow). Dynamic compenastion is applied to Tcold to compensate for transit times from the cold leg to the core, and independent dynamic compensation applied to Thot to compensate for the transit time from the core to the hot leg. The ΔT power signal can be directly compared with measured calorimetric reactor power.

   The existing ΔT formulation approximates the changes in density and heat capacity by modifying the trip setpoint (including rate-of-change in T_{avg}), such that the existing ΔT signal cannot be directly compared with the measured calorimetric power.

   This modification includes the Technical specification requirement to maintain the ΔT power signal within 1% RTP of the calorimetric power, monitoring that variation, and correcting when and if necessary. This is very similar to the existing requirement to maintain the indicated neutron flux signal with a certain percent of the measured calorimetric power. The comparison will be a simple check done be shift operators.

2. Convert trip setpoint to input tables.

The original OTDT design requires linearizing the non-linear core DNB limits. The revised design change uses digital technology to input the non-linear core limits as tables.

The following text details all the changes that are rquired to implement this modification.

7.2.1.1.3 Core Heat Removal Trips

Overtemperature ΔT Reactor Trip

The overtemperature ΔT trip provides core protection to prevent departure from nucleate boiling for combinations of pressure, power, coolant temperature, and axial power distribution. The protection is provided if the transient is slow with respect to piping transient delays from the core to the temperature detectors and pressure is within the range between the high and low pressure reactor trips. This setpoint includes corrections for changes in density and heat capacity of water with temperature and dynamic compensation for piping delays from the core to the loop temperature detectors. With normal axial power distribution, this reactor trip limit is always below the core safety limit. If axial peaks are greater than design, as indicated by the difference between upper and lower power range nuclear detectors, the reactor trip is automatically reduced according to the following calculation. Two hot leg temperature measurements per loop are combined with individual cold leg temperature measurements to form four ΔT power signals, $q_{\Delta T}$.

Deleted: and T_{avg}

Inserted: power

The ΔT power signal, $q_{\Delta T}$, is the calculated core power based on the properties of compressed water at the measured hot leg T_H, cold leg temperature, T_C, and pressurizer pressure, P_{PZR}:

$$q_{\Delta T} = f(T_H, T_C, P_{PZR})$$

$$q_{\Delta T} = \rho(T_C, P_{PZR})[h(T_H, P_{PZR}) - h(T_C, P_{PZR})]/\Delta T^{\circ}$$

Where:

T_C = $[(1+\tau_1 s)/(1+\tau_2 s)]T_{COLD}$, where T_{COLD} is the measured cold leg temperature (lead/lag compensation applied to compensate for cold leg-to-core transit time)

T_H = $[(1+\tau_3 s)/(1+\tau_4 s)]T_{HOT}$, where T_{HOT} is the measured hot leg temperature (lead/lag compensation applied to compensate for core-to-hot leg transit time)

$\rho(T_C, P_{PZR})$ = density of water at cold leg temperature in the cold leg (T_C) and pressure, P_{PZR}

$h(T, P_{PZR})$ = = enthalpy of water at the specified temperature (T_H or T_C) and pressure P_{PZR}

ΔT° = a conversion factor, such that the value of $q_{\Delta T}$ is 100 percent at normal rated thermal power

s = Laplace transform operator

The ΔT setpoint for the overtemperature trip is continuously calculated, with one set of temperature measurements per loop by interpolating from tabulated core safety limits, with correction (if needed) for adverse axial power distribution.

Deleted: this

$$OT\Delta T_{SP} = OT\Delta T^{\circ}_{SP} - f_1(\Delta I)$$

Where:

$f_1(\Delta I)$ = the penalty associated with an adverse axial power distribution

$OT\Delta T^{\circ}_{SP}$ = the core DNB thermal design limit with design axial power distribution

$OT\Delta T^{\circ}_{SP}$ = $f(P_{PZR},T_C)$. The function, f(P,T), is determined by interpolation from specified tables of allowable core thermal power as a function of core inlet temperature at various pressures.

P_{PZR} and T_C, pressurizer pressure and cold leg temperature, are as defined previously

A reactor trip is initiated if $q_{\Delta T} \geq OTDT_{SP}$ in two of the four divisions

Two separate ionization chambers supply the upper and lower flux signal for each overtemperature ΔT channel.

Increases in ΔI beyond a predefined deadband results in a decrease in trip setpoint.

The required one pressurizer pressure parameter per loop is obtained from four separate sensors connected to pressure taps at the top of the pressurizer.

Overpower ΔT Trip

The overpower ΔT reactor trip provides confidence of fuel integrity during overpower conditions, limits the required range for overtemperature ΔT protection, and provides a backup to the power range high neutron flux trip.

A reactor trip is initiated if the ΔT power signal, $q_{\Delta T}$, exceeds the setpoint in two of the four divisions; i.e.,

$$q_{\Delta T} \geq \quad OPDT_{SP} = K_4 - f_2(\Delta I),$$

Where

$q\Delta T$ is the same ΔT power signal used for the Overtemperature ΔT reactor trip

K4 = A preset bias

$f_2(\Delta I)$ = A function of the neutron flux difference between upper and lower ionization chamber flux signals; to correct, if necessary, for an adverse axial flux shape

Deleted: ¶
If $\frac{\Delta T(1+\tau_4 s)}{(1+\tau_5 s)} \geq \Delta T$ setpoint, a reactor trip is initiated.¶
ΔT setpoint is calculated from the following equation:¶
<#> $\Delta T_{SETPOINT} = \Delta T_o \left[K_1 - K_2 \right.$
¶
Where:¶
ΔT = Measured ΔT by resistance temperature detector instrumentation¶
ΔT_o = Indicated ΔT at rated thermal power¶
T_{avg} = Average reactor coolant temperature (°F) ¶
T°_{avg} = Nominal T_{avg} at rated thermal power¶
P = Pressurizer pressure (psig)¶
P_o = Nominal operating pressure¶
K_1 = Preset bias¶
K_2 = Preset gain which compensates for effects of temperature on the departure from nucleate boiling limits¶
K_3 = Preset gain which compensates for effects of pressure on the departure from nucleate boiling limits¶
τ_1, τ_2 = Preset constants which compensate for piping and instrument time delay(s)¶
τ_4, τ_5 = Preset constants used in lead-lag compensator for ΔT¶
$f_1(\Delta\varphi)$ = A function of the neutron flux difference between upper and lower ionization chamber flux signals ¶

Deleted: φ

Deleted: The ΔT setpoint for this trip is continuously calculated for each loop. ¶
If $\Delta T \frac{(1+\tau_4 s)}{(1+\tau_5 s)} \geq \Delta T$ setpoint, a reactor trip is initiated.

Deleted: ¶
ΔT setpoint is calculated from the following equation:¶
<#> $\Delta T_{SETPOINT} = \Delta T_o \left[K_4 - K_5 \right.$
¶
Where:¶
ΔT = Measured ΔT by resistance temperature detector instrumentation¶
ΔT_o = Indicated ΔT at rated thermal power¶
$f_2(\Delta\varphi)$ = A function of the neutron flux difference between upper and lower ionization chamber flux signals¶
K_5 = A constant which is equal to zero for decreasing T_{avg}¶
K_6 = A constant which is equal to zero for T_{avg} less than T'_{avg}¶
T'_{avg} = Indicated T_{avg} at rated thermal ... [24]

Increases in ΔI beyond a predefined deadband results in a decrease in trip setpoint

The source of temperature and neutron flux information is identical to that of the overtemperature ΔT trip, and the resultant ΔT setpoint is compared to the same measured ΔT power signal. Figure 7.2-1, sheet 5, shows the logic for this trip function.

Deleted: ¶

7.2.2.2.4 Conformance to Requirements on the Derivation of System Inputs for Reactor Trip (Paragraph 6.4 of IEEE 603-1991)

To the extent feasible, inputs used for reactor trip are derived from signals that are direct measurements of the desired variables. Two exceptions exist, overtemperature and overpower, which cannot be directly measured. The process variables that do affect these parameters can be measured and they are used to continuously calculate the setpoints.

The overtemperature ΔT trip setpoint is calculated from pressurizer pressure, reactor coolant temperature, and nuclear axial power shape. The setpoint is compared against the measured ΔT power signal.

Overpower ΔT is calculated from reactor coolant temperature and the nuclear axial power shape in the core. This value is compared against the measured ΔT power signal.

2.0 SAFETY LIMITS (SLS)

SLS

2.1.1 Reactor Core SLs

In MODES 1 and 2, the combination of THERMAL POWER, Reactor Coolant System (RCS) highest loop cold leg temperature, and pressurizer pressure shall not exceed the limits specified in the COLR; and the following SLs shall not be exceeded:

Deleted: average

2.1.1.1 The departure from nucleate boiling ratio (DNBR) shall be maintained ≥ [1.14 for the WRB-2M DNB correlations].

2.1.1.2 The peak fuel centerline temperature shall be maintained < [5080°F, decreasing by 58°F per 10,000 MWD/MTU of burnup].

2.1.2 RCS Pressure SL

In MODES 1, 2, 3, 4, and 5 the RCS pressure shall be maintained ≤ 2733.5 psig.

TABLE 3.3.1-1 (PAGE 5 OF 5)
REACTOR TRIP SYSTEM INSTRUMENTATION

Note 1: Overtemperature ΔT

The ΔT power signal, $q_{\Delta T}$, shall not be less than the measured reactor thermal power by more than [1]% of RTP, where the ΔT power signal, $q_{\Delta T}$, is computed as

$$q_{\Delta T} = \rho(T_C,P_{PZR})[h(T_H,P_{PZR}) - h(T_C,P_{PZR})]/\Delta T^\circ$$

where:

T_C = $[(1+\tau_1 s)/(1+\tau_2 s)]T_{COLD}$, where T_{COLD} is the measured cold leg temperature, °F, with lead/lag compensation applied to compensate for cold leg-to-core transit time

T_H = $[(1+\tau_3 s)/(1+\tau_4 s)]T_{HOT}$, where T_{HOT} is the measured hot leg temperature, °F, with lead/lag compensation applied to compensate for core-to-hot leg transit time

$\tau_1 \geq$ [*] sec $\tau_2 \leq$ [*] sec

$\tau_4 \geq$ [*] sec $\tau_5 \leq$ [*] sec

$\rho(T_C,P_{PZR})$ = density of water at the measured cold leg temperature in the cold leg (T_C), °F, and measured pressurizer pressure, P_{PZR}, psia

$h(T,P_{PZR})$ = enthalpy of water at the specified measured temperature (T_H or T_C) and measured pressurizer pressure, P_{PZR}, psia

ΔT° = a conversion factor, such that the value of $q_{\Delta T}$ is 100 percent at normal rated thermal power

s = Laplace transform operator

And, the Overtemperature ΔT setpoint shall not exceed the following nominal Trip Setpoint by more than [0.2% of RTP for T_{HOT}; 0.2% of RTP for T_{COLD}; 0.06% of RTP for pressure; and 0.14% of RTP for ΔI]R.

$OT\Delta T_{SP} = OT\Delta T^{\circ}_{SP} - f_1(\Delta I)$

where:

$OT\Delta T^{\circ}_{SP}$ = f(P_{PZR},T_C), determined by interpolation from tables [*] of allowable core thermal power as a function of core inlet temperature at various pressures.

P_{PZR} and T_C, pressurizer pressure and cold leg temperature, are as defined above.

$f_1(\Delta I)$ =	[*] {[*] + (q_t - q_b)}	when q_t - q_b ≤ -[*]% RTP
	0% of RTP	when -[*]% RTP < q_t - q_b ≤ [*]% RTP
	-[*]{(q_t - q_b) - [*]}	when q_t - q_b > [*]% RTP

Where q_t and q_b are percent RTP in the upper and lower halves of the core respectively, and q_t + q_b is the total THERMAL POWER in percent RTP.

*These values denoted with [*] are specified in the COLR.

Note 2: Overpower ΔT

The Overpower ΔT setpoint shall not exceed the following nominal Trip Setpoint by more than [0.2% of RTP for T_{HOT}; and 0.2% of RTP for T_{COLD}].

$OPDT_{SP} = K_4 - f_2(\Delta I)$

Where:

K_4 ≤ [*]

$f_2(\Delta I)$ = [*]

*These values denoted with [*] are specified in the COLR.

Deleted: Function Allowable Value

Deleted: ΔT span

Deleted: $\Delta T \frac{(1+\tau_4 s)}{(1+\tau_5 s)} \le \Delta T_0 \{K_1 - K_2 \frac{(}{(}$

Deleted: ¶

Deleted: Where: ΔT is measured RCS ΔT, °F.¶
ΔT_0 is the indicated ΔT at RTP, °F.¶
s is the Laplace transform operator, sec^{-1}.¶
T is the measured RCS average temperature, °F.¶
T' is the indicated T_{avg} at RTP, ≤ [*]°F.¶
P is the measured pressurizer pressure, psig.¶
P' is the nominal RCS operating pressure, 2235 psig.¶
K_1 ≤ [*] K_2 ≥ [*]/°F K_3 ≥ [*]/psig¶
τ_1 ≥ [*] sec τ_2 ≤ [*] sec¶
τ_4 ≥ [*] sec τ_5 ≤ [*] sec¶

Deleted: Function Allowable Value

Deleted: % of

Deleted: ΔT span

Deleted: $\Delta T \frac{(1+\tau_4 s)}{(1+\tau_5 s)} \le \Delta T_0 \{K_4 - K_5 \frac{}{1}$

Deleted: ΔT is measured RCS ΔT, °F.¶
ΔT_0 is the indicated ΔT at RTP, °F.¶
s is the Laplace transform operator, sec^{-1}.¶
T is the measured RCS average temperature, °F.¶
T" is the nominal T_{avg} at RTP, ≤ [*]°F.

Deleted: K_5 ≥ [*]/°F for increasing T_{avg} K_6 ≥ [*]/°F when T > T"¶
[*]/°F for decreasing T_{avg} [*]/°F when T ≤ T"¶
τ_3 ≥ [*] sec τ_4 ≥ [*] sec τ_5 ≤ [*] sec

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY

6. Overtemperature ΔT

The Overtemperature ΔT trip Function ensures that protection is provided to ensure that the design limit DNBR is met. This trip Function also limits the range over which the Overpower ΔT trip Function must provide protection. The inputs to the Overtemperature ΔT trip include all combinations of pressure, power, coolant temperature, and axial power distribution, assuming full reactor coolant flow. Protection from violating the DNBR limit is assured for those transients that are slow with respect to delays from the core to the measurement system. The Overtemperature ΔT trip Function uses the measured T_{HOT} and T_{COLD} in each loop, together with the measured pressurizer pressure, to compute the reactor core thermal power. Equations to fit the properties of density and enthalpy are programmed in the software, such that the ΔT power signal is presented as a percent of RTP for direct comparison with measured calorimetric power. The overtemperature ΔT setpoint is automatically varied for changes in the parameters that affect DNB as follows:

Deleted: each loop ΔT as a measure of reactor power and is automatically varied with the following parameters:

- reactor core inlet temperature – the Trip Setpoint is varied to correct for changes in core inlet temperature based on measured changes in cold leg temperature with dynamic compensation to account for cold leg-to-core transit time;

Deleted: coolant average

Deleted: coolant density and specific heat capacity with changes in coolant temperature

- pressurizer pressure – the Trip Setpoint is varied to correct for changes in system pressure; and
- axial power distribution – the Trip Setpoint is varied to account for imbalances in the axial power distribution as detected by the PMS upper and lower power range detectors. If axial peaks are greater than the design limit, as indicated by the difference between the upper and lower PMS power range detectors, the Trip Setpoint is reduced in accordance with Note 1 of Table 3.3.1-1.

Dynamic compensation of the ΔT power signal is included for system piping delays from the core to the temperature measurement system. The Overtemperature ΔT trip Function is calculated for each loop as described in Note 1 of Table 3.3.1-1. This Function also provides a signal to generate a turbine runback prior to reaching the Trip Setpoint. A turbine runback will reduce turbine power and reactor power. A reduction in power will normally alleviate the Overtemperature ΔT condition and may prevent a reactor trip. No credit is taken in the safety analyses for the turbine runback.

The LCO requires four channels of the Overtemperature ΔT trip Function to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. Note that the Overtemperature ΔT Function receives input from channels shared with other RTS Functions. Failures that affect multiple Functions require entry into the Conditions applicable to all affected Functions.

In MODE 1 or 2, the Overtemperature ΔT trip must be OPERABLE to prevent DNB. In MODE 3, 4, 5, or 6, this trip Function does not have to be OPERABLE because the reactor is not operating and there is insufficient heat production to be concerned about DNB.

7. Overpower ΔT

The Overpower ΔT trip Function ensures that protection is provided to ensure the integrity of the fuel (i.e., no fuel pellet melting and less than 1% cladding strain) under all possible overpower conditions. This trip Function also limits the required range of the Overtemperature ΔT trip function and provides a backup to the Power Range Neutron Flux – High Setpoint trip. The Overpower ΔT

trip Function ensures that the allowable heat generation rate (kW/ft) of the fuel is not exceeded. It uses the same ΔT power signal generated for the Overtemperature ΔT. The setpoint is automatically varied with the following parameters:

Deleted: of each loop as a measure of reactor power and

•

Deleted: reactor coolant average temperature – the Trip Setpoint is varied to correct for changes in coolant density and specific heat capacity with changes in coolant temperature; and

axial power distribution – the Trip Setpoint is varied to account for imbalances in the axial power distribution as detected by the PMS upper and lower power range detectors. If axial peaks are greater than the design limit, as indicated by the difference between the upper and lower PMS power range detectors, the Trip Setpoint is reduced in accordance with Note 2 of Table 3.3.1-1.

Deleted: rate of change of reactor coolant average temperature – including dynamic compensation for the delays between the core and the temperature measurement system.¶

II.9 FLUX DOUBLING/BORON DILUTION MODIFICATIONS

The "Flux Doubling" calculation is used to block a potential inadvertent boron dilution event during shutdown conditions. The following paragraphs summarize the changes that have been made to it to ensure that it can perform its safety function while permitting required operating flexibility during normal plant operation.

- Figure 7.2-1, Sheet 3 was changed to add a "one shot" function to the reset logic for the flux doubling function. This is to prevent a standing logical "1" input from existing in the logic whenever the intermediate range neutron flux is below the P-6 permissive setpoint. By doing so, the Memory with Actuation Block or "L/R Latch" function in the reset path, that is an edge dependent logic function, can accept a manual reset if required at some later time. The existing logic, without this change, would prevent any manual reset of the function any time after reactor shutdown until the P-6 permissive had been cleared during the following reactor startup. The existing logic could, therefore, have prevented the operators from being able to reset the function after it had been manually blocked during startup if the P-6 setpoint had not first been exceeded. The result in such a case would have been a deliberate violation of the technical specifications. The revised logic eliminates this potential conflict and will permit the function to be reset at any time.

- Technical Specifications Table 3.3.2-1, Note (f) required the flux doubling calculation to be active whenever below the P-6 setpoint. Reactor criticality normally occurs below the P-6 setpoint. The result of the note as written would be to have the boron dilution function actuate every time that the operators intentionally attempt to perform a reactor startup. The revised Note (f) supports the intended function of the flux doubling calculation to prevent inadvertent criticality while permitting intended and required operations during routine reactor startup.

- The "Limiting Setpoint Assumed in Analyses" for "Boron dilution block on source range flux doubling" in table 15.0-4a was increased from 1.6 to 2.2. The original setpoints selected for the flux doubling calculation for the analysis of the postulated decrease in the reactor coolant system boron concentration during shutdown as analyzed in Section 15.4.6 of the Accident Analyses were 1.6 and 50 minutes. Boron dilution protection functions would be actuated if the source range neutron flux were to increase by 60% (i.e., a factor of 1.6) during any rolling 50 minute interval. An analysis of the setpoints indicate that there is a significant likelihood that they could lead to inadvertent actuation of the boron dilution protection actions when the plant is shut down and the flux doubling function is active, even if no actual change in core neutron multiplication were occurring. This is due to the inherent variability of counting a discrete random process such as the leakage of neutrons from a reactor core, especially at relatively low count rates. A reanalysis of the event has been performed and it has been verified that an increase in the nominal setpoint from 1.6 to 2.2 demonstrates acceptable results. This increase in the nominal setpoint will substantially reduce the likelihood of inadvertent actuation during normal operation.

- The existing design realigns the makeup pump suction from the demineralized water tank to the boric acid tank to terminate the potential boron dilution and to begin to reborate the reactor coolant system to restore shutdown margin. These actions would initially cause the boron dilution to continue because the volume of water in the makeup line path would still be unborated until borated water from the boric acid tank began to reach the reactor coolant system. The function was changed to close the makeup line isolation valves (as well as the demineralized water isolation valves) to terminate the event as soon as possible. Long term recovery from the event would then be accomplished using either a different flow path with a smaller unpurged volume or by using the makeup line after purging most of the unborated water in it.

The following text changes along with the logic changes on Figure 7.2-1, Sheet 3 are rquired to implement this modication.

7.3.1.2.14 Boron Dilution Block

Signals to block boron dilution are generated from any of the following conditions:

1. Excessive increasing rate of source range flux doubling signal
2. Loss of ac power sources (low Class 1E battery charger input voltage)
3. Reactor trip (Table 7.3-2, interlock P-4)

Deleted: nuclear
Deleted: power

In the event of an excessive increasing rate of source range flux doubling signal, the block of boron dilution is accomplished by closing the chemical and volume control system makeup isolation valves and closing the makeup pump suction valves to the demineralized water storage tanks. This signal also provides an non-safety trip of the makeup pumps. These actions terminate the supply of potentially unborated water to the reactor coolant system as quickly as possible.

Deleted: T
Deleted: , and
Deleted: aligning the boric acid tank to the reactor coolant system makeup pumps

In the event of a loss of ac power sources or a reactor trip (as indicated by P-4), the block of boron dilution is accomplished by closing the makeup pump suction valves to the demineralized water storage tanks and aligning the boric acid tank to the suction of the makeup pumps. This permits makeup as needed but ensures that it will be from a borated source that will not reduce the available shutdown margin in the reactor core.

Condition 1 is an average of the source range count rate, sampled at least N times over the most recent time period T_1, compared to a similar average taken at time period T_2 earlier. If the ratio of the current average count rate to the earlier average count rate is greater than a preset value, a partial trip is generated in the division. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, boron dilution is blocked. This source range flux doubling signal may be manually blocked to permit plant startup and normal power operation. It is automatically reinstated when reactor power is decreased below the P-6 power level during shutdown.

Condition 2 results from the loss of ac power. A short, preset time delay is provided to prevent actuation upon momentary power fluctuations; however, actuation occurs before ac power is restored by the onsite diesel generators. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by each of the two sensors connected to two of the four battery chargers. The two-out-of-four logic is based on an undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

Condition 3 results from a reactor trip as indicated by the P-4 interlock.

The functional logic relating to the boron dilution block is illustrated in Figure 7.2-1, sheets 3 and 15.

7.3.1.2.15 Chemical and Volume Control System Isolation

A signal to close the isolation valves of the chemical and volume control system is generated from any of the following conditions:

1. High-2 pressurizer level
2. High-2 steam generator narrow range water level
3. Automatic or manual safeguards actuation signal (subsection 7.3.1.1) coincident with High-1 pressurizer level
4. High-2 containment radioactivity
5. Manual initiation
6. Excessive increasing rate of source range flux doubling signal

Condition 1 results from the coincidence of pressurizer level above the High-2 setpoint in any two of the four divisions. This function can be manually blocked when the reactor coolant system pressure is below the P-19 permissive setpoint to permit pressurizer water solid conditions with the plant cold and to permit pressurizer level makeup during plant cooldowns. This function is automatically unblocked when reactor coolant system pressure is above the P-19 setpoint.

Condition 2 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator.

Condition 3 results from the coincidence of two of the four divisions of pressurizer level above the High-1 setpoint, coincident with an automatic or manual safeguards actuation.

Condition 4 results from the coincidence of containment radioactivity above the High-2 setpoint in any two of the four divisions.

Condition 5 consists of two momentary controls. This action also initiates auxiliary spray and letdown purification line isolation (subsection 7.3.1.2.18).

Condition 6 is an average of the source range count rate, sampled at least N times over the most recent time period T1, compared to a similar average taken at time period T2 earlier. If the ratio of the current average count rate to the earlier average count rate is greater than a preset value, a partial trip is generated in the division. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, boron dilution is blocked. The Flux Doubling function is also delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious isolation due to the short term instability of the processed source range values. This source range flux doubling signal may be manually blocked to permit plant startup and normal power operation. It is automatically reinstated when reactor power is decreased below the P-6 power level during shutdown.

The functional logic relating to chemical and volume control system isolation is illustrated in Figure 7.2-1, sheets 3, 6 and 11.

Table 7.3-1 (Sheet 6 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
13. Block of Boron Dilution (Figure 7.2-1, Sheets 3 and 15)			
a. Flux doubling calculation	4	2/4-BYP[1]	Manual block permitted when critical or intentionally approaching criticality. Automatically unblocked below P-6
b. Undervoltage to Class 1E battery chargers	2/charger	2/2 per charger and 2/4 chargers[5]	None
c. Reactor trip (P-4)	1/division	2/4	None
14. Chemical Volume Control System Isolation (See Figure 7.2-1, Sheets 3, 6 and 11)			
f. Flux doubling calculation	4	2/4-BYP[1]	Manual block permitted when critical or intentionally approaching criticality Automatically unblocked below P-6

Deleted: above P-6

Table 7.3-4 (Sheet 2 of 2)

ENGINEERED SAFETY FEATURES ACTUATION, VARIABLES, LIMITS, RANGES, AND ACCURACIES (NOMINAL)

Variables to be Monitored	Range of Variables	Typical Accuracy	Typical Response Time (Sec)
Pressurizer water level	0 to 100% of cylindrical portion of pressurizer	± 2.25% of span	1.2(1)
Startup feedwater flow	0 to 1000 gpm	4.0% of span	1.6(1)
Neutron flux (flux doubling calculation)	1 to 10^6 c/sec	± 30% of span	1.0(3)
Control room supply air radiation level	10^{-7} to 10^{-2} μ Ci/cc	± 5.0% of full scale	5.0(1)
Containment radioactivity	10^0 to 10^7 R/hr	± 5.0% of full scale	5.0(1)

Deleted: 11
Deleted: .0
Deleted: 10
Deleted: (1)

Notes:
1. Listed response time is the time for a step change of a variable, from 5% below to 5% above the setpoint, to reach the actuated device.
2. Listed response time is the time for a negative 20% step change of steam line pressure to reach the actuated device.
3. Response time depends on flux doubling calculation

Deleted: time constant

DCD Figure 9.3.6-1 Sheet Revisions

Sheet 1, Note 8 – Change text to read "...High 1 Pressurizer Level, High-High Radiation, or Flux Doubling Signal"
Sheet 2, Note 3 – Add text "Pumps Stop on receipt of Flux Doubling Signal" to existing note.
Sheet 2, Note 8 – Remove text "A Source Range Flux Doubling Signal" from the existing note.

DCD Subsection 9.3.6.3.7 Revision

Makeup Line Containment Isolation Valves

These normally open, motor-operated globe valves provide containment isolation of the chemical and volume control system makeup line and automatically close on a high-2 pressurizer level, high steam generator level, or high-2 containment radiation signal from the protection and safety monitoring system. The valves close on a source range flux doubling signal to terminate possible unplanned boron dilution events. The valves also close on a safeguards actuation signal coincident with high-1 pressurizer level. This allows the chemical and volume control system to continue providing reactor coolant system makeup flow, if the makeup pumps are operating following a safeguards actuation signal. These valves are also controlled by the reactor makeup control system and close when makeup to other systems is provided. Manual control is provided in the main control room and at the remote shutdown workstation.

Table 15.0-4a (Sheet 2 of 2)

PROTECTION AND SAFETY MONITORING SYSTEM SETPOINTS AND TIME DELAY ASSUMED IN ACCIDENT ANALYSES

Function	Limiting Setpoint Assumed in Analyses	Time Delays (seconds)
"S" signal on high-1 containment pressure	8 psig	2.0
Reactor coolant pump trip following "S"	–	15.0
PRHR actuation of high-3 pressurizer water level	80% of span	2.0 (plus 15.0-second timer delay)
Chemical and volume control system isolation on high-2 pressurizer water level	67% of span	2.0
Chemical and volume control system isolation on high-1 pressurizer water level coincident with "S" signal	30% of span	2.0
Boron dilution block on source range flux doubling	2.2 over 50 minutes	80.0
ADS Stage 1 actuation on core makeup tank low level signal	67.5% of tank volume	20.0 seconds for control valve to begin to open)
ADS Stage 4 actuation on core makeup tank low-low level signal	20% of tank volume	30.0 seconds for squib valve to begin to open)

Deleted: 1.6
Deleted: 10
Deleted: .0
Deleted: multiplication

Table 15.0-6 (Sheet 3 of 4)

PLANT SYSTEMS AND EQUIPMENT AVAILABLE FOR TRANSIENT AND ACCIDENT CONDITIONS

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 15.4 (Cont.)			
Uncontrolled RCCA bank withdrawal at power	Power range high neutron flux, high power range positive neutron flux rate, overtemperature ΔT, over-power ΔT, high pressurizer pressure, high pressurizer water level, manual	–	Pressurizer safety valves, steam generator safety valves
RCCA misalignment	Overtemperature ΔT, manual	–	–
Startup of an inactive reactor coolant pump at an incorrect temperature	Power range high flux, low flow (P-8 interlock), manual	–	–
Chemical and volume control system malfunction that results in a decrease in boron concentration in the reactor coolant	Source range high flux, overtemperature ΔT, manual	Source range flux doubling	CVS to RCS isolation valves, makeup pump suction isolation valves from the demineralized water transfer and storage system
Spectrum of RCCA ejection accidents	Power range high flux, high positive flux rate, manual	–	Pressurizer safety valves

Deleted: Low insertion limit annunciators

15.4.6.1 Identification of Causes and Accident Description

Other than control rod withdrawal, the principal means of positive reactivity insertion to the core is the addition of unborated, primary-grade water from the demineralized water transfer and storage system into the reactor coolant system through the reactor makeup portion of the chemical and volume control system. Normal boron dilution with these systems is manually initiated under strict administrative controls requiring close operator surveillance. Procedures limit the rate and duration of the dilution. A boric acid blend system is available to allow the operator to match the makeup water boron concentration to that of the reactor coolant system during normal charging.

An inadvertent boron dilution is caused by the failure of the demineralized water transfer and storage system or chemical and volume control system, either by controller, operator or mechanical failure. The chemical and volume control system and demineralized water transfer and storage system are designed to limit, even under various postulated failure modes, the potential rate of dilution to values that, with indication by alarms and instrumentation, allowing sufficient time for automatic or operator response to terminate the dilution.
An inadvertent dilution from the demineralized water transfer and storage system through the chemical and volume control system may be terminated by isolating the makeup flow to the reactor coolant system, by isolating the makeup pump suction line to the demineralized water transfer and storage system storage tank or by tripping the makeup pumps. Lost shutdown margin may be regained by adding borated water (greater than 4000 ppm) to the reactor coolant system from the boric acid tank.
Generally, to dilute, the operator performs two actions:

- Switch control of the makeup from the automatic makeup mode to the dilute mode.
- Start the chemical and volume control system makeup pumps.

Failure to carry out either of those actions prevents initiation of dilution. Because the AP1000 chemical and volume control system makeup pumps do not run continuously (they are expected to be operated once per day to make up for reactor coolant system leakage), a makeup pump is started when the volume control system is placed into dilute mode.
The status of the reactor coolant system makeup is available to the operator by the following:

- Indication of the boric acid and blended flow rates
- Chemical and volume control system makeup pumps status
- Deviation alarms, if the boric acid or blended flow rates deviate by more than the specified tolerance from the preset values
- When reactor is subcritical
  - High flux at shutdown alarm
  - Indicated source range neutron flux count rates
  - Audible source range neutron flux count rate
  - Source range neutron flux-multiplication alarm

Deleted: .

Deleted: Flow from the demineralized water transfer and storage system, which is the source of unborated water, may be terminated by closing isolation valves in the chemical and volume control system.

Deleted: opening the isolation valve to the boric acid tank and thus allowing the addition of

- When the reactor is critical
  - Axial flux difference alarm (reactor power ≥ 50 percent rated thermal power)
  - Control rod insertion limit low and low-low alarms
  - Overtemperature ΔT alarm (at power)
  - Overtemperature ΔT reactor trip
  - Power range neutron flux-high, both high and low setpoint reactor trips.

This event is a Condition II incident (a fault of moderate frequency), as defined in subsection 15.0.1.

15.4.6.2.2 Dilution During Cold Shutdown (Mode 5)

The following conditions are assumed for inadvertent boron dilution while in this operating mode:

- A dilution flow of 175 gpm of unborated water exists.

- A volume of 2592.5 ft^3 is a conservative estimate of the minimum active reactor coolant system volume corresponding to the water level at mid-loop in the vessel while on normal residual heat removal. The assumed active volume does not include the volume of the reactor vessel upper head region.

- Control rods are fully inserted, which is the normal condition in cold shutdown and a critical boron concentration of 1483 ppm. This is a conservative boron concentration with control rods inserted and allows for the most reactive rod to be stuck in the fully withdrawn position.

- The shutdown margin is equal to 1.6-percent $\Delta k/k$, the minimum value required by the Technical Specifications for the cold shutdown mode. Combined with the preceding, this gives a shutdown boron concentration of 1675 ppm.

- At least one reactor coolant pump will be normally operating during plant operation in Mode 5. It may be possible under some conditions, however, to operate the plant in Mode 5 with no reactor coolant pumps operating. For this reason, the mixing volume assumed for the analysis in Mode 5 will include the reactor coolant loop and normal residual heat removal system volumes that are being actively mixed by the residual heat removal system pumps.

In the event of an inadvertent boron dilution transient during cold shutdown, the source range nuclear instrumentation detects an increase in the neutron flux by comparing the current source range flux to that of about 50 minutes earlier. Upon detecting a sufficiently large flux increase, an alarm is sounded for the operator, and valves are actuated to terminate the dilution automatically.

Upon the actuation of a source range flux doubling signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated, thereby terminating the dilution. In addition, the makeup pumps are tripped for equipment protection only.

Deleted: 200

Deleted: 2402

Deleted: 955

Deleted: 1135

Deleted: The reactor coolant system dilution volume is considered well-mixed. The Technical Specifications require that when in Mode 5, at least one reactor coolant pump shall be operable, which provides sufficient flow through the system to maintain the system well mixed. If a reactor coolant pump is not operating, the demineralized water isolation valves are closed and an uncontrolled boron dilution transient cannot occur, as discussed in section 15.4.6.2.1.

Deleted: of 60 percent of

Deleted: detection

Deleted: of the

Deleted: Upon any reactor trip signal, source range flux multiplication signal, low input voltage to the Class 1E dc and uninterruptable power supply system battery chargers, or safety injection signal, a safety function automatically isolates the potentially unborated water from the demineralized water transfer and storage system and thereby terminates the dilution. The suction lines for the chemical and volume control system pumps are automatically realigned to draw borated (greater than 4000 ppm) water from the chemical and volume control system boric acid tank. The realignment of the chemical and volume control system valves to terminate the dilution is a safety-related function. The realignment of pump suction to the boric acid tank is a nonsafety-related operation. The chemical and volume control system pumps are nonsafety-related, so their operation is not credited in the analysis. The analysis does consider the initial portion of this boration phase by treating it as a continuing dilution until any unborated water in the chemical and volume control system lines is purged.

The automatic protective actions initiate about 11 minutes after the start of dilution. These automatic actions minimize the approach to criticality and maintain the plant in a subcritical condition. After the automatic protection functions take place, the operator may take action to restore the Technical Specification shutdown margin.

Deleted: 12.03

15.4.6.2.3 Dilution During Safe Shutdown (Mode 4)

The following conditions are assumed for an inadvertent boron dilution while in this mode:

- A dilution flow of 175 gpm of unborated water exists.
- Reactor coolant system water volume is 7539.8 ft^3. This is a conservative estimate of the minimum active volume of the reactor coolant system while on normal residual heat removal.
- All control rods are fully inserted, except the most reactive rod which is assumed stuck in the fully withdrawn position, and a conservative critical boron concentration of 1449 ppm.
- The shutdown margin is equal to 1.6-percent k/k, the minimum value required by the Technical Specifications for the hot shutdown mode. This gives a shutdown boron concentration of 1649 ppm.
- The reactor coolant system dilution volume is considered well-mixed. The Technical Specifications require that when in Mode 4, at least one reactor coolant pump shall be operable, which provides sufficient flow through the system to maintain the system well-mixed. If a reactor coolant pump is not operating, the demineralized water isolation valves are closed and an uncontrolled boron dilution transient cannot occur, as discussed in section 15.4.6.2.1.

Deleted: 200

Deleted: 2805

Deleted: 898

Deleted: 1083

In the event of an inadvertent boron dilution transient during safe shutdown, the source range nuclear instrumentation detects a sufficiently large increase in the neutron flux, automatically initiates valve movement to terminate the dilution, and sounds an alarm.

Deleted: an

Deleted: of 60 percent of

Upon the actuation of a source range flux doubling signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated, thereby terminating the dilution. In addition, the makeup pumps are tripped for equipment protection only. The protective actions initiate about 32 minutes after the start of the dilution. No operator action is required to terminate this transient.

Deleted: ¶
As in Mode 5, the safety analysis considers the potential penalty of the subsequent nonsafety-related boration function by accounting for the purge volume associated with the chemical and volume control system piping.

Deleted: 12.3

15.4.6.2.4 Dilution During Hot Standby (Mode 3)

The following conditions are assumed for an inadvertent boron dilution while in this mode:

- A dilution flow of 175 gpm of unborated water exists.
- The reactor coolant system volume is 7539.8 ft^3. This is a conservative estimate of the minimum active volume of the reactor coolant system with the reactor coolant system filled and vented and one reactor coolant pump running.
- Critical boron concentration is 1281 ppm. This is a conservative boron concentration assuming control rods are fully inserted minus the most reactive rod, which is assumed stuck in the fully withdrawn position.
- The shutdown margin is equal to 1.6-percent k/k, the minimum value required by the Technical Specifications for the hot standby mode. This gives a shutdown boron concentration of 1509 ppm.
- The reactor coolant system dilution volume is considered well-mixed. The Technical Specifications require that when in Mode 3, at least one reactor coolant pump shall be operable, which provides sufficient flow through the system to maintain the system well mixed. If a reactor coolant pump is not operating, the demineralized water isolation valves are closed and an uncontrolled boron dilution transient cannot occur, as discussed in section 15.4.6.2.1.

In the event of an inadvertent boron dilution transient in hot standby, the source range nuclear instrumentation detects a sufficiently large increase in of the neutron flux, automatically initiates valve movement to terminate the dilution, and sounds an alarm.
Upon the actuation of a source range flux doubling signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated, thereby terminating the dilution. In addition, the makeup pumps are tripped for equipment protection only.

Protective actions initiate about 32 minutes after start of dilution. No operator action is required to terminate this transient.

Deleted: 200

Deleted: 7300

Deleted: 655

Deleted: 867

Deleted: an

Deleted: of 60 percent

Deleted: As in the analyses for Modes 4 and 5, the only consideration of the boration function in safety analysis is to account for the additional dilution effect due to the purge volume associated with the chemical and volume control system piping.

Deleted: 56.3

15.4.6.2.5 Dilution During Startup (Mode 2)

The plant is in the startup mode only for startup testing at the beginning of each cycle. During this mode of operation, rod control is in manual. Normal actions taken to change power level, either up or down, require operator actuation. The Technical Specifications require an available shutdown margin of 1.6-percent $\Delta k/k$ and four reactor coolant pumps operating. Other conditions assumed are the following:

- There is a dilution flow of 200 gpm of unborated water.
- Minimum reactor coolant system water volume is 8126 ft^3. This is a very conservative estimate of the active reactor coolant system volume, minus the pressurizer volume.
- An initial maximum critical boron concentration, corresponding to the rods inserted to the insertion limits, is 1327 ppm. The minimum change in boron concentration from this initial condition to a hot zero power critical condition with all rods inserted is 1088 ppm. Full rod insertion, minus the most reactive stuck rod, occurs because of reactor trip.

This mode of operation is a transitory operational mode in which the operator intentionally dilutes and withdraws control rods to take the plant critical. During this mode, the plant is in manual control. For a normal approach to criticality, the operator manually withdraws control rods and dilutes the reactor coolant with unborated water at controlled rates until criticality is achieved. Once critical, the power escalation is slow enough to allow the operator to manually block the source range reactor trip after receiving the P-6 permissive signal from the intermediate range detectors (nominally at 10^5 cps). Too fast a power escalation (due to an unknown dilution) would result in reaching P-6 unexpectedly, leaving insufficient time to manually block the source range reactor trip. Failure to perform this manual action results in a reactor trip and immediate shutdown of the reactor.

Deleted: initiates a limited dilution and then manually withdraws the control rods, a process that takes several hours. The Technical Specifications require that the operator determine the estimated critical position of the control rods prior to approaching criticality and thus provide confidence that the reactor does not go critical with the control rods below the insertion limits.

Upon the actuation of a source range flux doubling signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated, thereby terminating the dilution. In addition, the makeup pumps are tripped for equipment protection only. During an intentional approach to criticality, the operator can manually block the source range flux doubling function. During this period, special attention is given to reactivity control by the plant operators. Also, the source range and intermediate range reactor trips are available to trip the control rods that are withdrawn by such a point in the startup of the reactor.

Upon any reactor trip signal or low input voltage to the Class 1E dc and uninterruptable power supply system battery chargers, a safety-related function automatically isolates the potentially unborated water from the demineralized water transfer and storage system and thereby terminates the dilution. Additionally, the suction lines for the chemical and volume control system pumps are automatically realigned to draw borated water from the chemical and volume control system boric acid tank.

Deleted: , source range flux multiplication signal,

Deleted: or a safety injection signal,

After reactor trip, the dilution would have to continue for approximately 383 minutes to overcome the available shutdown margin. Even assuming that the nonsafety-related boration operation does not occur, the unborated water that may remain in the purge volume of the chemical and volume control system is not sufficient to return the reactor to criticality. Therefore, the automatic termination of the dilution flow from the demineralized water transfer and storage system prevents a post-trip return to criticality.

Deleted: Because the realignment of the suction for the chemical and volume control system pumps to the boric acid tank is a nonsafety-related operation, the only consideration given to the reboration phase of the event in the safety analysis is the unborated chemical and volume control system purge volume. Events are shown in Table 15.4-1.

3.1.9 Chemical and Volume Control System (CVS) Demineralized Water Isolation Valves and Makeup Line Isolation Valves

LCO 3.1.9 Two CVS Demineralized Water Isolation Valves shall be OPERABLE.

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

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One CVS demineralized water isolation valve or one makeup line isolation valve inoperable.	A.1	Restore two CVS demineralized water isolation valves and two makeup line isolation valves to OPERABLE status.	72 hours
B. Required Action and associated Completion Time of Condition not met. OR Two CVS demineralized water isolation valves or two makeup line isolation valves inoperable.	B.1	------------------------------------ - NOTE - Flow path(s) may be unisolated intermittently under administrative controls. ------------------------------------ Isolate the flow path from the demineralized water storage tank to the Reactor Coolant System by use of at least one closed manual or one closed and de-activated automatic valve.	1 hour

Deleted: B.1

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.1.9.1	Verify two CVS demineralized water isolation valves and two makeup line isolation valves are OPERABLE by stroking the valve closed.	In accordance with the Inservice Testing Program

B 3.1.9 Chemical and Volume Control System (CVS) Demineralized Water Isolation Valves

BASES

BACKGROUND

One of the principle functions of the CVS system is to maintain the reactor coolant chemistry conditions by controlling the concentration of boron in the coolant for plant startups, normal dilution to compensate for fuel depletion, and shutdown boration. In the dilute mode of operation, unborated demineralized water may be supplied directly to the reactor coolant system.

Although the CVS is not considered a safety related system, certain functions of the system are considered safety related functions. The appropriate components have been classified and designed as safety related. The safety related functions provided by the CVS include containment isolation of chemical and volume control system lines penetrating containment, termination of inadvertent boron dilution, and preservation of the Reactor Coolant System (RCS) pressure boundary, including isolation of CVS letdown from the RCS.

APPLICABLE SAFETY ANALYSES	One of the initial assumptions in the analysis of an inadvertent boron dilution event (Ref. 1) is the assumption that the increase in core reactivity, created by the dilution event, can be detected by the source range instrumentation. The source range instrumentation will then supply a signal to the demineralized water isolation valves and the makeup line isolation valves in the CVS causing these valves to close and terminate the boron dilution event. Thus the makeup line isolation valves and the demineralized water isolation valves are components which function to mitigate or prevent an AOO. CVS isolation valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The requirement that at least two demineralized water isolation valves and two makeup line isolation valves be OPERABLE assures that there will be redundant means available to terminate or prevent an inadvertent boron dilution event.
APPLICABILITY	The requirement that at least two demineralized water isolation valves and two makeup line isolation valves be OPERABLE is applicable in MODES 1, 2, 3, 4, and 5 because a boron dilution event is considered possible in these MODES, and the automatic closure of these valves is assumed in the safety analysis.

Deleted: 00

BASES

APPLICABILITY (continued)

In MODES 1 and 2, the detection and mitigation of a boron dilution event does not assume the detection of the event by the source range instrumentation. In these MODES, the event would be signalled by an intermediate range trip, a trip on the Power Range Neutron Flux - High (low setpoint nominally at 25% RTP), or Overtemperature delta T. The two demineralized water isolation valves close automatically upon reactor trip.

In MODE 6, a dilution event is precluded by the requirement in LCO 3.9.2 to close, lock and secure at least one valve in each unborated water source flow path.

ACTIONS

A.1

If only one demineralized water isolation valve or makeup line isolation valve is OPERABLE, the second valve must be restored to OPERABLE status in 72 hours. The allowed Completion Time assures expeditious action will be taken, and is acceptable because the safety function of automatically isolating the clean water source can be accomplished by the redundant demineralized water isolation valve.

B.1

If the Required Actions and associated Completion Time of Condition A are not met, or if both CVS demineralized water isolation valves or both makeup line isolation valves are not OPERABLE (i.e., not able to be closed automatically), then the demineralized water supply flow path to the RCS must be isolated. Isolation can be accomplished by manually isolating the CVS demineralized water isolation valve(s) or by positioning the 3-way blend valve to only take suction from the boric acid tank. Alternatively, the dilution path may be isolated by closing appropriate isolation valve(s) in the flow path(s) from the demineralized water storage tank to the reactor coolant system.

The Action is modified by a Note allowing the flow path to be unisolated intermittently under administrative controls. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the main control room. In this way, the flow path can be rapidly isolated when a need for isolation is indicated.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.9.1

Verification that the CVS demineralized water isolation valves and makeup line isolation valves are OPERABLE, by stroking each valve closed, demonstrates that the valves can perform their safety related function. The Frequency is in accordance with the Inservice Testing Program.

REFERENCES

1. Chapter 15, "Accident Analysis."

TABLE 3.3.2-1 (PAGE 9 OF 13)
ENGINEERED SAFEGUARDS ACTUATION SYSTEM INSTRUMENTATION

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
15. Boron Dilution Block						
a. Source Range Neutron Flux Doubling	2(f),3(f),4(m)	4	B,T	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		≤ Source Range Flux X 2.2 in 50 minutes
	5(m)	4	B,P	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		≤ Source Range Flux X 2.2 in 50 minutes
b. Reactor Trip	Refer to Function 18.a (ESFAS Interlocks, Reactor Trip, P-4) for all requirements.					
c. Battery Charger Input Voltage – Low	1,2,3,4(m)	4 divisions	B,T	SR 3.3.2.3 SR 3.3.2.4		≥ [343] V*
	5(m)	4 divisions	B,P	SR 3.3.2.3 SR 3.3.2.4		≥ [343] V*

Deleted: Multiplication

Deleted: 1.6

Deleted: 1.6

(f) Not applicable when critical or during intentional approach to criticality.

Deleted: Below the P-6 (Intermediate Range Neutron Flux) interlocks.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(m) Not applicable for valve isolation Functions whose associated flow path is isolated.

(p) Above the P-19 (RCS Pressure) interlock.

BASES
APPLICABLE SAFETY ANALYSES, LCOs and APPLICABILITY (continued)

15. Boron Dilution Block

The block of boron dilution is accomplished by closing the CVS suction valves to demineralized water storage tanks, and aligning the boric acid tank to the CVS makeup pumps. This Function is actuated by Source Range Neutron Flux Multiplication, Reactor Trip, and Battery Charger Input Voltage – Low.

15.a. Source Range Neutron Flux Multiplication

A signal to block boron dilution in MODES 2 or 3, when not critical or during an intentional approach to criticality, and MODES 4, or 5 is derived from source range neutron flow increasing at an excessive rate (source range flux doubling). This Function is not applicable in MODES 4 and 5 if the demineralized water makeup flowpath is isolated. The source range neutron detectors are used for this Function. The LCO requires four divisions to be OPERABLE. There are four divisions and two-out-of-four logic is used. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, demineralized water is isolated from the makeup pumps and reactor coolant makeup is isolated from the reactor coolant system to preclude a boron dilution event. In MODE 6, a dilution event is precluded by the requirement in LCO 3.9.2 to close, lock and secure at least one valve in each unborated water source flow path

Deleted: below the P-6 interlock

Deleted: 3,

Deleted: flow multiplication

Deleted: flow

Deleted: makeup

15.c. Battery Charger Input Voltage – Low

Demineralized water is isolated and the Makeup Pumps are aligned to the BAT by the loss of ac power. A short, preset time delay is provide to prevent actuation upon momentary power fluctuations; however, actuation occurs before ac power is restored by the onsite diesel generators. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. The loss of ac power signal is based on the detection of an

Deleted: Block of boron dilution is also actuated from undervoltage condition by each of the two sensors connected to two of the four battery chargers. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, and 5. This Function is not applicable in MODES 4 and 5 if the associated flowpath is closed. In MODE 6, a dilution event is precluded by the requirement in LCO 3.9.2 to close, lock and secure at least one valve in each unborated water source flow path.

Deleted: s

18.c. Intermediate Range Neutron Flux, P-6

The Intermediate Range Neutron Flux, P-6 interlock is actuated when the respective NIS intermediate range channel goes approximately one decade above the minimum channel reading. Below the setpoint, the P-6 interlock automatically unblocks the flux doubling function, permitting the block of born dilution. Normally, this Function is blocked by the main control room operator during reactor startup. This Function is required to be OPERABLE in MODE 2.

Deleted: Above the setpoint, the P-6 interlock allows a manual block of the flux multiplication actuation, permitting block of boron dilution.

II.10 MANUAL ISOLATION OF INDIVIDUAL STEAMLINES

Manual isolation of individual steamlines has been removed from the protection system functions. The function has been changed to be a true system-level actuation function consistent with traditional Westinghouse practice and the requirements of IEEE-603. The operation of either manual control will cause the isolation of both steam lines. This change to the design is consistent with the accident analysis as discussed in DCD Chapter 15.Manual isolation of both steamlines, therefore, continues to be available from the protection system and manual control of individual steamline isolation valves is available through the plant control system. See Figure 7.2-1, Sheet 9.

Revise Section 7.3.1.2.10 as shown:

7.3.1.2.10 Steam Line Isolation

A signal to isolate the steam line is generated from any one of the following conditions:

1. Manual initiation
2. High-2 containment pressure
3. Low lead-lag compensated steam line pressure
4. High steam line pressure negative rate
5. Low reactor coolant inlet temperature

The steam line isolation signal closes the main steam line isolation valves and the stop and bypass valves. In addition to manual system-level steam line isolation, steam line isolation valves can be closed individually via the non-safety plant control system.

Condition 1 consists of two momentary controls. Manual actuation of either of the two controls initiates steam line isolation for both steam generators.

Deleted: In addition, separate controls are provided for steam line isolation of each individual steam generator.

II.11 AUXILIARY SPRAY ISOLATION FUNCTION

The existing design combined the isolation of the pressurizer auxiliary spray line and the purification line. Though it is not a safety function, the auxiliary spray is the preferred method to depressurize the reactor coolant system for some plant cooldown scenarios and for a postulated steam generator tube rupture. A separate manual block of the Auxiliary Spray Isolation function is being added in order to allow the pressurizer auxiliary spray to be available to rapidly depressurize the reactor coolant system for such events. This change requires additions to Section 7.3.1.2.18 and Table 7.3-3 along with the modification of Figure 7.2-1, Sheet 12, as shown below.

7.3.1.2.18 Auxiliary Spray and Letdown Purification Line Isolation

A signal to isolate the auxiliary spray and letdown purification lines is generated upon the coincidence of pressurizer level below the Low-1 setpoint in any two of four divisions. This helps to maintain reactor coolant system inventory. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint. The auxiliary spray isolation function can be manually blocked anytime to allow the operators to use the auxiliary spray to rapidly depressurize the reactor coolant system. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 12.

Table 7.3-3 (Sheet 1 of 2)

SYSTEM-LEVEL MANUAL INPUT TO THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Manual Control	To Divisions				Figure 7.2-1 Sheet
Pressurizer pressure safeguards block control #4				D	11
Auxiliary Spray Isolation block control			C		12
Manual core makeup tank injection actuation #1	A	B	C	D	12

II.12 REMOVAL OF LOW-2 RCS HOT LEG SIGNAL FROM IRWST INJECTION LOGIC.

Low-2 RCS Hot Leg Level,as shown on Figure 7.2-1, Sheet 16 is an input to the 4th Stage ADS Actuation performed on Sheet 15. This same signal along with the 4th stage ADS Actuation signal are input to the logic on Sheet 16 that opens the IRWST injection valves. The separate Low-2 level signal input is, therefore, redundant to the 4th Stage ADS Actuation input to open the IRWST injection vales. It serves no additional purpose and has been removed from the design.

This change requires the removal of the Low-2 RCS Hot Leg Level signal going to the OR gate above the "OPEN IRWRST INJECTION VALVES" Box on Figure 7.2-1, Sheet 16, removal of the text "OR A LOW HL LEVEL SIGNAL" from Note 20 on Figure 6.3-2, modifying Table 7.3-2 (Sheet 3 of 4), and Section B 3.3.2.

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

18.d. Pressurizer Level, P-12

The P-12 interlock is provided to permit mid-loop operation without core makeup tank actuation, reactor coolant pump trip or purification line isolation. With pressurizer level channels less than the P-12 setpoint, the

Deleted: IRWST actuation

operator can manually block low pressurizer level signal used for these actuations. Concurrent with blocking CMT actuation on low pressurizer level, ADS 4th Stage actuation on Low 2 RCS hot leg level is enabled. When the pressurizer level is above the P-12 setpoint, the pressurizer level signal is automatically enabled and a confirmatory open signal is issued to the isolation valves on the CMT cold leg balance lines. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

Deleted: IRWST

II.13 CREATION OF NEW PERMISSIVE P-3 FOR SAFEGUARDS ACTUATION BLOCK

The current design allows the Safeguards Actuation Block when P-4 is true. P-4 is true when either a Reactor Trip command is active or the Reactor Trip Breaker is open. While P-4 is sufficient to allow the block of the Safeguards Function, it does not guarantee that the Reactor Breakers are open and by extension that the rods have dropped. By creating a separate permissive (i.e., P-3) that is only true when the Reactor Breakers are open, there is one less assumption about the assurance that negative reactivity has been added to the core. This would allow a higher confidence that adequate shutdown margin exists when the operator blocks/resets the Safeguards Signal.

Changes to Table 7.3-1 are necessary to accurately reflect the logic in the PMS. The P-3 permissive is interlocked with the Manual Block of the Automatic Safeguards actuations. This block needs to be included in the table in the Permissives and Interlocks column for the automatic signals. The portion of the safeguards block that is interlocked with P-3 does not affect the manual safeguards initiation; therefore, the Permissives and Interlocks column should read "None".

This change requires modifications to Figure 7.2-1, Sheets 2 and 11, text changes to Section 7.3.1.1, modifications of Table 7.3-1 (Sheet 1 of 8), Table 7.3-2 (Sheet 1 of 4), Technical Specifications Table 3.3.2-1 and Section B 3.3.2.

7.3.1.1 Safeguards Actuation (S) Signal

To permit startup and cooldown, the safeguards actuation signals generated from low pressurizer pressure, low steam line pressure, or low reactor coolant inlet temperature can be manually blocked when pressurizer pressure is below the P-11 setpoint. The signal is automatically unblocked when the pressurizer pressure is above the P-11 setpoint.

Separate momentary controls are provided, each of which will manually reset the safeguards actuation signal in a single division. Manual reset of a safeguards actuation signal in coincidence with reactor trip breaker open (P-3) blocks the safeguards actuation signal. Absence of P-3 automatically resets the blocking function. The safeguards actuation signal is manually reset based on a preset delay following initiation. Resetting the signal does not reposition any safeguards actuated equipment, since individual components are required to latch in and seal on the safeguards actuation signal.

Deleted: 4

Deleted: 4

Table 7.3-1 (Sheet 1 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
1. Safeguards Actuation Signal (Figure 7.2-1, Sheets 9 and 11)			
a. Low pressurizer pressure	4	2/4-BYP[1]	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
b. Low lead-lag compensated steam line pressure	4/steam line	2/4-BYP[1] in either steam line	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
c. Low reactor coolant inlet temperature (Low T_{cold})	4/loop	2/4-BYP[1] either loop[6]	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
d. High-2 containment pressure	4	2/4-BYP[1]	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
e. Manual safeguards initiation	2 switches	1/2 switches	None

Deleted: None¶

Deleted: Can be manually reset to block safeguards actuation upon P-4 . Block automatically removed on absence of P-4

Table 7.3-2 (Sheet 1 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Derivation	Function
P-3	Reactor trip breaker open	Permits manual reset of safeguards actuation signal to block automatic safeguards actuation
$\overline{\text{P-3}}$	Reactor trip breaker closed	Automatically resets the manual block of automatic safeguards actuation
P-4	Reactor trip initiated or reactor breakers open	(a) Isolates main feedwater if coincident with low reactor coolant temperature (b) Trips turbine (c) Blocks boron dilution
$\overline{\text{P-4}}$	No Reactor trip initiated and reactor breakers closed	Removes demand for isolation of main feedwater, turbine trip and boron dilution block

Deleted: (a)

Deleted: Permits manual reset of safeguards actuation signal to block automatic safeguards actuation

Deleted: switchgear open (reactor trip)

Deleted: b

Deleted: c

Deleted: d

Deleted: switchgear closed

Deleted: Automatically resets the manual block of automatic safeguards actuation

TABLE 3.3.2-1 (PAGE 10 OF 13)
ENGINEERED SAFEGUARDS ACTUATION SYSTEM INSTRUMENTATION

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
18. ESFAS Interlocks						
a. Reactor Trip, P-4	1,2,3	3 divisions	D,M	SR 3.3.2.3	N/A	N/A
b. Pressurizer Pressure, P-11	1,2,3	4	J,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		≤ [1970] sig
c. Intermediate Range Neutron Flux, P-6	2	4	J,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		≥ [1E-10] amps
d. Pressurizer Level, P-12	1,2,3,4,5,6	4	J,M BB,Y	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		Above Pressurizer Water Level – Low 1 setpoint of [20]%
e. RCS Pressure, P-19	1,2,3,4[(i)]	4	J,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6		≥ [700] psig
f. Reactor Trip Breaker Open, P-3	1,2,3	3 divisions	D,M	SR 3.3.2.3	N/A	N/A

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of every 92 days on a STAGGERED TEST BASIS provides a complete test of all four divisions once per year. This frequency is adequate based on the inherent high reliability of the solid state devices which comprise this equipment; the additional reliability provided by the redundant subsystems; and the use of continuous diagnostic test features, such as deadman timers, memory checks, numeric coprocessor checks, cross-check of redundant subsystems, and tests of timers, counters, and crystal time basis, which will report a failure within these cabinets to the operator.

SR 3.3.2.3

SR 3.3.2.3 is the performance of a TADOT of the manual actuations, initiations, and blocks for various ESF Functions, the Class 1E battery charger undervoltage inputs, the reactor trip breaker open (P-3) input and the reactor trip (P-4) input from the IPCs. This TADOT is performed every 24 months.

II.14 Addition of delay timers for enabling the Source Range Reactor Trip and Flux Doubling Signal

Because of the very low level signal that the source range neutron detectors measure, they and their interfacing electronics typically experience a several second period of instability whenever the detectors are energized. The addition of Source Range Reactor Trip and Flux Doubling Signal delay timers is to prevent spurious actuations during this period of time.

This change requires modifications to Figure 7.2-1, Sheet 3, text changes to Sections 7.2.1.1.1, 7.3.1.2.14, and Technical Specifications Section B 3.3.1.

7.2.1.1.1 Nuclear Startup Trips

Source Range High Neutron Flux Trip

Source range high neutron flux trips the reactor when two of the four source range channels exceed the trip setpoint. This trip provides protection during reactor startup and plant shutdown. This function is delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious trip due to the short term instability of the processed source range values. It may be manually blocked and the high voltage source range detector power supply de-energized when the intermediate range neutron flux is above the P-6 setpoint value. It is automatically blocked by the power range neutron flux interlock (P-10). The trip may be manually reset when neutron flux is between P-6 and P-10. The reset occurs automatically when the intermediate range flux decreases below P-6. The channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

7.3.1.2.14 Boron Dilution Block

Condition 1 is an average of the source range count rate, sampled at least N times over the most recent time period T1, compared to a similar average taken at time period T2 earlier. If the ratio of the current average count rate to the earlier average count rate is greater than a preset value, a partial trip is generated in the division. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, boron dilution is blocked. The Flux Doubling function is also delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious dilution block due to the short term instability of the processed source range values. This source range flux doubling signal may be manually blocked to permit plant startup and normal power operation. It is automatically reinstated when reactor power is decreased below the P-6 power level during shutdown.

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

5. Source Range Neutron Flux

The LCO requirement for the Source Range Neutron Flux trip Function ensures that protection is provided against an uncontrolled bank rod withdrawal accident from a subcritical condition during startup. This trip Function provides redundant protection to the Power Range Neutron Flux – Low Setpoint and Intermediate Range Neutron Flux trip Functions. In MODES 3, 4, and 5, administrative controls also prevent the uncontrolled withdrawal of rods. The PMS source range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The safety analyses do not take credit for the Source Range Neutron Flux trip Function. Even though the safety analyses take no credit for the Source Range Neutron Flux trip, the functional capability at the specified Trip Setpoint is assumed to be available and the trip is implicitly assumed in the safety analyses.

The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any events that result in a harsh environment. This trip can be manually blocked by the main control room operator when above the P-6 setpoint (Intermediate Range Neutron Flux interlock) and is automatically unblocked when below the P-6 setpoint. The manual block of the trip function also de-energizes the source range detectors. The source range detectors are automatically re-energized when below the P-6 setpoint. The trip is automatically blocked when above the P-10 setpoint (Power Range Neutron Flux interlock). The Flux Doubling function is also delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious dilution block due to the short term instability of the processed source range values. The source range trip is the only RTS automatic protective Function required in MODES 3, 4, and 5. Therefore, the functional capability at the specified Trip Setpoint is assumed to be available.

II.15 RT/ESF ACCURACIES AND RESPONSE TIMES CORRECTIONS

Tables 7.2-1 and 7.3-4 provide typical measurement accuracies and response times for the reactor trip and engineered safety features actuation functions. These tables do not serve as the regulatory basis for these parameters. The accident analyses as summarized in DCD Chapter 15 and the setpoint study serve this purpose. Tables 7.2-1 and 7.3-4 provide typical values to provide a basic understanding of system operation. Earlier versions of the DCD contained values typical for earlier generation plant designs and I&C equipment. More representative values for these parameters have become available as the AP1000 plant design has progressed and the tables have been revied to reflect the later information.

This change requires modifications to Section 7.3.1.5.2, Table 7.2-1 and Table 7.3-4.

7.3.1.5.2 Design Basis: Variables, Ranges, Accuracies, and Typical Response Times Used in Engineered Safety Features Actuation (Paragraphs 4.1, 4.2, and 4.4 of IEEE 603-1991)

Ranges, typical accuracies, and typical response times for the variables used in engineered safety features actuation are listed in Table 7.3-4. The time response is the maximum allowable time period for an actuation signal to reach the necessary components. It is based on following a step change in the applicable process parameter from 5 percent below to 5 percent above (or vice versa) the actuation setpoint with externally adjustable time delays set to OFF.

Deleted: Typical r

Table 7.2-1 (Sheet 1 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES (DESIGN BASIS FOR REACTOR TRIP) (NOMINAL)

Protective Functions	Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Source Range High Neutron Flux	Neutron flux	6 decades of neutron flux: 1 to 10^6 counts per second	±10% of span	0.6
Intermediate Range High Neutron Flux	Neutron flux	8 decades of neutron flux overlapping source range by 2 decades and including 100% power	±10% of span	0.6
Power Range High Neutron Flux (Low Setting)	Neutron flux	1 to 120% of full power	±5% of span	0.6
Power Range High Neutron Flux (Hi-Setting)	Neutron flux	1 to 120% of full power	±5% of span	0.6
Power Range High Positive Flux Rate	Neutron flux	1 to 120% of full power	±1% of span	0.6 (step input of 20% full power)
Overtemperature ΔT			±5% of ΔT span	
	Reactor coolant inlet temp. (T_{cold})	490° to 610°F		5.5
	Reactor coolant outlet temp. (T_{hot})	530° to 650°F		5.5
	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)		0.6

Deleted: s To Be Monitored
Deleted: '
Deleted: 11.0
Deleted: 2
Deleted: 12.5
Deleted: 2
Deleted: 7.0
Deleted: 2
Deleted: 7.0
Deleted: 2
Deleted: .0
Deleted: 2
Deleted: 11.5
Deleted: 7.0 (T_{avg} or ΔT)
Deleted: ±2.5% of span
Deleted: 6.0
Deleted: ±3.5% of span
Deleted: 6.0
Deleted: 2.5
Deleted: 1.5
Deleted: 2.0

Table 7.2-1 (Sheet 2 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES
(DESIGN BASIS FOR REACTOR TRIP)
(NOMINAL)

Protective Functions	Variable	Range of Variables	Typical Accuracy[(1)]	Typical Response Time (Sec)[(2)]
Overpower ΔT			±4% of ΔT span	
	Reactor coolant inlet temp. (T_{cold})	490° to 610°F		5.5
	Reactor coolant outlet temp. (T_{hot})	530° to 650°F		5.5
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% ($\Delta\varphi$)		0.6
Pressurizer Low Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Water Level	Pressurizer water level	0-100% of entire cylindrical portion of pressurizer	±5% of span	0.9
Low Reactor Coolant Flow	Coolant flow	0 to 120% of rated flow	±3% of span	0.9
Low Reactor Coolant Pump Speed	Pump speed	0 to 120% of rated speed	±1% of span	0.7
Low Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±22% of span	0.9
High Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±13% of span	0.9
Reactor Coolant Pump High Bearing Water Temperature	Reactor coolant pump bearing water temperature	70°-450°F	±2% of span	5.5

Deleted: s To Be Monitored
Deleted: [1]
Deleted: 3.5
Deleted: 7.0 (T_{avg} or ΔT)
Deleted: ±2.5% of span
Deleted: 6.0
Deleted: ±3.5% of span
Deleted: 6.0
Deleted: ±7.0% of span
Deleted: 2.0
Deleted: 2.5
Deleted: 1.2
Deleted: 2.5
Deleted: 1.2
Deleted: 2.25
Deleted: 1.6
Deleted: 3.0
Deleted: 1.6
Deleted: 0.2
Deleted: 42
Deleted: [(2)]
Deleted: 2.0
Deleted: 1.6
Deleted: 2.0
Deleted: 1.6
Deleted: 1.0
Deleted: 2.0

Table 7.2-1 (Sheet 3 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES
(DESIGN BASIS FOR REACTOR TRIP)
(NOMINAL)

Protective Functions	Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Automatic or Manual Safeguards Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Manual Reactor Trip	Switch position	N/A	N/A	N/A
Automatic or Manual Depressurization System Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Automatic or Manual Core Makeup Tank Injection	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4

Notes:
1. Measurement uncertainty typical of actual applications. Harsh environment allowances have been included where applicable.
2. Delay from the time that the process variable exceeds the setpoint until the time that the control rods are free to fall into the core (includes reactor trip breaker opening delay and control rod drive mechanism gripper release delay).

Deleted: s To Be Monitored

Deleted: 1

Deleted: Reference Leg Temperature Compensation(3) ... [25]

Deleted: Time from step change of the variable being monitored from 5% below to 5% above the setpoint. Value defined until the signal reaches the reactor trip breakers.

Deleted: The time delay is the time to generate a trip after the pump speed has reached the trip setpoint during a speed decrease which is linear with respect to time.

Deleted: 3. This temperature compensation is not a protective function per se; however, these signals provide density compensation used in the pressurizer high water level protective function.

Table 7.3-4 (Sheet 1 of 2)

ENGINEERED SAFETY FEATURES ACTUATION, VARIABLES, LIMITS, RANGES, AND ACCURACIES (NOMINAL)

Variable	Range of Variable	Typical Accuracy[(1)]	Typical Response Time (Sec)[(2)]
Pressurizer pressure	1700 to 2500 psig	±14% of span	1.0
Steam line pressure	500 to 1300 psig	±3% of span (Normal environment) ±10% of span (Adverse environment)	1.0
Steam line negative pressure rate	0 to 250 psig/sec	±0.2% of span	1.0
Reactor coolant inlet temperature (T_{cold})	490 to 610°F	±3% of span	5.5
Reactor coolant outlet temperature (T_{hot})	530 to 650°F	±2% of span	5.5
Containment pressure	-5 to 10 psig	±3% of span	1.0
Reactor coolant system hot leg level	0 to 100% of span	±5% of span	1.0
In-containment refueling water storage tank level	0 to 100% of span	±6% of span	1.0
Undervoltage on ac buses	0 to 500 V	±2% of setpoint	1.5
Steam generator narrow range water level	0 to 100% of span (narrow range taps)	±22% of span	1.0
Steam generator wide range water level	0 to 100% of span (wide range taps)	±32% of span	1.0
Core makeup tank narrow range upper water level	0 to 100% of span	±40% of span	1.0
Core makeup tank narrow range lower water level	0 to 100% of span	±40% of span	1.0
Reactor coolant pump bearing temperature	70 to 450°F	±2% of span	5.5
Spent fuel pool level	0 to 26 feet	±3% of span	1.0
Reactor coolant system wide range pressure	0 to 3300 psig	±3% of span	1.0

Deleted: ACCURACY'S
Deleted: to be Monitored
Deleted: (1)
Deleted: 1200
Deleted: 1.2
Deleted: (1)
Deleted: 3.0
Deleted: (2)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: 250 …400 …6.5 [... [26]
Deleted: (1)
Deleted: 1.6
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)
Deleted: (1)

Table 7.3-4 (Sheet 2 of 2)

ENGINEERED SAFETY FEATURES ACTUATION, VARIABLES, LIMITS, RANGES, AND ACCURACIES (NOMINAL)

Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Pressurizer water level	0 to 100% of cylindrical portion of pressurizer	± 10% of span	1.0
Startup feedwater flow	0 to 1000 gpm	±7% of span	1.0
Neutron flux (flux doubling calculation)	1 to 10^6 c/sec	± 30% of span	1.0(3)
Control room supply air radiation level	10^{-7} to 10^{-2} μ Ci/cc	± 50% of setpoint	20
Containment radioactivity	10^0 to 10^7 R/hr	± 50% of setpoint	20

Notes:

1. Measurement uncertainty typical of actual applications. Harsh environment allowances have been included where applicable.
2. Delay from the time that the process variable exceeds the setpoint until the time that an output is provided to the actuated device.
3. Response time depends on flux doubling calculation.

Deleted: s to be Monitored
Deleted: 2.25
Deleted: 1.2
Deleted: (1)
Deleted: 4.0
Deleted: 1.6
Deleted: (1)
Deleted: 11.0
Deleted: 10.0
Deleted: (1)
Deleted: 5.0
Deleted: full scale
Deleted: 5.0(1)
Deleted: 5.0
Deleted: full scale
Deleted: 5.0(1)
Deleted: Listed response time is the time for a step change of a variable, from 5% below to 5% above the setpoint, to reach the actuated device.¶
Deleted: Listed response time is the time for a negative 20% step change of steam line pressure to reach the actuated device.¶
Deleted: time constant settings

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.16 CORRECT CHAPTER 7 TECHNICAL SPECIFICATION REFERENCE

Section 7.3.1 currently refers to the "July 1993 Final Policy Statement on Technical Specification Improvements". This policy statement has been superseded by changes to the Code of Federal regulations at 10 CFR 50.36(c)(2)(ii). Section 7.3.1 has been revised accordingly.

This change requires modifications to Note 8 in Table 7.3-1 and text in the last paragraph of Section 7.3.1, as shown below.

Table 7.3-1 – Affected Note

8. This function does not meet the 10 CFR 50.36(c)(2)(ii) criteria and is not included in the Technical Specifications.

Deleted: July 1993 Final Policy Statement on Technical Specification Improvements

Section 7.3.1 (Last Paragraph) Excerpt

Table 7.3-1 summarizes the signals and initiating logic for each of the engineered safety features initiated by the protection and safety monitoring system. Most of the functions provide protection against design basis events which are analyzed in Chapter 15. However, not all the functions listed in Table 7.3-1 are necessary to meet the assumptions used in performing the safety analysis. For example, the design provides features which provide automatic actuations which are not required for performing the safety analysis. In addition, some functions are provided to support assumptions used in the probabilistic risk assessment, but are not used to mitigate a design basis accident. Only those functions which meet the 10 CFR 50.36(c)(2)(ii) criteria are included in the AP1000 DCD, Section 16.1, Technical Specifications. This accounts for any difference between functions listed in Table 7.3-1 and functions which are included in the Technical Specifications.

Deleted: July 1993 NRC Final Policy Statement on Technical Specification Improvements

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.17 CORRECT CORE MAKEUP TANK ACTUATION SIGNALS

Section 7.3.1.2.3 lists 6 conditions that will cause Core Makeup Tank actuation. Condition 6 needs to be deleted because it is not one of the signals that generates a CMT actuation, but is instead a permissive for blocking Condition 3 from generating a CMT actuation. This change requires modifications to Section 7.1.1.2.3.

7.3.1.2.3 Core Makeup Tank Injection

Signals to align the core makeup tanks for injection are generated from the following conditions:

1. Automatic or manual safeguards actuation (subsection 7.3.1.1)
2. Automatic or manual actuation of the first stage of the automatic depressurization system (subsection 7.3.1.2.4)
3. Low-2 pressurizer level
4. Low wide range steam generator level coincident with High hot leg temperature
5. Manual initiation

Conditions 1 through 5 initiates a block of the pressurizer heaters; trip the reactor and reactor coolant pumps; initiate alignment of the core makeup tank isolation valves for passive injection to the reactor coolant system; and provide a confirmatory open signal to the cold leg balance line isolation valves. The balance line isolation valves are normally open but can be closed by the operator. The confirmatory open signal automatically overrides any bypass features that are provided to allow the cold leg balance line isolation valves to be closed for short periods of time. The motive force for core makeup tank injection is provided by density differences between the fluids in the cold leg balance line and the core makeup tank water.

Deleted: <#>Pressurizer water level increasing above the P-12 interlock¶

Deleted: Condition 6 initiates a confirmatory open signal to the cold leg balance line isolation valves.

II.18 TRIPPING OF PRESSURIZER HEATERS

The electrical immersion heaters used to control reactor coolant system pressure during normal plant operation are tripped whenever the Core Makeup Tanks (CMTs) are actuated. The main heater breakers are tripped directly by an isolated output from the Protection and Safety Monitoring System (PMS). In addition, an isolated signal is provided from the PMS to the Plant Control System to independently trip the breakers for the individual heater groups. The design was not clearly shown in the existing logic on Figure 7.2-1, Sheet 12. In addition, the existing text in Section 7.3.1.2.23 and Table 7.3-1 regarding the function to be performed is ambiguous and must clarified.

This change requires modifications to the text in Section 7.3.1.2.23, Item 25 of Table 7.3-1 and Figure7.2-1, Sheet 12.

7.3.1.2.23 Pressurizer Heater Trip

Deleted: Block

Signals for disabling the operation of the pressurizer heaters are generated from any of the following conditions:

Deleted: blocking

1. Core makeup tank injection alignment signal (subsection 7.3.1.2.3)
2. High-3 pressurizer water level

Division A of the protection and safety monitoring system provides actuation signals to five load center circuit breakers which provide the power feed to five pressurizer heater electrical control centers. When these five power feed breakers are opened, the electrical power is removed from the pressurizer heaters. In addition, Division C of the protection and safety monitoring system provides a separate signal to the plant control system. This separate signal is used to command the plant control system to open the molded-case circuit breakers which provide a power feed to each individual pressurizer heater. This arrangement provides for complete disabling of the pressurizer heaters, even if a single component failure occurs.

Deleted: all

Deleted: all

Deleted: blocking

Table 7.3-1 (Sheet 8 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
25. Pressurizer Heater Trip (Figure 7.2-1, Sheets 6 and 12)			
a. Core makeup tank injection	(See items 6a through 6e)		
b. High-3 pressurizer level	4	2/4 BYP[1]	Manual block permitted below P-19 Automatically unblocked above P-19

Deleted: Block

II.19 CORRECT DESCRIPTION FOR PERMISSIVE P-19

Permissive P-19, based on increasing reactor coolant system hot leg pressure, permits the manual block of the trip of the pressurizer heaters on high pressurizer water level as shown on Figure 7.2-1, Sheet 6. The description of P-19 provided in Table 7.3-2 has been revised to add this function.

This change requires modifications to the P-19 description in Table 7.3-2.

Table 7.3-2 (Sheet 4 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	**Derivation**	**Function**
P-19	Reactor coolant system pressure below setpoint	(a) Permits manual block of chemical and volume control system isolation on high pressurizer water level (b) Permits manual block of passive residual heat removal heat exchanger alignment on high pressurizer water level <u>(c) Permits manual block of the pressurizer heater trip on high pressurizer water level</u>
$\overline{\text{P-19}}$	Reactor coolant system pressure above setpoint	(a) Prevents manual block of chemical and volume control system isolation on high pressurizer water level (b) Prevents manual block of passive residual heat removal heat exchanger alignment on high pressurizer water level <u>(c) Prevents manual block of the pressurizer heater trip on high pressurizer water level</u>

II.20 MINOR TEFCHNICAL CHANGES TO TABLE 7.3-1

A review of Table 7.3-1 identified five minor technical changes that need to be made to clarify some of the entries:

1. For Item 19, Sheet 18 has added to the Figure 7.2-1 reference.

2. There are several components whose actuation could lead to a plant event requiring a prolonged outage for clean-up and repair. The manual actuation of these components requires the simultaneous operation of either of two pairs of associated controls. Note #3 has been clarified to reflect the actual design.

3. Item 23 b. has added the missing phrase "coincident with" consistent with the logic for opening the containment recirculation valves shown on Figure 7.2-1, Sheet 16.

4. The containment recirculation valves are among the components that require the operation of two associated controls as described in Item 3, above. Item 23 c. has added Note 3 to the "2/4 controls" reference in the "Actuation Logic" Column.

5. Since there is no Item 23 a., the existing Items 23b and c has been renumbered as a and b.

Abridged versions of Table 7.3-1 with these changes are shown below.

Table 7.3-1 (Sheet 7 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
19. Normal Residual Heat Removal System Isolation (Figure 7.2-1, Sheets 13 and 18)			

Table 7.3-1 – Affected Note

3. Two associated controls must be actuated simultaneously.

Table 7.3-1 (Sheet 8 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
23. Open All Containment Recirculation Valves (Figure 7.2-1, Sheet 16)			
a. Automatic reactor coolant system depressurization (fourth stage coincident with)		(See items 3d through 3f)	
Low IRWST level (Low-3 setpoint)	4	2/4 BYP[1]	None
b. Manual initiation	4 controls	2/4 controls[3]	None

Deleted: b

Deleted: c

II.21 CVS LETDOWN ISOLATION LOGIC MODIFICATIONS

CVS Letdown Isolation is actuated if either of two reactor coolant system hot leg level divisions go below the Low-1 setpoint. A malfunction of a single measurement could, therefore, cause the inadvertent isolation of CVS letdown during normal plant operation. The letdown isolation function is only required during shutdown conditions when the pressurizer might drain. A manual block function has been added to permit the letdown isolation function to be blocked whenever pressurizer water level is above the P-12 setpoint. The letdown isolation function is automatically unblocked whenever the pressurizer water level goes below the P-12 setpoint.

This change requires modifications to Tier 1 Table 2.5.2-6 and Tier 2 Section 7.3.1.2.22, DCD Table 7.3-1 (Sheet 8 of 8), DCD Table 7.3-2 (Sheet 3 of 4), DCD Table 7.3-3 (Sheet 2 of 2), Figure 7.2-1, Sheets 12 and 16, and Technical Specifications Bases Section B 3.3.2.

Tier 1 Changes

TABLE 2.5.2-6 PMS BLOCKS
Engineered Safety Features: Automatic Safeguards Containment Isolation Main Feedwater Isolation Reactor Coolant Pump Trip Core Makeup Tank Injection Turbine Trip Steam Line Isolation Startup Feedwater Isolation Block of Boron Dilution Chemical and Volume Control System Isolation Chemical and Volume Control System Letdown Isolation Steam Dump Block Auxiliary Spray and Letdown Purification Line Isolation Passive Residual Heat Removal Heat Exchanger Alignment Normal Residual Heat Removal System Isolation

Tier 2 Changes

7.3.1.2.22 Chemical and Volume Control System Letdown Isolation

A signal to isolate the letdown valves of the chemical and volume control system is generated upon the occurrence of a Low-1 hot leg level in either of the two hot leg loops. This helps to maintain reactor coolant system inventory during mid-loop operation. This signal may be manually blocked by the operator when pressurizer level is above the P-12 setpoint. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 16. These letdown valves are also closed by the containment isolation function as described in subsection 7.3.1.2.1.

Table 7.3-1 (Sheet 8 of 8)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Controls	Actuation Logic	Permissives and Interlocks
24. Chemical and Volume Control System Letdown Isolation (Figure 7.2-1, Sheet 16)			
a. Low-1 hot leg level	1 per loop	1/2	Manual block permitted above P-12 Automatically unblocked below P-12

Deleted: None

Table 7.3-2 (Sheet 3 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Derivation	Function
P-12	Pressurizer level below setpoint	(e) Automatically unblocks chemical and volume control system letdown isolation on Low-1 hot leg level
$\overline{\text{P-12}}$	Pressurizer level above setpoint	(f) Permits manual block of chemical and volume control system letdown isolation on Low-1 hot leg level

Table 7.3-3 (Sheet 2 of 2)

SYSTEM-LEVEL MANUAL INPUT TO THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Manual Control	To Divisions				Figure 7.2-1 Sheet
CVS letdown isolation block control #1	A				16
CVS letdown isolation block control #2				D	16

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

18.d. Pressurizer Level, P-12

The P-12 interlock is provided to permit midloop operation without core makeup tank actuation, IRWST actuation, reactor coolant pump trip, or purification line isolation. With pressurizer level channels less than the P-12 setpoint, the operator can manually block low pressurizer level signal used for these actuations. Concurrent with blocking CMT actuation on low pressurizer level, IRWST actuation on Low 2 RCS hot leg level is enabled. Also, CVS letdown isolation on Low 1 RCS hot leg level is enabled. When the pressurizer level is above the P-12 setpoint, the pressurizer level signal is automatically enabled and a confirmatory open signal is issued to the isolation valves on the CMT cold leg balance lines. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

28.a. Hot Leg Level – Low 1

A signal to isolate the CVS letdown valves is generated upon the occurrence of a Low 1 hot leg level in either of the two RCS hot leg loops. This helps to maintain reactor system inventory in the event of a LOCA. This function can be blocked in Modes 1, 2 and 3 and is automatically enabled when P-12 is activated. These letdown valves are also closed by all of the initiating Functions and requirements that generate the Containment Isolation Function in Function 3.

II.22 REACTOR TRIP BREAKER STATUS INPUTS TO P-3 AND P-4 LOGIC

Figure 7.2-1, Sheet 2 shows the reactor trip breaker status inputs to the logic for the P-3 and P-4 permissives. The existing logic shows the breaker inputs being voted 2/4. There are actually 8 reactor trip breakers arranged in a 2/4 voting matrix as depicted by the simple diagram on Sheet 2. The breaker status voting has been changed to reflect the actual breaker arrangement and a Note 4 has been added to Sheet 2 that provides a logic equation defining the required functionality.

This change requires modifications to Figure 7.2-1, Sheet 2.

II.23 DELETION OF DIVISION TRIP STATUS BETWEEN DIVISIONS

The architecture of the AP1000 PMS, based on the Westinghouse Common Q platform architecture is different than the architecture of the Eagle platform that preceded it for safety applications. The Common Q architecture does not use the "Global Trip" feature that was used in the Eagle platform based protection system application that requires that each division to generate a "Trip Status". The Global Trip feature had already removed as documented in APP-GW-GLN-004 (Transmittal by Westinghouse to NRC in DCP/NRC1737 dated May 22, 2006. This change removes the remaining part of the logic associated with the Westinghouse Eagle platform application.

This change requires modifications to Figure 7.2-1, Sheet 2.

II.24 LOW T_{COLD} AND HIGH STEAM PRESSURE NEGATIVE RATE ESF ACTUATION LOGIC MODIFICATIONS

The existing logic shown on Figure 7.2-1, Sheet 9 for the Low T_{COLD} and High Steam Pressure Negative Rate functions does not segregate the across the divisions, thereby increasing the chance of an inadvertent reactor trip. For example, the prior logic would actuate if a sensor in one division associated with one loop and another sensor in another division monitoring the other loop tripped at the same time. This is inconsistent with traditional design practice that only will trip the reactor if two or more divisions monitoring the same loop are tripped. The existing logic creates an increased likelihood of inadvertent ESF actuations, thereby increasing the likelihood of challenges to safety systems. The design has been revised so that an ESF actuation will occur whenever either function is true in at least 2 divisions in one loop.

This change requires modifications to Figure 7.2-1, Sheet 9.

II.25 DELETION OF REDUNDANT AUTOMATIC SAFEGUARDS REACTOR TRIP

Figure 7.2-1, Sheet 11 shows an automatic reactor trip function composed of Low Pressurizer Pressure, High-2 Containment Pressure, Low Steamline Pressure, Low T_{COLD}, and Low-2 Pressurizer Level. The existing logic does not properly segregate the divisions and loops similar to the changes described in Items II.7, and II.24. In addition, an automatic reactor trip will already be generated by ESF actuation logic based on these same parameters as shown on revised Sheets 11 and 12. The existing logic on Sheet 11 is, therefore, both incorrectly designed and serves no purpose. It has been deleted.

This change does not affect conformance to regulatory requirements and guidance.

This change requires modifications to Figure 7.2-1, Sheets 9 and 11.

II.26 CORE MAKEUP TANK LEVEL INPUT TO ADS LOGIC MODIFICATIONS

Low-1 Core Makeup Tank (CMT) level is an input to the Automatic Depressurization System (ADS) 1st stage actuation logic and Low-2 Core Makeup Tank (CMT) level is an input to the Automatic Depressurization System (ADS) 4th stage actuation logic. The existing CMT level inputs shown on Figure 7.2-1, Sheet 15 has the same division segregation logic discrepancy that related to the changes described in Items II.7, II.24 and II.25. The logic has been revised so that the CMT level inputs to the ADS actuation logic will be properly segregated by CMT.

This change does not affect conformance to regulatory requirements and guidance.

This change requires modifications to Figure 7.2-1, Sheet 15.

II.27 CMT AND PRHR ISOLATION VALVE LOGIC CHANGES

The MAINTAIN CLOSE feature associated with both the Core Makeup Tank (CMT) and the Passive Residual Heat Removal (PRHR) isolation functions shown on Figure 7.2-1, Sheet 17 cannot be implemented as depicted. The MAINTAIN CLOSE feature is performed in the Plant Control System (PLS) and having to provide an input to the Protection and safety Monitoring System (PMS) is not permitted. The Common Q system architecture used for AP1000 uses a Component Interface Module (CIM) to accept inputs from both the PMS and PLS and perform required priority and component logic to interface to the actuated components. The MAINTAIN CLOSE feature will be implemented throughout the PLS connection to the CIM for the CMT and PRHR isolation valves.

This change does not affect conformance to regulatory requirements and guidance.

This change requires modifications to Figure 7.2-1, Sheet 17.

II.28 EDITORIAL CHANGES AND CLARIFICATIONS

None of these changes affect conformance to regulatory requirements and guidance.

Revise Section 7.1.1 to be consistent with Section 18.2.3.1

The Operation and Control Centers System description in Section 7.1.1 needs to be revised to match the similar description in section 18.2.3.1 and shown:

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system).

Deleted: workstation

Improve justification in Section 7.2.1.1.3

The fourth paragraph in the fifth sub-section of DCD 7.2.1.1.3 should be modified as shown to more-fully describe the use of the reactor coolant pump underspeed trip.

7.2.1.1.3 Core Heat Removal Trips

Reactor Trip on Reactor Coolant Pump Underspeed

The reactor coolant pump underspeed trip provides a direct measurement of the parameter of interest. It permits the plant to ride through many postulated voltage or frequency dip transients without reactor trip if safety limits are not violated. Selection of the underspeed trip setpoint and time response provide for the timely initiation of reactor trip during the complete loss of flow accident and the limiting frequency decay event, consistent with the analysis results reported in Chapter 15.

Clarify Section 7.2.1.2.3

A statement in DCD Section 7-2 implies there are three RTD thermowells in each hot leg containing dual-element RTDs that are sent to separate PMS Divisions. There are six RTD thermowells per hot leg, and there is no "sharing" between Divisions of RTD elements in the same thermowell. The RTDs are dual-element, but the second element is used as an installed spare.

7.2.1.2.3 Design Basis: Spatially Dependent Parameters Used in Reactor Trip (Paragraph 4.6 of IEEE-603-1991)

The hot and cold leg temperature signals required for input to the protection and control functions are obtained using thermowell-mounted RTDs installed in each reactor coolant loop. The hot leg temperature measurement in each loop is accomplished using six fast-response, narrow-range RTDs, each in its own thermowell; three thermowells and RTDs for each of the two divisions monitoring that hot leg. The three thermowells for each division are mounted approximately 120 degrees apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. Therefore, these signals are averaged using electronic weighting to generate a hot leg average temperature. Provisions are incorporated into the process electronics to allow for operation with only two RTDs in service. The two RTD measurements can be biased to compensate for the loss of the third RTD.

Deleted: three

Deleted: dual-element,

Deleted: in each hot leg

Correct terminology in Table 7.2-1

Table 7.2-1 should be modified as shown for consistency of format and terminology.

Table 7.2-1 (Sheet 1 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES (DESIGN BASIS FOR REACTOR TRIP) (NOMINAL)

Protective Functions	Variables To Be Monitored	Range of Variables	Typical Accuracy	Typical Response Time (Sec)(1)
Power Range Neutron Flux (Low Setpoint)	Neutron flux	1 to 120% of full power	±7.0% of span	0.2

Deleted: High
Deleted: Setting

Correct main control room damper in Table 7.5-9

Table 7.5-9 (Sheet 3 of 4) incorrectly labels the MCR isolation valves as 'dampers.' These isolation devices are actually valves. Table 7.5-9 (Sheet 3 of 4) should be corrected as shown below. Table 7.5-1 (Sheet 10 of 12) correctly lists these as valves. Table 7.5-7 (Sheet 4 of 4) was corrected in Reference 4.

Table 7.5-9 (Sheet 3 of 4)

SUMMARY OF TYPE F VARIABLES

Variable	**Type/Category**
Main control room supply air isolation valve status	F3
Main control room return air isolation valve status	F3

Deleted: damper
Deleted: damper

Add omitted manual Reactor Trip Block to Table 7.2-4

The manual block for the High-2 Steam Generator Water Level Reactor Trip that is referenced as part of Section 7.2.1.1.11 of the DCD was omitted from Table 7.2-4. Add the text shown below to the existing table to correct this omission.

Table 7.2-4

SYSTEM-LEVEL MANUAL INPUTS TO THE REACTOR TRIP FUNCTIONS

Manual Control	To Divisions				Figure 7.2-1 Sheet
Steamline / Feedwater Isolation and Safeguards Block, Division A	A				9
Steamline / Feedwater Isolation and Safeguards Block, Division B		B			9
Steamline / Feedwater Isolation and Safeguards Block, Division C			C		9
Steamline / Feedwater Isolation and Safeguards Block, Division D				D	9

Index and symbols changes and additions

Several additions and clarifications have been made to Figure 7.2-1, Index and Symbols. SET/RESET MEMEORY and ONE SHOT functions have been added and state tables have been included for both of the memory functions used. General notes that apply to the entire set of functional diagrams presented in Figure 7.2-1.

Outputs to PLS

A variety of isolated outputs provided to the Plant Control System (PLS). Sheet numbers for the appropriate PLS functional diagrams have been updated consistent with current documentation.

Steam generator water level reactor trip logic organization

The logic for most reactor trip appear at the left hand side of Figure 7.2-1, Sheet 2 as a single input to the "Big OR" logic gate that makes up the automatic reactor trip function. The existing steam generator low and high water level trips are exceptions, with each steam generator appearing as a separate input. The depiction has been changed to have only one input for each function with the combination of the two steam generators performed on Sheets 7 and 10. This change in depiction is for presentation consistency only; it does not change the actual implementation of the functions.

This change requires modifications to figure 7.2-1, sheets 2, 7, and 10.

Cumulative timer to monitor vital instrument bus battery charger voltage

Because there is no vital AC power, the instrumentation bus batteries can become depleted if input power to their chargers is unavailable for an extended period of time. The timer shown on Figure 7.2-1 has been renamed to a CUMULATIVE rather a RETENTIVE time to better describe its function to accumulate time without power to the battery chargers at to actuate required safety functions if the batteries might be near to depletion. NOTE 6 is added to the timer and the note is revised to better describe the timer function.

This change requires modifications to figure 7.2-1, sheet 15.

Special Monitoring System description

The description of the special monitoring system was modified to allow a minimum of 2 sensors at each location instead of just 2 sensors at each location, as well as depicting channel separation. Paragraph 2 on page 7.1-4 was modified as follows:

The special monitoring system is the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system is composed of digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service. Then metal impact monitoring system is described in subsection 4.4.6.4.

Deleted: The sensors and their related signal processing devices are mounted in pairs

---

Update references in Chapter 7 to reflect proper format

Reference 18 on page 7.1-15 is updated with the current reference date, May 2006 and the "Westinghouse Electric Company LLC" is removed.

Establishing a cross reference between figure 7.2-1 and AP1000 drawings

Figure 7.2-1 was derived from AP1000 drawings and the references on this figure are tied to those drawings. Paragraph 3 on page 7.2-2 is updated to describe this and table 7.2-5 is added to list the appropriate drawing number for each sheet. Changes to paragraph 3 are as follows:

Subsection 7.2.1.1 provides a description of each of the reactor trip functions. Figure 7.2-1 shows the functional diagrams for reactor trips, as well as functional diagrams for other related plant functions. Figure 7.2-1 sheets are derived from the APP-PMS-J1 drawings and the references shown on Figure 7.2-1 sheets are tied to these parent drawings and not the sheets. Table 7.2-5 provides a cross reference to match the APP-PMS-J1 drawing to its corresponding Figure 7.2-1 sheet.

Add the following table 7.2-5 to section 7.2 of chapter 7.

Table 7.2-5

FIGURE 7.2-1 CROSS REFERENCES

APP-PMS-J1 Drawing Number	Figure 7.2-1 Sheet Number
APP-PMS-J1-101	1
APP-PMS-J1-102	2
APP-PMS-J1-103	3
APP-PMS-J1-104	4
APP-PMS-J1-105	5
APP-PMS-J1-106	6
APP-PMS-J1-107	7
APP-PMS-J1-108	8
APP-PMS-J1-109	9
APP-PMS-J1-110	10
APP-PMS-J1-111	11
APP-PMS-J1-112	12
APP-PMS-J1-113	13
APP-PMS-J1-114	14
APP-PMS-J1-115	15
APP-PMS-J1-116	16
APP-PMS-J1-117	17
APP-PMS-J1-119	18
APP-DAS-J1-102	19
APP-DAS-J1-103	20

II.29 CLARIFICATION OF REMOTE SHUTDOWN WORKSTATION REDUNDANCY

The AP1000 Remote Shutdown Workstation (RSW) is non-safety. It is designed with redundancy so it retains functionality with most single failures. The words in DCD Section 7.4.3.1.3 could be interpreted as implying that the RSW meets the safety system single-failure requirement.

This change does not affect conformance to regulatory requirements and guidance.

The fifth bullet of section 7.4.3.1.3 will be revised as shown:

- The remote shutdown workstation is designed with redundancy. When a random event, such as a fire, or an allowable technical specification maintenance results in one safety-related division being unavailable, a single failure in a redundant division is not postulated. When a random event other than fire causes a main control room evacuation, a coincident single failure in the safety systems controlled from the remote shutdown workstation is considered.

Deleted: for a single failure

II.30 CONTROL SYSTEM FUNCTIONAL MODIFICATIONS

Correction to description of signal selector algorithm

The signal selector algorithm applies to analog signals only. Binary signals use 2/4 voting logic to prevent a single failure in the protection and safety monitoring system from affecting the control system.

This change does not affect conformance to regulatory requirements and guidance.

The fourth paragraph of section 7.1.3.2 will be revised as shown:

7.1.3.2 Signal Selector Algorithms

Signal selector algorithms provide the plant control system with the ability to obtain inputs from the protection and safety monitoring system. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if one of four redundant protection channels is degraded by random failure simultaneous with another of the four channels bypassed for test or maintenance.

Each signal selector algorithm receives data from each of the redundant divisions of the protection and safety monitoring system. The data is received from each division through an isolation device.

The signal selector algorithms provide validated process values to the plant control system. They also provide the validation status, the average of the valid process values, the number of valid process values, an alarm (if one process value has been rejected), and another alarm (if two process values have been rejected).

For the logic values received from the protection and safety monitoring system, such as permissives, two-out-of-four (2/4) voting is used to provide a valid logic value to the plant control system.

Deleted: the signal selector algorithms perform voting on the logic values

Deleted: They also provide the validation status, the number of valid logic values, an alarm if one logic value differs from the voted value, and another alarm if two logic values differ from the voted value.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the description of pressurizer water level control

The pressurizer water level in the AP1000 is maintained within an operating region which is programmed as a function of T_{avg}. No action is taken to increase or decrease the water level if it is anywhere within the operating band. The system setpoints are on the upper and lower limits of the operating region, not on the programmed nominal level. Compensation is applied to the nominal water level only during load regulation operations. The pressurizer water level control paragraph of section 7.7.1 will be revised as shown:

Pressurizer Water Level Control - The pressurizer water level control system establishes, and maintains or restores pressurizer water level to its programmed operating region. The required water level operating region is programmed as a function of reactor coolant system temperature to minimize charging and letdown requirements. No challenges to the protection system result from normal operational transients.

Deleted: value

Deleted: and power generation

Section 7.7.1.7 has been revised as shown:

7.7.1.7 Pressurizer Water Level Control System

The pressurizer water inventory, or level control, provides a reservoir for the reactor coolant system inventory changes that occur due to changes in reactor coolant system density. As the reactor coolant system temperature is increased from hot zero-load to full-load values, the reactor coolant system fluid expands. The pressurizer level is programmed to absorb this change. A deadband is provided around the nominal pressurizer level program to intermittently control charging and letdown. When the pressurizer water level reaches the lower limit of the deadband, it actuates the charging system. The charging system continues to operate until the level is restored to a limit above the nominal program value. When the pressurizer water level reaches the upper limit of the deadband, it actuates letdown to the liquid waste processing system.

Deleted: med setpoint

Pressurizer water level control provides stable and accurate control of pressurizer level within a prescribed deadband around the programmed setpoint value, as derived from the plant operating parameters. Automatic level control is supplied from the point in the startup cycle where the hot zero-load level is established through

100-percent power. The nominal water level program is also compensated for changes in operating temperature that occur during load regulation operations.

Deleted: reference

Deleted: result from such items as rod control deadband, or reduced T_{avg} return to power operation

---

Correction to the description of MSHIM operation

Westinghouse is reevaluating the MSHIM operating strategy to emphasize base load operations and to support a reduction of effluent production during boron concentration changes to account for fuel burnup. DCD section 4.3.4.2.16 is affected by this change. Revise subsection of 4.3.2.4.16 as shown:

4.3.2.4.16 Load Follow Control and Xenon Control

During load follow maneuvers, power changes are primarily accomplished using control rod motion alone, as required. Control rod motion is limited by the control rod insertion limits as provided in the technical specifications and discussed in subsections 4.3.2.4.12 and 4.3.2.4.13. The power distribution is maintained within acceptable limits through limitations on control rod insertion. Reactivity changes due to the changing xenon concentration are also controlled by rod motion.

Rapid power increases (five percent/min) from part power during load follow operation are accomplished with rod motion.

The rod control system is designed to automatically provide the power and temperature control described above 30 percent rated power for most of the cycle length without the need to change boron concentration as a result of the load maneuver. The automated mode of operation is referred to as mechanical shim (MSHIM) because of the usage of mechanical means to control reactivity and power distribution simultaneously. MSHIM operation allows load maneuvering without boron change because of the degree of allowed insertion of the control banks in conjunction with the independent power distribution control of the axial offset (AO) control bank. The worth and overlap of the MA, MB, MC, MD, M1, and M2 control banks are designed such that the AO control bank insertion will always result in a monotonically decreasing axial offset. MSHIM operation uses the MA, MB, MC, MD, M1, and M2 control banks to maintain the programmed coolant average temperature throughout the operating power range. The AO control bank is independently modulated by the rod control system to maintain a nearly constant axial offset throughout the operating power range. The degree of control rod insertion under MSHIM operation allows rapid return to power without the need to change boron concentration.

Deleted: Anticipated MSHIM load follow operation operates with two gray banks fully inserted to provide enough reactivity worth to compensate for transient reactivity effects without the need for soluble boron changes. The degree of control rod insertion under MSHIM operation allows rapid return to power without the need to change boron concentration.¶

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the description of T_{avg} compensation

The DCD describes lead/lag compensation applied to the T_{avg} signal before it passes through the high auctioneer. The AP1000 design is revised so that the lead/lag compensation is applied after the high auctioneer. In addition to simplifying the implementation, this approach does not require compensation to be factored into signal quality check acceptance criteria in the auctioneer. The second paragraph of section 7.7.1.1.1 will be revised as shown:

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the highest of the T_{avg} measured temperatures from each of the reactor coolant loops constitutes the primary control signal. The programmed coolant temperature increases linearly with turbine load from the zero-power to the full-power condition.

Deleted: lead/lag compensated

Correction to the description of the T_{avg} control band

Base load and load follow operations use the same T_{avg} control dead band. There is no advantage to increasing the dead band during load follow operations; in fact, doing so would erode margins to reactor trip setpoints. Expanding the dead band during load regulation operations allows some of the power change to be handled by the negative moderator coefficient. The sixth paragraph of section 7.7.1.1.1 will be revised as shown:

Separate reactor control deadbands are used for various modes of control. If the plant is in a load regulation mode of operation, then the deadband is widened from that used for base load or load follow operation. This allows the core reactivity feedbacks to assist in stabilizing the plant at the conclusion of the maneuver and reduces the total control rod movement and subsequent wear on the control rods.

Deleted: each

Deleted: (load follow, load regulation, or base load)

Deleted: load follow or

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the description of the axial offset control

The AP1000 transient specification does not require complex "time weighted average" nuclear flux and axial offset signal compensation on the inputs to the axial offset control band calculation. Simple lag compensation is adequate. Section 7.7.1.1.2 will be revised as shown:

7.7.1.1.2 Axial Offset Control

The axial offset control subsystem controls the core axial offset (power difference between the top and bottom halves of the core) to a value that is within the desired control range for load follow and grid frequency change transients. This is accomplished by using control rod banks separate from those used for the reactor power control described in subsection 7.7.1.1.1. Measurements of axial offset are input into the axial offset control subsystem and then compared to an axial offset control "window." This window is calculated from measurements of compensated excore nuclear flux, along with operator inputs for the desired axial offset target value and target bandwidth and the mode of control (load follow, load regulation, or base load). The nuclear flux signals are compensated by measurements of cold leg temperature to account for the effects of moderation of the neutron flux by the reactor vessel downcomer flow. If the plant is in a load regulation mode of control, then lag compensation is applied to both the nuclear flux and the axial offset signals. This provides a smoothed nuclear flux and axial offset signal input to the axial offset controller to avoid rapid temporary changes from actuating axial offset control. When the axial offset error is outside the acceptable control window, the axial offset rods are actuated until the axial offset error is back inside the control window.

Deleted: a "smoothing"

Deleted: time-weighted average

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the control rod group-to-bank assignments

In the current control rod group-to-bank assignments there is one bank with three groups, two banks with two groups, and three banks with one group each. The fifth paragraph of section 7.7.1.2 will be revised as shown:

The power and axial offset control rod banks are the only rods that can be manipulated under automatic control. Each bank contains one or more groups of four control rod assemblies. Each control rod assembly in a group is electrically paralleled to move simultaneously. There is individual position indication for each control rod assembly.

Deleted: is divided into two or more groups to obtain smaller incremental reactivity changes per step

---

Correction to the control rod insertion limits

The interlock and "low" and "low-low" alarms associated with control rod insertion limits have ben revised. Section 7.7.1.4 will be revised as shown:

7.7.1.4 Control Rod Insertion Limits

With the reactor critical, the normal indication of reactivity status in the core is the position of the control rod bank in relation to reactor power (as indicated by the ΔT power monitors). The ΔT power signal is used to calculate insertion limits for the banks. The following two alarms are provided for each bank.

- A "low" alarm alerts the operator of an approach to the M bank or AO bank insertion limits. Further approach is avoided by following appropriate plant operating procedures.

- A "low-low" alarm alerts the operator to take immediate action to restore margin to the M bank or AO bank insertion limits. Interlocks will terminate automatic AO bank withdrawal (to prevent further insertion of the M banks) or insertion (to avoid the AO bank insertion limit).

The purpose of the control bank rod insertion alarms and interlocks is to provide warning to the operator of excessive rod insertion and to terminate the insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip. It also provides a limit on the maximum inserted rod worth in the unlikely event

Deleted: and interlock

Deleted: rod

Deleted: and acts to terminate automatic AO bank rod insertion (on reaching the AO bank "low" setpoint) or AO bank rod withdrawal (on reaching a M bank "low" setpoint). The operator terminates M bank insertion and reactor coolant system boron concentration changes by following appropriate plant procedures

Deleted: and

Deleted: within the appropriate limits by terminating M bank insertion or AO bank withdrawal (for "low-low" M bank alarm), or terminating AO bank insertion (for "low-low" AO bank alarm) that were not stopped by the "low" setpoint interlock of a hypothetical rod ejection. Insertion limits provide confidence that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits are decreased (the rods must be withdrawn further) with increasing power. The insertion limits for the M banks and the AO bank are calculated from the reactor power, as measured by the ΔT power monitor, according to the following equations:

$$Z^{M}_{LL} = A + B \cdot \Delta T + C \cdot Z_{AO} + D \cdot \Delta T \cdot Z_{AO}$$

$$Z^{AO}_{LL} = E$$

where:

Z^{M}_{LL} = Maximum permissible insertion limit for the affected M control bank

Z^{AO}_{LL} = Maximum permissible insertion limit for the affected AO control bank

Z_{AO} = Current AO bank position

ΔT = Mediam value of the ΔT measurements

Deleted: Average signal of valid

A,B,C,D,E = Constants chosen to maintain $Z_{LL} \geq$ the actual limit based on physics calculations

The control rod bank demand position (Z) for the M banks and the AO bank is compared to the respective ZLL as follows:

- If Z - ZLL ≤ F, a low alarm is actuated.
- If Z - ZLL ≤ G, a low-low alarm and interlock is actuated.

Deleted: and interlock

Since nuclear peaking factors can be aggravated by the opposite movement of the M banks and the AO bank, the interlocks on the AO bank are different, depending on whether the M bank or the AO bank insertion limit setpoint is actuated. If an M bank insertion limit is reached, this stops AO bank withdrawal and reduces the increases in the core peaking factor. If an AO bank insertion limit is reached, this stops AO bank insertion. If the M banks are fully withdrawn, AO bank automatic insertion is blocked.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the description of the pressurizer pressure control system

Variable heater control is not sensitive to the rate of change in pressure. It will respond the same to fast or slow small changes in pressure. The third paragraph of section 7.7.1.6 will be revised as shown:

Small changes in pressure are regulated by modulation of the variable heater control. Reset (integral) action is included to maintain pressure at its setpoint. Decreases in pressure larger than that which can be accommodated by the variable heater control results in the actuation of the backup heaters. The backup heaters are deactivated when the variable heaters alone are capable of restoring pressure. Large increases in the pressurizer water level also result in activation of the backup heaters. The purpose of this action is to avoid the accumulation of subcooled fluid in the pressurizer, thereby allowing flashing of the pressurizer fluid to limit the pressure decrease on any subsequent outsurge.

Deleted: or slowly varying

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to the description of feedwater control logic

DCD Section 7.7.1.8 provides information on the feedwater controls. This section discusses controlling the lift on the main and startup feedwater control valves using predicted differential pressure across the control valve and the characteristic C_V of the valve. This logic has been revised. Also, in the current feedwater control system design, only feedwater temperature (low power mode) and steam flow (high power mode) are used to tune the integrator setpoints. Sections 7.7.1.8.1 and 7.7.1.8.2 will be revised as shown:

7.7.1.8.1 Feedwater Control

The feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during steady-state operation, and limits the water level shrink and swell during normal plant transients. This prevents an undesirable reactor trip actuation. Indication is provided for monitoring system operation. Alarms and indications are provided to alert the plant operator of control system malfunctions or abnormal operating conditions.

Two modes of feedwater control are incorporated in the feedwater control subsystem. In the high-power control mode, the feedwater flow is regulated in response to changes in steam flow and proportional plus integral (PI)-compensated steam generator narrow range water level deviation from setpoint. In the low-power control mode, the feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow range water level deviation from setpoint.

Deleted: A separate low range feedwater flow measurement is used in the low-power feedwater control mode.

The transition from the low to the high-power control mode is initiated on the basis of the filtered high range feedwater flow signal. The transition point is set at a feedwater flow corresponding to a power at which reliable steam flow indication is expected. The transition point is also low enough to allow effective feedforward control using wide range water level, and to allow feedwater flow indication within the upper limit of the low range feedwater flow measurement. Tracking is provided to allow a smooth transition between control modes and between manual and automatic control.

Deleted: If feedwater flow indication falls below the lower limit of the effective span of the low range feedwater flow measurement, integration (reset) action of the low-power mode feedwater flow controller is inhibited.

A high steam generator water level signal reduces the feedwater flow demand signal and closes the feedwater control valves.

Deleted: The feedwater valve lift required to provide the demanded feedwater flow is computed on the basis of the estimated ΔP available across the feedwater control valve, and the CV characteristic of the valve. This compensation improves the response to changes in system ΔP, such as following the loss of one feedwater pump during high-power operation. ¶

7.7.1.8.2 Startup Feedwater Control

During no-load or very low power conditions, the main feedwater control subsystem is not intended to be used for automatic control of the steam generator water level. The startup feedwater control subsystem performs this function.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

The startup feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during low power (below approximately 10 percent of plant rated thermal power), no-load, and plant heatup and cooldown modes. During low feedwater flow demand, feedwater is controlled by the startup feedwater control subsystem. Transition between the main and startup feedwater line is automatically controlled based on flow measurements within the respective lines. The startup feedwater is also automatically actuated on signals which indicate a loss of water inventory or heat sink in the secondary side of the steam generator and will attempt to recover the inventory loss and return the steam generator water level to the programmed value. If the startup feedwater cannot recover the inventory deficit, reactor cooling is initiated by the passive residual heat removal system.

Deleted: control subsystem

Deleted: control subsystem

The startup feedwater control subsystem regulates the flow of feedwater in a manner which is similar to the way (main) feedwater is controlled in the low-power control mode. Feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow range water level deviation from setpoint. Tracking is provided to allow a smooth transition between control modes and between manual and automatic control.

Deleted: The startup feedwater control valve lift required to provide the demanded startup feedwater flow is computed on the basis of the estimated ΔP available across the startup feedwater control valve, and the C_V characteristic of the valve. This compensation improves the response to changes in system ΔP, such as during plant heatup or cooldown where the steam pressure can change drastically.¶

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Revision to Section 7.6 to be Consistent with Technical Specifications

Section 7.6.2.3 is revised as shown to be consistent with the technical specifications 3.5.1, 3.5.6, 3.5.7, and 3.5.8.

7.6.2.3 Interlocks for the Accumulator Isolation Valve and IRWST Discharge Valve

The accumulator isolation and in-containment refueling water storage tank injection isolation valves are safety-related in order to retain their pressure boundary and remain in their open position. The accumulator isolation and in-containment refueling water storage tank injection valve operators are nonsafety-related since the valves are not required to change position to mitigate an accident. The DCD Chapter 15 safety analyses assume that these valves are not subject to valve mispositioning (prior to an accident) or spurious closure (during an accident). Valve mispositioning and spurious closure are prevented by the following:

- The Technical Specifications, Section 16.1, require these valves to be open and power locked out whenever these injection paths are required to be available. The accumulators are required to be available when the reactor coolant system pressure is above 1000 psig. Both in-containment refueling water storage tank injection lines are required to be available in Modes 1, 2, 3, and 4. One in-containment refueling water storage tank injection line is required to be available in Mode 5 and in Mode 6.

Deleted: psia

Deleted: with the reactor upper internals not removed and the refueling cavity not filled

---

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.33 POST-ACCIDENT MONITORING SYSTEM TABLE CHANGES

This section contains changes in the post-accident monitoring system tables that affect chapter 7 of the DCD that are described in APP-GW-GLN-004 (TR-39) and APP-GW-GLN-118 (TR-118).

This change does not affect conformance to regulatory requirements and guidance.

Table 7.5-1 is revised as shown below and as described in APP-GW-GLN-004 (TR-39)

Table 7.5-1 (Sheet 3 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Startup feedwater flow	0-1000 gpm	F2	Mild	Yes	1/steam generator (Note 11)	1E	No	
Startup feedwater control valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Containment pressure	-5 to 10 psig	B1, C2, D2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
Containment pressure (extended range)	0 to 240 psig	C1	Harsh	Yes	3 (Note 4)	1E	Yes	
Containment area radiation (high range)	10^0-10^7 R	C1, E2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
Reactor vessel hot leg water level	0-100% of span	B2, B3	Harsh	Yes	1	1E	Yes	Two instruments are provided
Plant vent radiation level	(Note 3)	C2, E2	Mild	None	1	Non-1E	No	
Remotely operated containment isolation valve status	Open/ Closed	B1, D2	Harsh/mild	Yes	1/valve (Note 7)	1E	Yes	Separate divisions on series valves
Boundary environs radiation	N/A	C3, E3	None	None	N/A	Non-1E	No	Site specific
Hydrogen concentration	0-20%	C3	None	None	1	Non-1E	No	Three instruments are provided

Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 4 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Class 1E dc switchboard voltages	0-150 Vdc	D2	Mild	Yes	1/switchboard	1E	Yes	
Diesel generator status	On/Off	F3	None	None	1/diesel generator	Non-1E	No	
Diesel generator load	0-6000 kW	F3	None	None	1/diesel generator	Non-1E	No	
Voltage for diesel-backed buses	0-8600V	F3	None	None	3/bus	Non-1E	No	
Power supply to diesel-backed buses	On/Off	F3	None	None	1/supply source/bus	Non-1E	No	
RCP bearing water temperature	70-450°F	F3	Mild	Yes	1/RCP (Note 10)	1E	Yes	
RCP breaker status	Open/ Closed	D2, F3	Mild	Yes	1/breaker (Note 11)	1E	No	
Reactor trip breaker status	Open/ Closed	D2	Mild	Yes	1/breaker (Note 11)	1E	No	
MCR air storage bottle pressure	0-5000 psig	D2	Mild	None	1	Non-1E	No	Two instruments are provided
Turbine stop valve status	Open/ Closed	D2	None (Note 12)	None	1/valve	Non-1E	No	
Turbine control valve status	Open/ Closed	D2	None (Note 12)	None	1/valve	Non-1E	No	
Pressurizer pressure	1700-2500 psig	B1, D2	Harsh	Yes	3 (Note 4)	1E	Yes	
Pressurizer safety valve status	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
Pressurizer heater power (current)	0-800 amps	F3	None	None	1/group	Non-1E	No	
Steam generator PORV status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	

Deleted: None
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: ¶

Table 7.5-1 (Sheet 5 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
Steam generator PORV block valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam generator safety valve status	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
Main feedwater isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main feedwater flow	0-9x10^6 lb/hr	F3	None	None	1/feedline	Non-1E	No	
Main feedwater control valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam generator blowdown isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam flow	0-9x10^6 lb/hr	F3	None	None	1/steam generator	Non-1E	No	
Main steam line isolation valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main steam line isolation bypass valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main feedwater pump status	On/Off	D2, F3	Mild	None	1/pump	Non-1E	No	
Main to startup feedwater crossover valve status	Open/ Closed	D2, F3	Mild	None	1/valve	Non-1E	No	
Startup feed-water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Circulating water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Condenser backpressure	0-1 atm	F3	None	None	1	Non-1E	No	

Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 6 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
Startup feedwater Isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Condenser steam dump valve status	Open/ Closed	D2, F3	Mild	None	1/valve	Non-1E	No	
Condensate storage tank water level	0-100% of span	F3	None	None	1	Non-1E	No	
PCS water storage tank isolation valve status (Non-MOV)	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
PCS water storage tank series isolation valve status (MOV)	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Containment temperature	32-400°F	D2, F3	Harsh	None	1	Non-1E	No	
CCS surge tank level	0-100% of span	F3	None	None	1	Non-1E	No	
CCS flow	0-15,000 gpm	F3	None	None	1	Non-1E	No	
CCS pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
CCS flow to RNS valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
CCS flow to RCPs valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
CCS pump inlet temperature	50-200°F	F3	None	None	1	Non-1E	No	
CCS heat exchanger outlet temperature	50-130°F	F3	None	None	1	Non-1E	No	
Containment fan cooler status	On/Off	F3	None	None	1/fan	Non-1E	No	

Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 7 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
Water-cooled chiller status	On/Off	F3	None	None	1/chiller	Non-1E	No	
Water-cooled chilled water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Water-cooled chilled water valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Spent fuel pool pump flow	0-1500 gpm	F3	None	None	1/pump	Non-1E	No	
Spent fuel pool temperature	50-250°F	F3	None	None	1	Non-1E	No	
Spent fuel pool water level	0-100% of span	D2, F3	Mild	Yes	3 (Note 4)	1E	Yes	
CMT discharge isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT upper water level switch	Above/ Below	D2, F2	Harsh	Yes	1/tank	1E	Yes	
CMT lower water level switch	Above/ Below	D2, F2	Harsh	Yes	1/tank	1E	Yes	
IRWST injection isolation valve (Squib)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
IRWST line isolation valve status (MOV)	Open/ Closed	D3	None	None	1/valve	Non-1E	No	
ADS: first, second and third stage valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	

Deleted: No
Deleted: Non-
Deleted: No

Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 8 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification: Environmental	Qualification: Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
ADS fourth stage valve status (Non-MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
ADS fourth stage valve status (MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
PRHR HX inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1 (Note 7)	1E	Yes	
PRHR HX control valve status	Position	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
IRWST gutter bypass isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Accumulator pressure	100-800 psig	D2	Harsh	None	1/tank	Non-1E	No	
Accumulator isolation valve status	Open/ Closed	D3	None	None	1/valve	Non-1E	No	
Accumulator vent valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Pressurizer spray valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Auxiliary spray line isolation valve status	Open/ Closed	D2, F3	Harsh	Yes	1 (Note 7)	1E	Yes	
Purification stop valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 11)	1E	No	
Containment recirculation isolation valve status (Non-MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Containment recirculation isolation valve status (MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	

Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 9 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
Purification return line stop valve status	Open/ Closed	D2	Harsh	None	1	Non-1E	No	
Boric acid tank level	0-100%	F3	None	None	1	Non-1E	No	
Demineralized water isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Boric acid flow	0-300 gpm	F3	None	None	1	Non-1E	No	
Makeup blend valve status	Position	F3	None	None	1	Non-1E	No	
Makeup flow	0-300 gpm	F3	None	None	1	Non-1E	No	
Makeup pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Makeup flow control valve status	Position	F3	None	None	1	Non-1E	No	
Letdown flow	0-250 gpm	F3	None	None	1	Non-1E	No	
RNS hot leg suction isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
RNS flow	0-3000 gpm	F3	None	None	1/pump	Non-1E	No	

Deleted: None

Deleted: Non-

Deleted: No

Table 7.5-1 (Sheet 10 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification: Environmental	Qualification: Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
IRWST to RNS suction valve status	Open/ Closed	B1, F3	Harsh	Yes	1 (Note 7)	1E	Yes	
RNS discharge to IRWST valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
RNS pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Reactor vessel head vent valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
MCR return air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR toilet exhaust isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR supply air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR differential pressure	-1" to +1" wg	D2	Mild	Yes	2	1E	Yes	
MCR air delivery flowrate	0-80 cfm	D2	Mild	Yes	2	1E	Yes	

Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No
Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 (Sheet 11 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification Environmental	Qualification Seismic	Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
MCR air delivery isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Instrument air header pressure	0-125 psig	F3	None	None	1	Non-1E	No	
Service water flow	0-10,000 gpm	F3	None	None	1/pump	Non-1E	No	
Service water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Service water pump discharge valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Service water pump discharge temperature	50-150°F	F3	None	None	1/pump	Non-1E	No	
Main control room supply air radiation	Note 5	E3, F3	Mild	Yes	2 (Note 9)	1E	No	
Plant vent air flow	0-110% design flow	E2	Mild	None	1	Non-1E	No	
Turbine island vent discharge radiation level	10^{-6} - 10^{-5} μCi/cc	C2, E2	Mild	None	1	Non-1E	No	
Steam generator blowdown discharge radiation	10^{-6} - 10^{-1} μCi/cc	C2	Mild	None	1	Non-1E	No	
Steam generator blowdown brine radiation level	10^{-6} - 10^{-1} μCi/cc	C2	Mild	None	1	Non-1E	No	

Deleted: None
Deleted: Non-
Deleted: No

Table 7.5-1 is revised as shown below and as described in APP-GW-GLN-118 (TR-118)

Table 7.5-1 (Sheet 9 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Purification return line stop valve status	Open/ Closed	D2	Harsh	None	1	Non-1E	No	
Boric acid tank level	0-100%	F3	None	None	1	Non-1E	No	
Demineralized water isolation valve status	Open/ Closed	D2	Mild	None	1/valve	Non-1E	No	
Boric acid flow	0-~~300~~ gpm 175	F3	None	None	1	Non-1E	No	
Makeup blend valve status	Position	F3	None	None	1	Non-1E	No	
Makeup flow	0-~~300~~ gpm 175	F3	None	None	1	Non-1E	No	
Makeup pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Makeup flow control valve status	Position	F3	None	None	1	Non-1E	No	
Letdown flow	0-~~250~~ gpm 120	F3	None	None	1	Non-1E	No	
RNS hot leg suction isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
RNS flow	0-3000 gpm	F3	None	None	1/pump	Non-1E	No	

II.34 DAS PLATFORM TECHNOLOGY AND REMOTE INDICATION CHANGES

This section contains changes in the DAS system that affect chapter 7 of the DCD that are described in APP-GW-GLN-022 (TR-97).

This change does not affect conformance to regulatory requirements and guidance.

Section 7.7.1.11 has been revised as follows:

Automatic Actuation Function

The automatic actuation signals provided by the diverse actuation system are generated in a functionally diverse manner from the protection system actuation signals. The common-mode failure of sensors of a similar design is also considered in the selection of these functions.

The automatic actuation function is accomplished by redundant logic subsystems. Input signals are received from the sensors by an input signal conditioning block, which consists of one or more electronic modules. This block converts the signals to standardized levels, provides a barrier against electromagnetic and radio frequency interference, and presents the resulting signal to the input signal conversion block. The conversion block continuously performs analog to digital signal conversions and stores the value for use by the signal processing block.

Deleted: ~~microprocessor-based~~

The signal processing block polls the various input signals, evaluates the input signals against stored setpoints, executes the logic when thresholds are exceeded, and issues actuation commands.

Deleted: ~~inputs under the control of a software-based algorithm~~

Deleted: ~~programmed~~

The resulting output signals are passed to the output signal conversion block, whose function is to convert logic states to parallel, low-level dc signals. These signals are passed to the output signal conditioning block. This block provides high-level signals capable of switching the traditional power plant loads, such as breakers and motor controls. It also provides a barrier against electromagnetic and radio frequency interference.

Deleted: ~~microprocessor~~

Diversity is achieved by the use of a different architectures, hardware implementations, and any software from that of the protection and safety monitoring system.

Deleted: ~~different~~

Deleted: ~~different~~

Diversity of any software is achieved by running different operating systems and programming in different languages.

Deleted: ~~The diverse design uses standard input modules designed for use with small industrial computer systems. It also uses a microprocessor board different from those used in the protection system.~~¶
~~Software diversity~~

Manual Actuation Function

*[The manual actuation function of the diverse actuation system is implemented by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the control room multiplexers, the protection and safety monitoring system cabinets, and the diverse actuation system automatic logic.]**

The diverse manual functions are:

- Reactor and turbine trip
- Passive containment cooling actuation
- Core makeup tank actuation and reactor coolant pump trip
- Open stage 1 automatic depressurization system valves
- Open stage 2 automatic depressurization system valves
- Open stage 3 automatic depressurization system valves
- Open stage 4 automatic depressurization system valves
- Open the passive residual heat removal discharge isolation valves and close the in-containment refueling water storage tank gutter isolation valves
- Selected containment penetration isolation
- Containment hydrogen igniter actuation
- Initiate in-containment refueling water storage tank injection
- Initiate containment recirculation
- Initiate in-containment refueling water storage tank drain to containment

In addition to the above functions, a redundant method of actuating the following components is provided at the DAS squib valve control cabinet:

- **Open stage 4 automatic depressurization system valves**
- **Initiate in-containment refueling water storage tank injection**

- **Initiate containment recirculation**
- **Initiate in-containment refueling water storage tank drain to containment**

Indication

To support the diverse manual actuations, sensor outputs are displayed in the main control room in a manner that is diverse from the protection system display functions. The instrument sensor output displayed in the main control room is repeated at the DAS instrumentation cabinet. The indications that are provided from at least two sensors per function are:

- Steam generator water level – for reactor trip and passive residual heat removal actuations, and for overfill prevention by manual actuation of the automatic depressurization system valves
- Hot leg temperature – for passive residual heat removal actuation
- Core exit temperature – for automatic depressurization system actuation and subsequent initiation of in-containment refueling water storage tank injection and also containment hydrogen igniter actuation
- Pressurizer level – for core makeup tank actuation and reactor coolant pump trip
- Containment temperature – for containment isolation and passive containment cooling system actuation

Equipment Qualification and Quality Standards

The diverse actuation system is located in a controlled environment, but is capable of functioning during and after normal and abnormal events and conditions that include:

- Wide temperature range of 40° to 120°F
- Noncondensing relative humidity up to 95 percent
- Radio frequency and electromagnetic interference

The diverse actuation system processor cabinets are located in the portion of the Annex Building that is a Seismic Category II structure. The diverse actuation system equipment, including actuated devices, is designed and tested in accordance with industry standards. The adequacy of the hardware and any software is demonstrated through the verification and validation program discussed in subsection 7.1.2.14. This program provides for the use of commercial off-the-shelf hardware and software. As the diverse actuation system performs many of the protection functions associated within the ATWS systems used in existing plants, the diverse actuation system is designed to meet the quality guidelines established by Generic Letter 85-06, "Quality Assurance Guidelines for ATWS Equipment that is not Safety-Related."

PART B – CHANGES TO BE INCORPORATED IN NEXT DCD REVISION

II. TECHNICAL DESCRIPTIONS AND JUSTIFICATIONS

II.1 DESIGN COMPLETION

Table 1.6-1 is revised to correct the references.

1. Delete the reference to WCAP-13382, which is AP600 specific and described the Eagle product line.

2. Delete the reference to WCAP-13383, which is AP600 specific and related to the Eagle product line.

3. Delete the reference to WCAP-14080 and WCAP 14081 which are AP600 specific.

4. Change the reference for the Software Program Manual from CE-CES-195 Rev. 01 to WCAP-16096-NP-A 01A. The new reference is the latest Nuclear Regulatory Commission accepted version. The Software Program Manual was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML0305507760 (Reference 8), and ML042730580 (Reference 9).

5. Change the reference for the Common Qualified Platform Topical Report from CENPD-396-P, Rev. 01 to WCAP-16097-P-A, Rev. 0. The new reference is the latest Nuclear Regulatory Commission accepted version. The Common Q Platform was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML011690170 (Reference 7), and ML0305507760 (Reference 8).

6. Add the reference to WCAP-16361 which is an AP1000 technical report that has been separately submitted to the Nuclear Regulatory Commission.

7. Add the reference to WCAP-16675 which is an AP1000 technical report that has been separately submitted to the Nuclear Regulatory Commission.

8. Added a section 7.2 reference to WCAP-16097-P-A, Rev. 0. The new reference is the latest Nuclear Regulatory Commission accepted version. The Common Q Platform was accepted by the Nuclear Regulatory Commission in ML003740165 (Reference 6), ML011690170 (Reference 7), and ML0305507760 (Reference 8).

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Table 1.6-1 (Sheet 12 of 20)

MATERIAL REFERENCED

DCD Section Number	Westinghouse Topical Report Number	Title
7.1		
	[*WCAP-14605 (P)* *WCAP-14606*	*Westinghouse Setpoint Methodology for Protection Systems - AP600, April 1996*]*
	WCAP-15775	AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, Revision 2, March 2003
	[*WCAP-16096-P-A*	*Software Program Manual for Common Q Systems, Revision 01A, January 2004*]*
	[*WCAP-16097-P-A* *WCAP-16097-NP-A*	*Common Qualified Platform, Revision 01, May 2003*]*
	WCAP-15776	Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002
	WCAP-16361-P WCAP-16361-NP	Westinghouse Setpoint Methodology for Protection Systems – AP1000, May 2006
	WCAP-16675-P WCAP-16675-NP	AP1000 Protection and Safety Monitoring System Architecture Technical Report, February 2007
7.2	WCAP-16438-P WCAP-16438-NP	FMEA of AP1000 Protection and Safety Monitoring System, Revision 1, June 2006
	WCAP-16592-P WCAP-16592-NP	Software Hazards Analysis of AP1000 Protection and Safety Monitoring System, Revision 0, June 2006
	WCAP-15776	Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002

Deleted: WCAP-13382 (P) WCAP-13391

Deleted: AP600 Instrumentation and Control Hardware Description, May 1992

Deleted: [*WCAP-13383*

Deleted: *AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report, Revision 1, June 1996*]*

Deleted: WCAP-14080 (P) WCAP-14081

Deleted: AP600 Instrumentation and Control Software Architecture and Operation Description, June 1994

Deleted: *CE-CES-195*

Deleted: *May 2000*

Deleted: *2000*

Deleted: *CENPD-396-P (P)*

Deleted: [*WCAP-15927*

Deleted: *Design Process for AP1000 Common Q Safety Systems, August 2002*]*

	WCAP-16097-P-A WCAP-16097-NP-A	Common Qualified Platform, Digital Plant Protection System, Appendix 3, May 2003
7.3	WCAP-15776	Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002

Section 7.1.2.14.2 is revised to delete the reference to AP600/Eagle specific document WCAP-13383 and to update the Common Qualified Platform Topical Report from CENPD-396-P to WCAP-16097-P-A

7.1.2.14.2 Commercial Dedication

[*WCAP-16097-P-A (Reference 8) provides for the use of commercial off-the-shelf hardware and software through a commercial dedication process.*]* Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant as described in subsection 13.5.1.

Deleted: *13383 (Reference 3) and CENPD-396-P*

The last sentence of section 7.1.3 is revised to correctly describe the Figure 7.1-1.

Figure 7.1-1 provides an illustration of the instrumentation and control architecture for the AP1000 and the plant control system.

Deleted: 0

Section 7.1.7 is revised to correct Reference 20.

7.1.7 References

20. NABU-DP-00014-GEN, Rev. 1 (Proprietary), "Design Process for Common Q Safety Systems," March 2006.

Deleted: NAMB

II.3 ELIMINATION OF CONTROL ROOM MULTIPLEXER

Section 3.1.3 and section 7.7.1.11 are revised to eliminate text that described the way Eagle product line interfaces to control board switch. Is does not apply to Common Q and is extraneous to these sections.

This change does not affect conformance to regulatory requirements and guidance.

Section 3.1.3 has been revised as follows:

3.1.3 Protection and Reactivity Control Systems

Criterion 20 – Protection System Functions

The protection system shall be designed (1) to initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

AP1000 Compliance

The protection system is a microprocessor-based system that trips the reactor and actuates engineered safety features when predetermined limits are exceeded or when manually initiated.

The reactor trip portion of the protection system includes four independent, redundant, physically separated, electrically-isolated divisions. The coincidence circuits guard against the loss of protection or the generation of false protection signals due to equipment failures through the use of a two-out-of-four logic and built-in operational bypasses.

Independent, redundant, physically separated, electrically-isolated engineered safety features trains are provided. Signal conditioning for the plant sensors is provided.

Deleted: Control and status signals are transmitted between the protection system and the main control room and the remote shutdown workstation by electrical data links and between the distributed logic circuits by internally redundant fiber optic data highways.

See Chapter 7 for additional information concerning the design of the protection system.

Section 7.7.1.11 has been revised as follows:

Manual Actuation Function

*[The manual actuation function of the diverse actuation system is implemented by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the protection and safety monitoring system cabinets, and the diverse actuation system automatic logic.]**

Deleted: *the control room multiplexers,*

II.7 LOW REACTOR COOLANT FLOW REACTOR TRIP LOGIC MODIFICATIONS

See Rev 16 change section II.7 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

7.2.1.1.3 Core Heat Removal Trips

Reactor Trip on Low Reactor Coolant Flow

This trip protects against departure from nucleate boiling in the event of low reactor coolant flow. Flow in each hot leg is measured at the hot leg elbow. The trip on low flow in the hot legs is automatically blocked when reactor power is below the P-10 permissive setpoint. This enhances reliability by preventing unnecessary reactor trips. The trip function is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 5 shows the logic for this trip. The development of permissive P-10 is shown in Figure 7.2-1, sheet 4.

Deleted: s

Deleted: and P-8 are

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Table 15.0-4a (Sheet 1 of 2)

PROTECTION AND SAFETY MONITORING SYSTEM SETPOINTS AND TIME DELAY ASSUMED IN ACCIDENT ANALYSES

Function	Limiting Setpoint Assumed in Analyses	Time Delays (seconds)
Reactor trip on power range high neutron flux, high setting	118%	0.9
Reactor trip on power range high neutron flux, low setting	35%	0.9
Reactor trip on source range neutron flux reactor trip	Not applicable	0.9
Overtemperature ΔT	Variable (see Figure 15.0.3-1)	2.0
Overpower ΔT	Variable (see Figure 15.0.3-1)	2.0
Reactor trip on high pressurizer pressure	2460 psia	2.0
Reactor trip on low pressurizer pressure	1800 psia	2.0
Reactor trip on low reactor coolant flow in either hot leg	87% loop flow	1.45
Reactor trip on reactor coolant pump under speed	90%	0.767
Reactor trip on low steam generator narrow range level	95,000 lbm	2.0
High-2 steam generator level	100% of narrow range level span	2.0 (reactor trip) 0.0 (turbine trip) 2.0 (feedwater isolation)
Reactor trip on high-3 pressurizer water level	76% of span	2.0
PRHR actuation on low steam generator wide range level	55,000 lbm	2.0
"S" signal and steamline isolation on low T_{cold}	500°F	2.0
"S" signal and steamline isolation on low steamline pressure	405 psia (with an adverse environment assumed) 535 psia (without an adverse environment assumed)	2.0
"S" signal on low pressurizer pressure	1700 psia	2.0

Deleted: High neutron flux, P-... [27]

Table 15.0-6 (Sheet 3 of 4)

PLANT SYSTEMS AND EQUIPMENT AVAILABLE FOR TRANSIENT AND ACCIDENT CONDITIONS

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 15.4 (Cont.)			
Uncontrolled RCCA bank withdrawal at power	Power range high neutron flux, high power range positive neutron flux rate, overtemperature ΔT, over-power ΔT, high pressurizer pressure, high pressurizer water level, manual	–	Pressurizer safety valves, steam generator safety valves
RCCA misalignment	Overtemperature ΔT, manual	–	–
Startup of an inactive reactor coolant pump at an incorrect temperature	Power range high flux, low flow (P-10 interlock), manual	–	–
Chemical and volume control system malfunction that results in a decrease in boron concentration in the reactor coolant	Source range high flux, overtemperature ΔT, manual	Source range flux doubling	Low insertion limit annunciators
Spectrum of RCCA ejection accidents	Power range high flux, high positive flux rate, manual	–	Pressurizer safety valves
Section 15.5			
Increase in reactor coolant inventory			
Inadvertent operation of the ECCS during power operation	High pressurizer pressure, manual, "safeguards" trip, high pressurizer level	High pressurizer level, low T_{cold}	Core makeup tank, pressurizer safety valves, chemical and volume control system isolation, PRHR
Chemical and volume control system malfunction that increases reactor coolant inventory	High pressurizer pressure, "safeguards" trip, high pressurizer level, manual	High pressurizer level, low T_{cold}	Core makeup tank, pressurizer safety valves, chemical and volume control system isolation, PRHR

Deleted: 8

II.8 OVERTEMPERATURE/OVERPOWER ΔT REACTOR TRIP MODIFICATIONS

See Revision 16 change section II.8 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

Bases section B.2.1

SAFETY LIMITS

The figure provided in the COLR shows the loci of points of THERMAL POWER, RCS pressure, and cold temperature for which the minimum DNBR is not less than the safety analysis limit, that fuel centerline temperature remains below melting, that the average enthalpy in the hot leg is less than or equal to the enthalpy of saturated liquid, or that the exit quality is within the limits defined by the DNBR correlation.

Deleted: average

The reactor core SLs are established to preclude violation of the following fuel design criteria:

a. There must be at least a 95% probability at a 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience DNB and

b. There must be at least a 95% probability at a 95% confidence level that the hot fuel pellet in the core does not experience centerline fuel melting.

The reactor core SLs are used to define the various RPS functions such that the above criteria are satisfied during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs). To ensure that the RPS precludes the violation of the above criteria, additional criteria are applied to the Overtemperature and Overpower ΔT reactor trip functions. That is, it must be demonstrated that the average enthalpy in the hot leg is less than or equal to the saturation enthalpy and the core exit quality is within the limits defined by the DNBR correlation. Appropriate functioning of the RPS ensures that for variations in the THERMAL POWER, RCS Pressure, RCS cold leg temperature, RCS flow rate, and ΔI that the reactor core SLs will be satisfied during steady state operation, normal operational transients, and AOOs.

Deleted: average

II.9 FLUX DOUBLING/BORON DILUTION MODIFICATIONS

See Revision 16 change section II.9 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

Table 7.3-2 (Sheet 1 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Derivation	Function
P-6	Intermediate range neutron flux channels above setpoint	None
P-6	Intermediate range neutron flux channels below setpoint	Prevents manual block of flux doubling actuation, permitting block of boron dilution

Deleted: Allows manual block of flux doubling actuation of the boron dilution block.

DCD Figure 9.3.6-1 Sheet Revisions

Sheet 1, Note 8 – Change text to read "...High 1 Pressurizer Level, High-High Radiation, or Flux Doubling Signal"

Sheet 2, Note 3 – Add text "Pumps Stop on receipt of Flux Doubling Signal" to existing note.

Sheet 2, Note 8 – Remove text "A Source Range Flux Doubling Signal" from the existing note.

DCD Subsection 9.3.6.3.7 Revision

Makeup Line Containment Isolation Valves

These normally open, motor-operated globe valves provide containment isolation of the chemical and volume control system makeup line and automatically close on a high-2 pressurizer level, high steam generator level, or high-2 containment radiation signal from the protection and safety monitoring system. The valves close on a source range flux doubling signal to terminate possible unplanned boron dilution events. The valves also close on a safeguards actuation signal coincident with high-1 pressurizer level. This allows the chemical and volume control system to continue providing reactor coolant system makeup flow, if the makeup pumps are operating following a safeguards actuation signal. These valves are also controlled by the reactor makeup control system and close when makeup to other systems is provided. Manual control is provided in the main control room and at the remote shutdown workstation.

9.3.6.4.5.1 Boron Dilution Events

The chemical and volume control system is designed to address a boron dilution accident by closing redundant safety-related valves, tripping the makeup pumps and/or aligning the suction of the makeup pumps to the boric acid tank.

Deleted: either one of two

Deleted: , air-operated

Deleted: valves

Deleted: from the demineralized water system to the makeup pump suction

For dilution events occurring at power (assuming the operator takes no action), a reactor trip is initiated on either an overpower trip or an overtemperature ΔT trip. Following a reactor trip signal, the line from the demineralized water system is isolated by closing two safety-related, air-operated valves. The three-way pump suction control valve aligns so the makeup pumps take suction from the boric acid tank. If the event occurs while the makeup pumps are operating, the realignment of these valves causes the makeup pumps, if they continue to operate, to borate the plant.

Deleted: remotely

Deleted: When

Deleted: trip

For dilution events during shutdown, the source range flux doubling signal is used to isolate the makeup line to the reactor coolant system by closing the two safety related, motor operated valves, isolate the line from the demineralized water system by closing the two safety-related, air-operated valves and trip the makeup pumps. For refueling operations, administrative controls are used to prevent boron dilutions by verifying the valves in the line from the demineralized water system are closed and secured.

Deleted: remotely

Deleted: The three-way pump suction control valve aligns the makeup pumps to take suction from the boric acid tank and therefore stops the dilution.

9.3.6.6.1.2 Flow Testing

Each chemical and volume control system pump is tested to measure the flow rate from each makeup pump to the reactor coolant system. Testing will be performed with the pump suction aligned to the boric acid tank and the discharge aligned to the reactor coolant system. Testing will also be performed with the pump suction aligned to the boric acid tank and the discharge aligned to the pressurizer auxiliary spray. Flow will be measured using instrumentation in the pump discharge line. Testing will confirm that each pump provides at least 100 gallons per minute of makeup flow at normal reactor coolant system operating pressure. This is the minimum flow rate necessary to meet the chemical and volume control system functional requirement of providing makeup and pressurizer spray to support the functions described in subsection 9.3.6.4.4.1. Testing is performed to verify that the maximum makeup flow with both pumps operating is less than 175 gpm, as assumed in the boron dilution analyses presented in subsection 15.4.6. Testing is performed with both pumps operating and taking suction from the demineralized water system. The chemical and volume control system is aligned to the reactor coolant system at a pressure at or near atmospheric pressure.

Deleted: 200

DCD Subsection 9.3.6.7 Revisions

- **Demineralized water system isolation valves** – To prevent inadvertent boron dilution, the demineralized water system isolation valves close on a signal from the protection and safety monitoring system derived from either a reactor trip signal, a source range flux doubling signal, low input voltage (loss of ac power) to the 1E dc and uninterruptible power supply system battery chargers, or a safety injection signal providing a safety-related method of stopping an inadvertent dilution. The main control room and remote shutdown workstation provide manual control for these valves.

Deleted: a

Deleted: uninterruptable

- **Makeup isolation valves** – To isolate the makeup flow to the reactor coolant system, two valves are provided in the chemical and volume control system makeup line. These valves automatically close on a signal from the protection and safety monitoring system derived from, source range flux doubling, high-2 pressurizer level, high steam generator level, or a safeguards signal coincident with high-1 pressurizer level to protect against pressurizer or steam generator overfill. Manual control for these valves is provided in the main control room and at the remote shutdown workstation. In addition, the valves close on a high-2 containment radiation signal to protect containment integrity.

Deleted: either

Deleted: a

Deleted: signal

Table 14.3-2 **DESIGN BASIS ACCIDENT ANALYSIS**		
Reference	**Design Feature**	**Value**
Section 7.3.1.2.14	The demineralized water system isolation valves close on a signal from the protection and safety monitoring system derived from either a reactor trip signal, a source range flux doubling signal, or low input voltage to the 1E dc uninterruptible power supply battery chargers.	
Section 7.3.1.2.15	The chemical and volume control system makeup line isolation valves automatically close on a signal from the protection and monitoring system derived from a source range flux doubling, high-2 pressurizer level, high-2 steam generator level signal, a safeguards signal coincident with high-1 pressurizer level, or high-2 containment radioactivity.	
Section 9.3.6.7	The chemical and volume control system makeup line isolation valves automatically close on a signal from the protecttion and safety monitoring system derived from a source range flux doubling, high-2 pressurizer level, high steam generator level signal, or a safeguards signal coincident with high-1 pressurizer level.	

Deleted: and

Deleted: either

Deleted: either

Table 19.59-18 (Sheet 23 of 24)

AP1000 PRA-BASED INSIGHTS

Insight	Disposition
70. One CVS pump is configured to operate on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically.	9.3.6.3.1 & 19.15
On a source range flux doubling signal, the PMS automatically closes two safety-related CVS makeup line isolation valves, closes two safety-related CVS demineralized water suction valves to the makeup pumps and trips the makeup pumps. On a reactor trip or low input voltage to the Class 1E dc power system battery chargers, the PMS closes the two safety-related CVS demineralized water suction valves to the makeup pumps and aligns the makeup pump suction to the boric acid tank.	7.3.1.2.14

Deleted: The safety-related PMS boron dilution signal automatically re-aligns CVS pump suction to the boric acid tank. This signal also closes the two safety-related CVS demineralized water supply valves. This signal actuates on reactor trip signal (interlock P-4), source range flux doubling signal, or low input voltage to the Class 1E dc power system battery chargers.

BASES

APPLICABLE SAFETY ANALYSES, LCOs and APPLICABILITY (continued)

15. Boron Dilution Block

The block of boron dilution is accomplished by closing the CVS suction valves to demineralized water storage tanks, and aligning the boric acid tank to the CVS makeup pumps. This Function is actuated by Source Range Neutron Flux Doubling, Reactor Trip, and Battery Charger Input Voltage – Low.

Deleted: Multiplication

15.a. Source Range Neutron Flux Doubling

Deleted: Multiplication

A signal to block boron dilution in MODES 2 or 3, when not critical or during an intentional approach to criticality, and MODES 4, or 5 is derived from source range neutron flow increasing at an excessive rate (source range flux doubling). This Function is not applicable in MODES 4 and 5 if the demineralized water makeup flowpath is isolated. The source range neutron detectors are used for this Function. The LCO requires four divisions to be OPERABLE. There are four divisions and two-out-of-four logic is used. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, demineralized water is isolated from the makeup pumps and reactor coolant makeup is isolated from the reactor coolant system to preclude a boron dilution event. In MODE 6, a dilution event is precluded by the requirement in LCO 3.9.2 to close, lock and secure at least one valve in each unborated water source flow path

Deleted: below the P-6 interlock

Deleted: 3,

Deleted: flow multiplication

Deleted: flow

Deleted: makeup

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.12 REMOVAL OF LOW-2 RCS HOT LEG SIGNAL FROM IRWST INJECTION LOGIC.

See Revision 16 change section II.12 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

Table 7.3-1 (Sheet 8 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves (Figure 7.2-1, Sheets 12 and 16)			
a. Automatic reactor coolant system depressurization (fourth stage)	(See items 3d and 3e)		
b. Manual initiation	4 controls	2/4 controls[3]	None

Deleted: b. Coincident loop 1 and loop 2 Low-2 hot leg level (after delay)

Deleted: 1 per loop

Deleted: 2/2

Deleted: Manual unblock permitted below P-12 . Automatically blocked above P-12

Deleted: c

Table 7.3-2 (Sheet 3 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Derivation	Function
P-12	Pressurizer level below setpoint	(d) Coincident with manual action of (a), automatically unblocks fourth stage automatic depressurization system initiation on low hot leg level to provide protection during mid-loop operation
$\overline{\text{P-12}}$	Pressurizer level above setpoint	(e) Automatically blocks fourth stage automatic depressurization system initiation on low hot leg level to reduce the probability of spurious actuation

Deleted: in-containment refueling water storage tank injection and

Deleted: in-containment refueling water storage tank injection and

II.13 CREATION OF NEW PERMISSIVE P-3 FOR SAFEGUARDS ACTUATION BLOCK

See Revision 16 change section II.13 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

This change requires modifications to Section B 3.3.2, as shown below.

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

18. ESFAS Interlocks

To allow some flexibility in unit operations, several interlocks are included as part of the ESFAS. These interlocks permit the operator to block some signals, automatically enable other signals, prevent some actions from occurring, and cause other actions to occur. The interlock Functions backup manual actions to ensure bypassable Functions are in operation under the conditions assumed in the safety analyses.

18.a. Reactor Trip, P-4

There are eight reactor trip breakers with two breakers in each division. The P-4 interlock is enabled when the breakers in two-out-of-four divisions are open. Additionally, the

P-4 interlock is enabled by all Automatic Reactor Trip Actuations. The Functions of the P-4 interlock are:

- Trip the main turbine
-
- Block boron dilution

Deleted: Permit the block of automatic Safeguards Actuation after a predetermined time interval following automatic Safeguards Actuation.

18 f. Reactor Trip Breaker Open, P-3

Permit the block of automatic Safeguards Actuation after a predetermined time interval following automatic Safeguards Actuation

BASES

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY (continued)

The reactor trip breaker position switches that provide input to the P-3 interlock only Function to energize or de-energize or open or close contacts. Therefore, this Function has no adjustable Trip Setpoint.

BASES

ACTIONS (continued)

D.1

With one required division inoperable, the affected division must be restored to OPERABLE status within 6 hours.

Condition D applies to one inoperable required division of the P-3 & P-4 Interlocks (Function 18.f and 18.a). With one required division inoperable, the 2 remaining OPERABLE divisions are capable of providing the required interlock function, but without a single failure. The P-3 & P-4 Interlock is enabled when RTBs in two divisions are detected as open. The status of the other inoperable, non-required P-3 & P-4 division is not significant, since P-3 & P-4 divisions can not be tripped or bypassed. In order to provide single failure tolerance, 3 required divisions must be OPERABLE.

Deleted: a

II.14 ADDITION OF DELAY TIMERS FOR ENABLING THE SOURCE RANGE REACTOR TRIP AND FLUX DOUBLING SIGNAL

See Revision 16 change section II.14 for description and justification for change

This change does not affect conformance to regulatory requirements and guidance.

7.2.1.1.1 Nuclear Startup Trips

Source Range High Neutron Flux Trip

Source range high neutron flux trips the reactor when two of the four source range channels exceed the trip setpoint. This trip provides protection during reactor startup and plant shutdown. This function is delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious trip due to the short term instability of the processed source range values. This trip function may be manually blocked and the high voltage source range detector power supply de-energized when the intermediate range neutron flux is above the P-6 setpoint value. It is automatically blocked by the power range neutron flux interlock (P-10). The trip may be manually reset when neutron flux is between P-6 and P-10. The reset occurs automatically when the intermediate range flux decreases below P-6. The channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

Deleted: It

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.15 RT/ESF ACCURACIES AND RESPONSE TIMES CORRECTIONS

See Revision 16 change section II.15 for description and justification for change.

This change does not affect conformance to regulatory requirements and guidance.

Table 7.3-4 (Sheet 2 of 2)

ENGINEERED SAFETY FEATURES ACTUATION, VARIABLES, LIMITS, RANGES, AND ACCURACIES (NOMINAL)

Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Pressurizer water level	0 to 100% of cylindrical portion of pressurizer	± 10% of span	1.0
Startup feedwater flow	0 to 1000 gpm	±7% of span	1.0
Neutron flux (flux doubling calculation)	1 to 10^6 c/sec	± 30% of span	1.0(3)
Control room supply air radiation level	10^{-12} to 10^{-2} μ Ci/cc	± 50% of setpoint	20
Containment radioactivity	10^0 to 10^7 R/hr	± 50% of setpoint	20

Deleted: s to be Monitored

II.28 EDITORIAL CHANGES

These changes do not affect conformance to regulatory requirements and guidance.

Correction to the description of MSHIM operation

Westinghouse is reevaluating the MSHIM operating strategy to emphasize base load operations and to support a reduction of effluent production during boron concentration changes to account for fuel burnup. DCD sections 4.3.4.2.16 and 7.7.1.1 are affected by this change. Revise subsection of 4.3.2.4.16 as shown:

4.3.2.4.16 Load Follow Control and Xenon Control

During load follow maneuvers, power changes are primarily accomplished using control rod motion alone, as required. Control rod motion is limited by the control rod insertion limits as provided in the technical specifications and discussed in subsections 4.3.2.4.12 and 4.3.2.4.13. The power distribution is maintained within acceptable limits through limitations on control rod insertion. Reactivity changes due to the changing xenon concentration are also controlled by rod motion.

Rapid power increases (five percent/min) from part power during load follow operation are accomplished with rod motion.

The rod control system is designed to automatically provide the power and temperature control described above 30 percent rated power for most of the cycle length without the need to change boron concentration as a result of the load maneuver. The automated mode of operation is referred to as mechanical shim (MSHIM) because of the usage of mechanical means to control reactivity and power distribution simultaneously. MSHIM operation allows load maneuvering without boron change because of the degree of allowed insertion of the control banks in conjunction with the independent power distribution control of the axial offset (AO) control bank. The worth and overlap of the MA, MB, MC, MD, M1, and M2 control banks are designed such that the AO control bank insertion will always result in a monotonically decreasing axial offset. MSHIM operation uses the MA, MB, MC, MD, M1, and M2 control banks to maintain the programmed coolant average temperature throughout the operating power range. The AO control bank is independently modulated by the rod control system to maintain a nearly constant axial offset throughout the operating power range. The degree of control rod insertion under MSHIM operation allows rapid return to power without the need to change boron concentration.

The target axial offset used during MSHIM load follow operation is roughly the base load operation target axial offset less 10 percent. The negative bias is necessary to allow both positive and negative axial offset control effectiveness by the AO control bank. Extended base load operation is performed by controlling axial offset to the equilibrium target with the first moving M bank nearly fully withdrawn (at bite position) and AO bank fully withdrawn. The "bite" position is defined as the minimum control rod bank position required to provide a differential rod worth of at least 2 pcm/step.

Deleted: Anticipated MSHIM load follow operation operates with two gray banks fully inserted to provide enough reactivity worth to compensate for transient reactivity effects without the need for soluble boron changes. The degree of control rod insertion under MSHIM operation allows rapid return to power without the need to change boron concentration.¶

Revise the fourth paragraph of section 7.7.1.1 as shown:

The reactor power control system uses a different control strategy for the rods used to regulate core power (M banks) from the control strategy used to regulate axial offset (AO bank). Reactor coolant system boron concentration is adjusted by the operator to account for long-term core burnup. The adjustment also maintains the M banks and the AO bank in a position suitable for the current mode of operation (load follow or base load operation). During load follow or load regulation response transients, the power control and the axial offset control subsystems jointly function to control both core power and axial offset. The following two subsections provide a description of each control subsystem.

Deleted: two gray

Deleted: both black M banks (M1 and M2) in a near fully withdrawn position, the first two moving gray M banks fully inserted, and the AO bank slightly inserted

Correction to the description of the steam dump control system

Unlike the auctioneered high T_{avg} signal used in the rod control system, the steam dump T_{avg} signal does not provide additional operating margin under normal conditions. The steam dump signal is actuated only by large and rapid power reduction events (e.g., load rejection), which, by their nature (core power reducers), cause core margin increases. Hence, there is no advantage to using a high auctioneered T_{AVG} in the steam dump controller. A previously designed signal selector will be used instead. The first bullet of the third paragraph of Section 7.7.1.9 will be revised as shown:

- The T_{avg} mode uses the difference between a signal selected loop T_{avg} and a reference temperature derived from turbine first-stage impulse pressure, to generate a steam dump demand signal. This mode is largely used for at-power transients requiring steam dump, such as load rejections and turbine trips (where the load rejection T_{avg} mode is used) and reactor trips (where the plant trip T_{avg} mode is used). The load rejection controller is discussed in subsection 7.7.1.9.1. The plant trip controller is discussed in subsection 7.7.1.9.2.

Deleted: measured auctioneered

Correction to the description of the rapid power reduction rod selection

DCD section 7.7.1.10.2 implies that the control system will determine and then select the rods to be dropped during a rapid power reduction event. In the current design, BEACON will periodically determine if the rods to drop should be changed to improve system performance. BEACON is not qualified to interact directly with the plant control system, so any needed changes would be offered to the operator for evaluation. Following concurrence, the operator will make the necessary changes in the rod control logic cabinet. The first paragraph of Section 7.7.1.10.2 will be revised as shown:

7.7.1.10.2 Rapid Power Reduction Rod Selection

The number of rods needed to obtain this power reduction is dependent on the core burnup during the fuel cycle. In addition, if a large load rejection (grid disconnect) is initiated at a part-power condition (50-percent to 100-percent power), then a reduced number of control rods need to be released. Therefore, a means is provided to alter which rods will be released by the rapid power reduction system. Following concurrence, the operator uses a control room workstation to implement the suggested changes in the rod control logic cabinet.

Deleted: have the control system select

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Correction to table 7.3-1 (Sheet 1 of 9)

Revision 16 to the DCD inadvertently removed permissive P-11 from table 7.3-1. P-11 has been put back into table 7.3-1 as shown below.

Table 7.3-1 (Sheet 1 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Channels/ Switches	Actuation Logic	Permissives and Interlocks
1. Safeguards Actuation Signal (Figure 7.2-1, Sheets 9 and 11)			
a. Low pressurizer pressure	4	2/4-BYP[1]	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
b. Low lead-lag compensated steam line pressure	4/steam line	2/4-BYP[1] in either steam line	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
c. Low reactor coolant inlet temperature (Low T_{cold})	4/loop	2/4-BYP[1] either loop[6]	Manual block permitted below P-11 Automatically unblocked above P-11 Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
d. High-2 containment pressure	4	2/4-BYP[1]	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
e. Manual safeguards initiation	2 switches	1/2 switches	None

Correction to Sections 7.1, 7.2, and 7.3 due to figure deletions

Section 7.1.1 revised as follows:

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network. To meet cyber security concerns, the real-time data highway will be separated into security levels as described in Reference 22.

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the right is the protection and safety monitoring system. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

Deleted: left

Section 7.1.3 revised as follows:

7.1.3 Plant Control System

The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The plant control system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The plant control system also provides control of the nonsafety-related decay heat removal systems during shutdown. The plant control system accomplishes these functions through use of the following:

- Rod control
- Pressurizer pressure and level control
- Steam generator water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The plant control system provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The plant control system acts to maximize margins to plant safety limits and maximize the plant transient performance. The plant control system also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance.

The plant control system includes the equipment from the process sensor input circuitry through to the modulating and nonmodulating control outputs as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Nonmodulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The plant control system cabinets contain the process sensor inputs and the modulating and nonmodulating outputs. The plant control system also includes equipment to monitor and control the control rods.

The functions of the plant control system are performed by system assemblies including:

- Distributed controllers
- Signal selector algorithms
- Operator controls and indication
- Real-time data network
- Rod control system
- Rod position indication
- Rod drive motor-generator sets

Deleted: Figure 7.1-10 provides an illustration of the plant control system.¶

Section 7.2.1 revised as follows:

7.2.1 Description

Considerations, such as mechanical or hydraulic limitations on equipment or heat transfer requirements on the reactor core, define a safe operating region for the plant. Maneuvering of the plant within this safe operating region is permitted in response to normal power generation demands. The plant design provides margin to the safety limits so that an unsafe condition is not caused by the transients induced by normal operating changes. The plant control system attempts to keep the reactor operating away from any safety limit. Excursions toward a limit occur because of abnormal demands, malfunctions in the control system, or by severe transients induced by occurrence of a Condition II or III event, as discussed in Chapter 15. Hypothetical events (Condition IV) are analyzed with respect to plant safety limits. The safety system keeps the reactor within the safe region by shutting down the reactor whenever safety limits are approached. Reactor trip is a protective function performed by the protection and safety monitoring system when it anticipates an approach of a parameter to its safety limit. Reactor shutdown occurs when electrical power is removed from the rod drive mechanism coils, allowing the rods to fall by gravity into the reactor core.

Section 7.1 provides a description of the reactor trip equipment. The equipment involved is:

Deleted: The equipment involved in reactor trip is shown in simplified block diagram form in Figure 7.1-2.

- Sensors and manual inputs
- Protection and safety monitoring system cabinets
- Reactor trip switchgear

Section 7.3.1 revised as follows:

7.3.1 Description

The protection and safety monitoring system is actuated when safety system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary ruptures. Once the required logic combination is generated, the protection and safety monitoring system equipment sends the signals to actuate appropriate engineered safety features components.

Deleted: A block diagram of the protection and safety monitoring system is provided in Figure 7.1-2.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Update of Table 7.5-1

Revision 16 of the DCD corrected the pressure range on steam line pressure on table 7.3-4. The range was increased to 1300 psig. Table 7.5-1 (Sheet 2 of 12) was inadvertently missed as part of the correction. Table 7.5-1 has been corrected to reflect the same information as 7.3-4. The table is revised as follows:

Table 7.5-1 (Sheet 2 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Core exit temperature	200-2300°F	B1, C1, F2	Harsh	Yes	3/quadrant	1E	Yes	
PRHR HX inlet temperature	50-650°F	D3	None	None	1	Non-1E	No	Primary indication is RCS T_H
PRHR HX outlet temperature	50-500°F	B1, D2	Harsh	Yes	1	1E	Yes	Diverse variable to PRHR flow
PRHR flow	700-3000 gpm	B1, D2, F2	Harsh	Yes	2	1E	Yes	Diverse measurement: PRHR outlet temperature
IRWST water level	0-100% of span	B1, D2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
RCS subcooling (Note 6)	200°F Sub-cooling to 35°F super heat	B1, F2	Harsh	Yes	2	1E	Yes	Diverse measurement: Core exit temperature & wide range RCS pressure
Passive containment cooling water flow	0-150 gpm	B1, D2	Mild	Yes	1 (Note 1)	1E	Yes	
PCS storage tank water level	5-100% of tank height	B1, D2	Mild	Yes	2	1E	Yes	Diverse measurement: PCS flow
IRWST surface temperature	50-300°F	D3	None	None	1	Non-1E	No	
IRWST bottom temperature	50-300°F	D3	None	None	1	Non-1E	No	
Steam line pressure	0-1300 psig	F2	Harsh/ Mild (Note 8)	Yes	1/steam generator (Note 11)	1E	No	

Deleted: 1200

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.31 CORRECTION TO CMT LEVEL INSTRUMENT RANGE

DCD table 7.5-1 needs to be revised to match TR 123. Specifically sheet 7 of 12 the narrow range CMT level, upper and lower, range/span column.

This change does not affect conformance to regulatory requirements and guidance.

Table 7.5-1 (sheet 7 of 12) will be revised as shown:

Table 7.5-1 (Sheet 7 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Water-cooled chiller status	On/Off	F3	None	None	1/chiller	Non-1E	No	
Water-cooled chilled water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Water-cooled chilled water valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Spent fuel pool pump flow	0-1500 gpm	F3	None	None	1/pump	Non-1E	No	
Spent fuel pool temperature	50-250°F	F3	None	None	1	Non-1E	No	
Spent fuel pool water level	0-100% of span	D2, F3	Mild	Yes	3 (Note 4)	1E	Yes	
CMT discharge isolation valve status	Open/ Closed	D2	Harsh	No	1/valve	Non-1E	No	
CMT inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT upper water level sensor	74.5% - 64% of span	D2, F2	Harsh	Yes	1/tank	1E	Yes	
CMT lower water level sensor	27% - 17% of span	D2, F2	Harsh	Yes	1/tank	1E	Yes	
IRWST injection isolation valve (Squib)	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
IRWST line isolation valve status (MOV)	Open/ Closed	D3	None	None	1/valve	Non-1E	No	
ADS: first, second and third stage valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	

Deleted: 78.0

Deleted: 63.5

Deleted: 30.5

Deleted: 16

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.32 INSTRUMENTATION AND CONTROL DESIGN CHANGE

This section contains changes in the instrumentation and control that affect chapter 7 of the DCD that are described in APP-GW-GLN-004 (TR-39).

This change does not affect conformance to regulatory requirements and guidance.

Revise the first paragraph of subsection 7.3.1.2.17 as shown below and as described in APP-GW-GLN-004 (TR-39).

7.3.1.2.17 Control Room Isolation and Air Supply Initiation

Signals to initiate isolation of the main control room, to initiate the air supply, and to open the control room pressure relief isolation valves are generated from either of the following conditions:

1. High-2 control room air supply radioactivity level
2. Loss of ac power sources (low Class 1E battery charger input voltage)
3. Manual initiation

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

Revise the table 7.3-1

Revise the table 7.3-1 as shown below and as described in APP-GW-GLN-004 (TR-39).

Add note 8 to item 13.b.

Table 7.3-1 (Sheet 6 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	**No. of Divisions/ Controls**	**Actuation Logic**	**Permissives and Interlocks**
f. High-3 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-19 Automatically unblocked above P-19
13. Block of Boron Dilution (Figure 7.2-1, Sheets 3 and 15)			
a. Flux doubling calculation	4	2/4-BYP[1]	Manual block permitted above P-6 Automatically unblocked below P-6
b. Undervoltage to Class 1E battery chargers[(8)]	2/charger	2/2 per charger and 2/4 chargers[5]	None
c. Reactor trip (P-4)	1/division	2/4	None

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

II.33 POST-ACCIDENT MONITORING SYSTEM TABLE CHANGES

This section contains changes in the post-accident monitoring system table in chapter 7 of the DCD that have been identified in APP-GW-GEE-054 and APP-GW-GLN-110. The variables should also be listed in the summary of type variable table.

This change does not affect conformance to regulatory requirements and guidance.

The MCR pressure relief isolation valve is an ESF actuated valve. All valves actuated by ESF must be monitored by PAMS. Therefore, the MCR pressure relief isolation valve must be added to table 7.5-1.

Table 7.5-1 has been modified as follows:

Table 7.5-1 (Sheet 10 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
IRWST to RNS suction valve status	Open/ Closed	B1, F3	Harsh	Yes	1 (Note 7)	1E	Yes	
RNS discharge to IRWST valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
RNS pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Reactor vessel head vent valve status	Open/ Closed	D2	Harsh	Yes	1/valve Note 7)	1E	Yes	
MCR return air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR toilet exhaust isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR supply air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR differential pressure	-1" to +1" wg	D2	Mild	Yes	2	1E	Yes	
MCR air delivery flowrate	0-80 cfm	D2	Mild	Yes	2	1E	Yes	
MCR pressure relief isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve	1E	Yes	

Table 7.5-7 has been modified as follows:

Table 7.5-7 (Sheet 4 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Type/Category
Containment Cooling	Containment temperature	D2
	PCS water storage tank series isolation valve status (MOV)	D2
	PCS water storage tank isolation valve status (non-MOV)	D2
	Passive containment cooling water flow	D2
	PCS storage tank water level	D2
HVAC System Status	MCR return air isolation valve status	D2
	MCR toilet exhaust isolation valve status	D2
	MCR supply air isolation valve status	D2
	MCR air delivery isolation valve status	D2
	MCR pressure relief isolation valve status	D2
	MCR air storage bottle pressure	D2
	MCR differential pressure	D2
	MCR air delivery flowrate	D2
Main Steam	Turbine stop valve status	D2
	Turbine control valve status	D2
	Condenser steam dump valve status	D2

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

TR-110 identifies a variable to be added, the RCS sampling line isolation valve status. This particular variable is already listed in table 7.5-7 as primary sampling.

Table 7.5-1 has been modified as follows:

Table 7.5-1 (Sheet 9 of 12)

POST-ACCIDENT MONITORING SYSTEM

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Purification return line stop valve status	Open/ Closed	D2	Harsh	None	1	Non-1E	No	
Boric acid tank level	0-100%	F3	None	None	1	Non-1E	No	
Demineralized water isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Boric acid flow	0-175 gpm	F3	None	None	1	Non-1E	No	
Makeup blend valve status	Position	F3	None	None	1	Non-1E	No	
Makeup flow	0-175 gpm	F3	None	None	1	Non-1E	No	
Makeup pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Makeup flow control valve status	Position	F3	None	None	1	Non-1E	No	
Letdown flow	0-120 gpm	F3	None	None	1	Non-1E	No	
RNS hot leg suction isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
RNS flow	0-3000 gpm	F3	None	None	1/pump	Non-1E	No	
RCS sampling line isolation valve status	Open/ Closed	E3	Harsh	None	1/valve	Non-1E	No	

III. REGULATORY IMPACT

A. FSER IMPACT

Modifications have been made to Tier 1 Sections 2.5.1 and 2.5.2 and Tier 2 Table 1-1, Chapter 3, Chapter 4, Chapter 7, Chapter 9, Chapter 14, Chapter 15, Chapter 16 (Technical Specifications and Bases) and Chapter 19 in order to refine and better illustrate the approach taken in the AP1000 design. The corresponding FSER sections will be affected.

B. SCREENING QUESTIONS (Check correct response and provide justification for that determination under each response)

1. Does the proposed change involve a change to an SSC that adversely affects a DCD described design function? ☐ YES ☒ NO

   The changes included in this document include DCD changes to correct descriptions and figures in the DCD and changes due to completion of elements of the design process of the PMS. Many of the changes correct the depiction of the logic and do not impact PMS functionality. The functions identified as new or added are a result of implementing the requirements phase of the design process.

2. Does the proposed change involve a change to a procedure that adversely affects how DCD described SSC design functions are performed or controlled? ☐ YES ☒ NO

3. Does the proposed activity involve revising or replacing a DCD described evaluation methodology that is used in establishing the design bases or used in the safety analyses? ☐ YES ☒ NO

4. Does the proposed activity involve a test or experiment not described in the DCD, where an SSC is utilized or controlled in a manner that is outside the reference bounds of the design for that SSC or is inconsistent with analyses or descriptions in the DCD? ☐ YES ☒ NO

   The subject changes do not require that the RCS or connected systems be operated outside their design parameters. Requirements for startup testing are not altered by the subject changes.

Document Number: APP-GW-GLR-080 **Revision Number:** 0
Title: Mark-up of AP1000 Design Control Document Chapter 7

C. EVALUATION OF DEPARTURE FROM TIER 2 INFORMATION (Check correct response and provide justification for that determination under each response)

10 CFR Part 52, Appendix D, Section VIII. B.5.a. provides that an applicant for a combined licensee who references the AP1000 design certification may depart from Tier 2 information, without prior NRC approval, if it does not require a license amendment under paragraph B.5.b. The questions below address the criteria of B.5.b.

1. Does the proposed departure result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce a new failure mode in components that would result in an accident previously evaluated.	
2. Does the proposed departure result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety and previously evaluated in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce a new failure mode in equipment relied upon to prevent or mitigate design basis accidents. The performance and response to postulated accident conditions of equipment in the reactor coolant system and connecting systems is not changed.	
3. Does the proposed departure result in more than a minimal increase in the consequences of an accident previously evaluated in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce the possibility of a change in the consequences of an accident. The subject changes do not change the response of the reactor coolant system and engineered safeguard systems to postulated accident conditions.	
4. Does the proposed departure result in more than a minimal increase in the consequences of a malfunction of an SSC important to safety previously evaluated in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce the possibility of a change in the consequences of a malfunction because the subject changes do will not cause components in the reactor coolant system to malfunction and result in a larger release to the environment. The subject changes have no adverse effect on systems and components used to mitigate the consequences of postulated accidents.	
5. Does the proposed departure create a possibility for an accident of a different type than any evaluated previously in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce the possibility of a new accident because the subject changes do not introduce a new failure mode in systems that provide fission product barriers and mitigate postulated accidents. The subject changes do not change the manner in which the operator controls the plant or responds to transients or accident conditions.	
6. Does the proposed departure create a possibility for a malfunction of an SSC important to safety with a different result than any evaluated previously in the plant-specific DCD?	☐ YES ☒ NO
The subject changes do not introduce the possibility for a malfunction of an SSC with a different result because the subject changes do not change the operation or function of systems and components and does not	

introduce a new failure mode in systems and components.	
7. Does the proposed departure result in a design basis limit for a fission product barrier as described in the plant-specific DCD being exceeded or altered?	☐ YES ☒ NO
The subject changes do not result in a change that would cause fuel or system parameters to change. The subject changes do not change the response of the reactor coolant system and engineered safeguard systems to postulated accident conditions. Therefore, the subject changes do does not result in a design basis limit for a fission product barrier as described in the DCD being exceeded or altered.	
8. Does the proposed departure result in a departure from a method of evaluation described in the plant-specific DCD used in establishing the design bases or in the safety analyses?	☐ YES ☒ NO
The methods used to evaluate the subject changes do not constitute a departure from a method of evaluation described in the DCD. Standard versions of the previously approved methodologies, all of which are described in the DCD, were used to support the conclusions drawn in this evaluation.	
☒ The answers to the evaluation questions above are "NO" and the proposed departure from Tier 2 does not require prior NRC review to be included in plant specific FSARs as provided in 10 CFR Part 52, Appendix D, Section VIII. B.5.b ☐ One or more of the answers to the evaluation questions above are "YES" and the proposed change requires NRC review.	

D. IMPACT ON RESOLUTION OF A SEVERE ACCIDENT ISSUE

10 CFR Part 52, Appendix D, Section VIII. B.5.a. provides that an applicant for a combined licensee who references the AP1000 design certification may depart from Tier 2 information, without prior NRC approval, if it does not require a license amendment under paragraph B.5.c. The questions below address the criteria of B.5.c.

1. Is there is a substantial increase in the probability of a severe accident such that a particular severe accident previously reviewed and determined to be not credible could become credible?	☐ YES ☒ NO
The changes have no effect on the operation, performance, and pressure boundary integrity of the reactor coolant system and connected systems. Therefore, there is no effect on the calculation of the probability of a severe accident.	
2. Is there is a substantial increase in the consequences to the public of a particular severe accident previously reviewed?	☐ YES ☒ NO
The changes have no effect on the operation, performance, and pressure boundary integrity of the primary pressure boundary. Therefore, there is no effect on the calculation of the release of radioactive material during a severe accident.	
☒ The answers to the evaluation questions above are "NO" and the proposed departure from Tier 2 does not require prior NRC review to be included in plant specific FSARs as provided in 10 CFR Part 52, Appendix D, Section VIII. B.5.c ☐ One or more of the he answers to the evaluation questions above are "YES" and the proposed change requires	

NRC review.

E. SECURITY ASSESSMENT

1. Does the proposed change have an adverse impact on the security assessment of the AP1000. ☐ YES ☒ NO

The changes will not alter barriers or alarms that control access to protected areas of the plant. The changes will not alter requirements for security personnel.

F. REFERENCES

1. APP-GW-GLR-018, "Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System," June 2006.
2. APP-GW-GLR-024, "AP1000 Setpoint Calculations for Protective Functions," May 2006.
3. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC Items," May 2006.
4. APP-GW-GLN-004, "Instrumentation and Control Design Change," May 2006.
5. APP-GW-GLN-022, AP1000 Standard Combined License Technical Report, "DAS Platform Technology and Remote Indication Change," April 2007.
6. APP-GW-GLN-110, AP1000 Standard Combined License Technical Report, "Changes to AP1000 Design Control Document (DCD) Chapter 3.11 – Environmental Qualification of Mechanical and Electrical Equipment and Chapter 3 Appendix 3D – Methodology for Qualifying AP1000 Safety Related Electrical and Mechanical Equipment," April 2007.
7. APP-GW-GLN-123, "Core Makeup Tank Narrow Level Instrumentation Change," June 2007.
8. ML003740165, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 1 (TAC No. MA1677)," August 11, 2000.
9. ML011690170, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE CES 195, Rev. 01 (TAC No. MB0780)," June 22, 2001.
10. ML0305507760, "Acceptance of the Changes to Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Closeout of Category 2 Open Items (TAC No. MB2553)," February 24, 2003.
11. ML042730580, "Final Safety Evaluation for Topical Report WCAP-16096-NP-A, Revision 1, 'Software Program Manual for Common Q Systems' (TAC No. MC2294)," September 28, 2004.
12. WCAP 16675 P, Revision 0 (Proprietary), "Protection and Monitoring System Architecture Topical Report," December 2006.