Chapter 7

Instrumentation and Control

CONTENTS

Section	Title	Page
7.1	INTRODUCTION	7.1-1
7.1.1	DEFINITIONS	7.1-1
7.1.2	IDENTIFICATION OF SAFETY-RELATED SYSTEMS	7.1-4
7.1.3	IDENTIFICATION OF SAFETY CRITERIA	7.1-5
7.1.3.1	Design Bases	7.1-5
7.1.3.2	Independence of Redundant Safety-Related Systems	7.1-5
7.1.3.3	Physical Identification of Safety-Related Equipment	7.1-6
7.1.3.4	Conformance with IEEE Standards	7.1-7
7.1.4	REFERENCES	7.1-8
7.2	REACTOR TRIP SYSTEM	7.2-1
7.2.1	DESIGN BASES	7.2-1
7.2.1.1	General Design Criterion 2, 1967 – Performance Standards	7.2-1
7.2.1.2	General Design Criterion 11, 1967 – Control Room	7.2-1
7.2.1.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.2-1
7.2.1.4	General Design Criterion 14, 1967 – Core Protection Systems	7.2-1
7.2.1.5	General Design Criterion 19, 1967 – Protection Systems Reliability	7.2-2
7.2.1.6	General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence	7.2-2
7.2.1.7	General Design Criterion 21, 1967 – Single Failure Definition	7.2-2
7.2.1.8	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.2-2
7.2.1.9	General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems	7.2-2
7.2.1.10	General Design Criterion 24, 1967 – Emergency Power for Protection Systems	7.2-2
7.2.1.11	General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems	7.2-3
7.2.1.12	General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design	7.2-3
7.2.1.13	General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction	7.2-3
7.2.1.14	General Design Criterion 49, 1967 – Containment Design Basis	7.2-3

CONTENTS

Section	Title	Page
7.2.1.15	Reactor Trip System Safety Function Requirements	7.2-3
7.2.1.16	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.2-4
7.2.1.17	Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions	7.2-4
7.2.1.18	NUREG-0737 (Items II.K.3.10 and II.K.3.12), November 1980 – Clarification of TMI Action Plan Requirements	7.2-4
7.2.1.19	Generic Letter 83-28 (Actions 4.3 and 4.5), July 1983 – Required Actions Based on Generic Implications of Salem ATWS Events	7.2-4
7.2.2	SYSTEM DESCRIPTION	7.2-5
7.2.2.1	Reactor Trips	7.2-5
7.2.2.2	Reactor Trip System Interlocks	7.2-15
7.2.2.3	Coolant Temperature Sensor Arrangement and Calculational Methodology	7.2-16
7.2.2.4	Pressurizer Water Level Reference Leg Arrangement	7.2-19
7.2.2.5	Process Protection System	7.2-19
7.2.2.6	Solid State (Digital) Logic Protection	7.2-19
7.2.2.7	Reactor Trip Breakers	7.2-20
7.2.2.8	Isolation Devices	7.2-20
7.2.2.9	Energy Supply and Environmental Qualification Requirements	7.2-20
7.2.2.10	Reactor Trip System Instrumentation Trip Setpoints	7.2-20
7.2.2.11	Specific Control and Protection Interactions	7.2-21
7.2.2.12	Tests and Inspections	7.2-26
7.2.2.13	Current System Drawings	7.2-27
7.2.3	SAFETY EVALUATION	7.2-27
7.2.3.1	General Design Criterion 2, 1967 – Performance Standards	7.2-27
7.2.3.2	General Design Criterion 11, 1967 – Control Room	7.2-29
7.2.3.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.2-29
7.2.3.4	General Design Criterion 14, 1967 – Core Protection Systems	7.2-30
7.2.3.5	General Design Criterion 19, 1967 – Protection Systems Reliability	7.2-31
7.2.3.6	General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence	7.2-31
7.2.3.7	General Design Criterion 21, 1967 – Single Failure Definition	7.2-33
7.2.3.8	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.2-34

CONTENTS

Section	Title	Page
7.2.3.9	General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems	7.2-35
7.2.3.10	General Design Criterion 24, 1967 – Emergency Power for Protection Systems	7.2-35
7.2.3.11	General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems	7.2-35
7.2.3.12	General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design	7.2-37
7.2.3.13	General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction	7.2-37
7.2.3.14	General Design Criterion 49, 1967 – Containment Design Basis	7.2-38
7.2.3.15	Reactor Trip System Safety Function Requirements	7.2-38
7.2.3.16	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.2.38
7.2.3.17	Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions	7.2-39
7.2.3.18	NUREG-0737 (Items II.K.3.10 and II.K.3.12), November 1980 – Clarification of TMI Action Plan Requirements	7.2-40
7.2.3.19	Generic Letter 83-28 (Actions 4.3 and 4.5), July 1983 – Required Actions Based on Generic Implications of Salem ATWS Events	7.2-40
7.2.4	COMPLIANCE WITH IEEE STANDARDS	7.2-39
7.2.4.1	Compliance with IEEE 279-1971	7.2-39
7.2.4.2	Compliance with IEEE 317-1971	7.2-50
7.2.4.3	Evaluation of Compliance with IEEE 344-1971	7.2-50
7.2.4.4	Evaluation of Compliance with IEEE 603-1980	7.2-50
7.2.4.5	Evaluation of Compliance with ANSI/IEEE-ANS-7-4.3.2-1982	7.2-50
7.2.5	REFERENCES	7.2-50
7.2.6	REFERENCE DRAWINGS	7.2-53
7.3	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM	7.3-1
7.3.1	DESIGN BASES	7.3-1
7.3.1.1	General Design Criteria 2, 1967 – Performance Standards	7.3-1
7.3.1.2	General Design Criterion 11, 1967 – Control Room	7.3-1
7.3.1.3	General Design Criterion 15, 1967 – Engineered Safety Features Protection Systems	7.3-1

CONTENTS

Section	Title	Page
7.3.1.4	General Design Criterion 19, 1967 – Protection Systems Reliability	7.3-1
7.3.1.5	General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence	7.3-1
7.3.1.6	General Design Criterion 21, 1967 – Single Failure Criterion	7.3-2
7.3.1.7	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.3-2
7.3.1.8	General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems	7.3-2
7.3.1.9	General Design Criterion 24, 1967 – Emergency Power for Protection Systems	7.3-2
7.3.1.10	General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems	7.3-2
7.3.1.11	General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design	7.3-2
7.3.1.12	General Design Criterion 37, 1967 – Engineered Safety Features Basis for Design	7.3-2
7.3.1.13	General Design Criterion 38, 1967 – Reliability and Testability of Engineered Safety Features	7.3-3
7.3.1.14	General Design Criterion 40, 1967 – Missile Protection	7.3-3
7.3.1.15	General Design Criterion 48, 1967 – Testing of Operational Sequence of Emergency Core Cooling Systems	7.3-3
7.3.1.16	General Design Criterion 49, 1967 – Containment Design Basis	7.3-3
7.3.1.17	Engineered Safety Features Actuation System Safety Function Requirements	7.3-3
7.3.1.18	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.3-3
7.3.1.19	Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions	7.3-3
7.3.2	SYSTEM DESCRIPTION	7.3-4
7.3.2.1	Functional Design	7.3-4
7.3.2.2	Signal Computation	7.3-5
7.3.2.3	Devices Requiring Actuation	7.3-5
7.3.2.4	Implementation of Functional Design	7.3-6
7.3.2.5	Additional Design Information	7.3-9
7.3.2.6	Current System Drawings	7.3-10
7.3.3	SAFETY EVALUATION	7.3-10
7.3.3.1	General Design Criteria 2, 1967 – Performance Standards	7.3-10

CONTENTS

Section	Title	Page
7.3.3.2	General Design Criterion 11, 1967 – Control Room	7.3-10
7.3.3.3	General Design Criterion 15, 1967 – Engineered Safety Features Protection Systems	7.3-11
7.3.3.4	General Design Criterion 19, 1967 – Protection Systems Reliability	7.3-12
7.3.3.5	General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence	7.3-13
7.3.3.6	General Design Criterion 21, 1967 – Single Failure Criterion	7.3-13
7.3.3.7	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.3-14
7.3.3.8	General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems	7.3-14
7.3.3.9	General Design Criterion 24, 1967 – Emergency Power for Protection Systems	7.3-15
7.3.3.10	General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems	7.3-15
7.3.3.11	General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design	7.3-15
7.3.3.12	General Design Criterion 37, 1967 – Engineered Safety Features Basis for Design	7.3-16
7.3.3.13	General Design Criterion 38, 1967 – Reliability and Testability of Engineered Safety Features	7.3-16
7.3.3.14	General Design Criterion 40, 1967 – Missile Protection	7.3-16
7.3.3.15	General Design Criterion 48, 1967 – Testing of Operational Sequence of Emergency Core Cooling Systems	7.3-16
7.3.3.16	General Design Criterion 49, 1967 – Containment Design Basis	7.3-17
7.3.3.17	Engineered Safety Features Actuation System Safety Function Requirements	7.3-17
7.3.3.18	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.3-17
7.3.3.19	Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions	7.3-17
7.3.4	COMPLIANCE WITH IEEE STANDARDS	7.3-18
7.3.4.1	Evaluation of Compliance with IEEE-279, 1971 – Criteria For Protection Systems for Nuclear Power Generating Stations	7.3-18
7.3.4.2	Evaluation of Compliance with IEEE-308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations	7.3-25

CONTENTS

Section	Title	Page
7.3.4.3	Evaluation of Compliance with IEEE-323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations	7.3-26
7.3.4.4	Evaluation of Compliance with IEEE-338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems	7.3-26
7.3.4.5	Evaluation of Compliance with IEEE-344-1971, Trial-Use Guide for Seismic Qualifications of Class I Electric Equipment for Nuclear Power Generating Stations	7.3-26
7.3.4.6	Evaluation of Compliance with IEEE-317-1971, Electric Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations	7.3-27
7.3.4.7	Evaluation of Compliance with IEEE-336-1971, Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations	7.3-27
7.3.4.8	Eagle 21 and Process Control System Design, Verification and Validation	7.3-27
7.3.5	REFERENCES	7.3-27
7.3.6	REFERENCE DRAWINGS	7.3-32
7.4	SYSTEMS REQUIRED FOR SAFE SHUTDOWN	7.4-1
7.4.1	DESIGN BASES	7.4-1
7.4.1.1	General Design Criterion 3, 1971 – Fire Protection	7.4-1
7.4.1.2	General Design Criterion 11, 1967 – Control Room	7.4-1
7.4.1.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.4-1
7.4.1.4	Safe Shutdown Systems Safety Function Requirements	7.4-2
7.4.2	DESCRIPTION	7.4-2
7.4.2.1	Safe Shutdown Equipment	7.4-3
7.4.2.2	Equipment, Services, and Approximate Time Required After Incident that Requires Hot Shutdown (MODE 4)	7.4-11
7.4.2.3	Equipment and Systems Available for Cold Shutdown (MODE 5)	7.4-11
7.4.3	SAFETY EVALUATION	7.4-12
7.4.3.1	General Design Criterion 3, 1971 – Fire Protection	7.4-12

CONTENTS

Section	Title	Page
7.4.3.2	General Design Criterion 11, 1967 – Control Room	7.4-12
7.4.3.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.4-13
7.4.3.4	Safe Shutdown Systems Safety Function Requirements	7.4-14
7.4.4	REFERENCES	7.4-14
7.4.5	REFERENCE DRAWINGS	7.4-18
7.5	SAFETY-RELATED DISPLAY INSTRUMENTATION	7.5-1
7.5.1	DESIGN BASES	7.5-1
7.5.1.1	General Design Criterion 2, 1967 – Performance Standards	7.5-1
7.5.1.2	General Design Criterion 11, 1967 – Control Room	7.5-1
7.5.1.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.5-1
7.5.1.4	General Design Criterion 17, 1967 – Monitoring Radioactivity Releases	7.5-1
7.5.1.5	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.5-1
7.5.1.6	Regulatory Guide 1.97, Revision 3, May 1983 – Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident	7.5-1
7.5.1.7	NUREG-0737 (Items I.D.2, II.D.3, II.E.1.2, II.F.1, II.F.2, and III.A.1.2), November 1980 – Clarification of TMI Action Plan Requirements	7.5-2
7.5.2	DESCRIPTION	7.5-2
7.5.2.1	Post-Accident Reactor Coolant Pressure and Containment Monitors	7.5-3
7.5.2.2	Instrumentation for Detection of Inadequate Core Cooling	7.5-4
7.5.2.3	Plant Vent Post-Accident Radiation Monitors	7.5-7
7.5.2.4	ALARA Monitors for Post-Accident Monitor Access	7.5-8
7.5.2.5	Radioactive Gas Decay Tank Pressure	7.5-8
7.5.2.6	Auxiliary Feedwater Flow Indication	7.5-8
7.5.2.7	Dedicated Shutdown Panel	7.5-8
7.5.2.8	Pressurizer Safety Valve Position Indication System and Power Operated Relief Valve Position Indication	7.5-9
7.5.2.9	Emergency Response Facility Data System	7.5-10
7.5.2.10	Safety Parameter Display System	7.5-13

CONTENTS

Section	Title	Page
7.5.3	SAFETY EVALUATION	7.5-14
7.5.3.1	General Design Criterion 2, 1967 – Performance Standards	7.5-14
7.5.3.2	General Design Criterion 11, 1967 – Control Room	7.5-14
7.5.3.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.5-16
7.5.3.4	General Design Criterion 17, 1967 – Monitoring Radioactivity Releases	7.5-16
7.5.3.5	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.5-16
7.5.3.6	Regulatory Guide 1.97, Revision 3, May 1983 – Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident	7.5-17
7.5.3.7	NUREG-0737 (Items I.D.2, II.D.3, II.E.1.2, II.F.1, II.F.2, and III.A.1.2), November 1980 – Clarification of TMI Action Plan Requirements	7.5-19
7.5.4	REFERENCES	7.5-22
7.5.5	REFERENCE DRAWINGS	7.5-26
7.6	ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY	7.6-1
7.6.1	DESIGN BASES	7.6-1
7.6.1.1	General Design Criterion 2, 1967 – Performance Standards	7.6-1
7.6.1.2	General Design Criterion 11, 1967 – Control Room	7.6-1
7.6.1.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.6-1
7.6.1.4	Other Instrumentation Systems Safety Function Requirements	7.6-1
7.6.1.5	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.6-2
7.6.1.6	10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients Without Scrams (ATWS) Events for Light-Water-Cooled Nuclear Power Plants	7.6-2
7.6.2	DESCRIPTION	7.6-2
7.6.2.1	Residual Heat Removal Isolation Valves	7.6-2
7.6.2.2	Pipe Break Isolation System	7.6-3
7.6.2.3	ATWS Mitigation System Actuation Circuitry (AMSAC)	7.6-4
7.6.3	SAFETY EVALUATION	7.6-4

CONTENTS

Section	Title	Page
7.6.3.1	General Design Criterion 2, 1967 – Performance Standards	7.6-4
7.6.3.2	General Design Criterion 11, 1967 – Control Room	7.6-5
7.6.3.3	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.6-6
7.6.3.4	Other Instrumentation Systems Safety Function Requirements	7.6-7
7.6.3.5	10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	7.6-7
7.6.3.6	10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients Without Scrams (ATWS) Events for Light-Water-Cooled Nuclear Power Plants	7.6-8
7.6.4	REFERENCES	7.6-8
7.6.5	REFERENCE DRAWINGS	7.6-12
7.7	CONTROL SYSTEMS NOT REQUIRED FOR SAFETY	7.7-1
7.7.1	DESIGN BASES	7.7-1
7.7.1.1	General Design Criterion 11, 1967 – Control Room	7.7-1
7.7.1.2	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.7-1
7.7.1.3	General Design Criterion 13, 1967 – Fission Process Monitors and Controls	7.7-1
7.7.1.4	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.7-1
7.7.1.5	General Design Criterion 26, 1967 –Reactivity Control System Redundancy and Capability	7.7-2
7.7.1.6	General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction	7.7-2
7.7.2	SYSTEM DESCRIPTION	7.7-2
7.7.2.1	Reactor Control System	7.7-4
7.7.2.2	Rod Control System	7.7-5
7.7.2.3	Plant Control Signals for Monitoring and Indicating	7.7-7
7.7.2.4	Plant Control System Interlocks	7.7-11
7.7.2.5	Pressurizer Pressure Control	7.7-13
7.7.2.6	Pressurizer Water Level Control	7.7-13
7.7.2.7	Steam Generator Water Level Control	7.7-14
7.7.2.8	Steam Dump Control	7.7-15
7.7.2.9	Incore Instrumentation	7.7-16
7.7.2.10	Control Locations	7.7-19

CONTENTS

Section	Title	Page
7.7.3	SAFETY EVALUATION	7.7-26
7.7.3.1	General Design Criterion 11, 1967 – Control Room	7.7-26
7.7.3.2	General Design Criterion 12, 1967 – Instrumentation and Control Systems	7.7-26
7.7.3.3	General Design Criterion 13, 1967 – Fission Process Monitors and Controls	7.7-29
7.7.3.4	General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems	7.7-29
7.7.3.5	General Design Criterion 26, 1971 –Reactivity Control System Redundancy and Capability	7.7-30
7.7.3.6	General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction	7.7-33
7.7.4	REFERENCES	7.7-33
7.7.5	REFERENCE DRAWINGS	7.7-34

Chapter 7

TABLES

Table	Title
7.1-1	Applicable Design Basis Criteria
7.2-1	List of Reactor Trips
7.2-2	Protection System Interlocks
7.2-3	Deleted in Revision 22
7.3-1	Instrumentation Operating Condition for Engineered Safety Features
7.3-2	Engineered Safety Features Actuation System Instrumentation Operating Conditions for Isolation Functions
7.3-3	Interlocks for Engineered Safety Features Actuation System
7.5-1	Main Control Board Indicators and/or Recorders Available to the Operator (Conditions II and III Events)
7.5-2	Main Control Board Indicators and/or Recorders Available to the Operator (Condition IV Events)
7.5-3	Control Room Indicators and/or Recorders Available to the Operator to Monitor Significant Plant Parameters During Normal Operation
7.5-4	Postaccident Monitoring Panel Indicators and/or Recorders Available to the Operator
7.5-5	Information Required on the Subcooled Margin Monitors (SCMMs)
7.5-6	Summary of Compliance with Regulatory Guide 1.97, Rev. 3
7.7-1	Plant Control System Interlocks
7.7-2	Deleted in Revision 14

FIGURES

Figure	Title
7.2-1[a]	Instrumentation and Control System Logic Diagrams
7.2-2	Setpoint Reduction Function for Overpower and Overtemperature ΔT Trips
7.2-3	Deleted.
7.2-4	Pressurizer Sealed Reference Leg Level System
7.2-5	Design to Achieve Isolation Between Channels
7.2-6	Seismic Sensor Locations (2 Sheets)
7.2-7	Deleted in Revision 8 (Reassigned as Figure 7.2-1, Sheets 35 and 36)
7.3-1[a]	Logic Diagram Symbols
7.3-2[a]	Logic Diagram - Reactor Coolant Pump
7.3-3[a]	Logic Diagram - Reciprocating Charging Pump
7.3-4[a]	Logic Diagram - Centrifugal Charging Pumps
7.3-5[a]	Logic Diagram - Auxiliary Saltwater Pumps
7.3-6[a]	Logic Diagram - Containment Fan Coolers
7.3-7[a]	Logic Diagram - Component Cooling Water Pumps
7.3-8[a]	Logic Diagram - Auxiliary Feedwater Pumps
7.3-9[a]	Logic Diagram - Residual Heat Removal Pumps
7.3-10[a]	Logic Diagram - Safety Injection Pumps
7.3-11[a]	Logic Diagram - Containment Spray Pumps
7.3-12[a]	Logic Diagram - Primary Makeup Water Pumps
7.3-13[a]	Logic Diagram - Boric Acid Transfer Pumps

FIGURES (Continued)

Figure	Title
7.3-14[a]	Schematic Diagram - Auxiliary Feedwater Motor-Operated Valves
7.3-15[a]	Schematic Diagram - Turbine Control
7.3-16[a]	Schematic Diagram - Feedwater Pump Turbine Control
7.3-17[a]	Schematic Diagram - Motor-Driven Auxiliary Feedwater Pumps
7.3-18[a]	Schematic Diagram - Auxiliary Feedwater Pumps Turbine Control
7.3-19[a]	Schematic Diagram - Main Feedwater Isolation Valves
7.3-20[a]	Schematic Diagram - Reactor Coolant Pump
7.3-21[a]	Schematic Diagram - Reactor Coolant Motor-Operated Valves and Reactor Coolant System Solenoid Valves
7.3-22[a]	Schematic Diagram - Safety Injection System Solenoid Valves
7.3-23[a]	Schematic Diagram - Safety Injection Pumps
7.3-24[a]	Schematic Diagram - Containment Spray Pumps
7.3-25[a]	Schematic Diagram - Residual Heat Removal Pumps
7.3-26[a]	Schematic Diagram - Residual Heat Removal Flow Control Valves
7.3-27[a]	Schematic Diagram - Component Cooling Water Pumps
7.3-28[a]	Schematic Diagram - Auxiliary Saltwater Pumps
7.3-29[a]	Schematic Diagram - Charging Pumps
7.3-30[a]	Schematic Diagram - Chemical and Volume Control System
7.3-31[a]	Schematic Diagram - Containment Fan Coolers
7.3-32[a]	Schematic Diagram - Containment Spray System Motor-Operated Valves
7.3-33[a]	Schematic Diagram - Safety Injection System Motor-Operated Valves

FIGURES (Continued)

Figure	Title
7.3-34[a]	Schematic Diagram - Chemical and Volume Control System Motor-Operated Valves
7.3-35[a]	Schematic Diagram - Component Cooling Water System Motor-Operated Valves
7.3-36[a]	Schematic Diagram - Reactor Trip Breakers
7.3-37[a]	Schematic Diagram - Fire Pumps
7.3-38[a]	Schematic Diagram - Containment Purge System
7.3-39[a]	Schematic Diagram - Plant Air Compressors
7.3-40[a]	Schematic Diagram - Control Rod Drive Motor Generator Set
7.3-41[a]	Schematic Diagram - Diesel Fuel Transfer Pumps
7.3-42[a]	Schematic Diagram - Main Steam Isolation Valves
7.3-43[a]	Schematic Diagram - Sampling System Solenoid Valves
7.3-44[a]	Schematic Diagram - Component Cooling Water Solenoid Valves
7.3-45[a]	Schematic Diagram - Chemical and Volume Control System Solenoid Valves
7.3-46[a]	Schematic Diagram - Liquid Radwaste Solenoid Valves
7.3-47[a]	Schematic Diagram - Steam Generator Blowdown Solenoid Valves
7.3-48[a]	Schematic Diagram - Generator Control
7.3-49[a]	Schematic Diagram - Permissive and Bypass Lights
7.3-50[a]	Separation and Color Code Instrumentation and Control – Engineered Safety Features
7.3-51	Deleted in Revision 11
7.3-52[a]	Containment Electrical Penetrations, Cable Trays, and Supports

FIGURES (Continued)

Figure	Title
7.5-1	Containment Water Level Indication
7.5-1A	Deleted in Revision 8
7.5-1B	Unit 2 Containment Water Level Wide-Range Indication with Installed Spare Wide-Range Level Transmitter in Service
7.5-2	Reactor Vessel Level Instrumentation Process Connection Schematic (Train A)
7.6-1[(a)]	Instrumentation and Control Power Supply
7.6-2	Deleted in Revision 8 (Reassigned as Figure 7.2-1, Sheets 33 and 34)
7.7-1	Simplified Block Diagram of Reactor Control System
7.7-2	Control Bank Rod Insertion Monitor
7.7-3	Rod Deviation Comparator
7.7-4	Block Diagram of Pressurizer Pressure Control System
7.7-5	Block Diagram of Pressurizer Level Control System
7.7-6[(a)]	Functional Logic Diagram, Digital Feedwater Control System, FW Flow Controller & Cv Demand
7.7-7[(a)]	Functional Logic Diagram, Digital Feedwater Control System, Feedwater Control & Isolation
7.7-8	Block Diagram of Steam Dump Control System
7.7-9	Basic Flux Mapping System
7.7-10	Deleted in Revision 14
7.7-11	Deleted in Revision 14
7.7-12	Deleted in Revision 14
7.7-13	Deleted in Revision 14

FIGURES (Continued)

Figure	Title
7.7-14	Deleted in Revision 15
7.7-15	Deleted in Revision 15
7.7-16[a]	Arrangement of Control Room
7.7-17[a]	Location of Control Console and Main Control Board
7.7-18[a]	Arrangement of Control Console Nuclear Instrumentation System (CC1), Primary Plant Control (CC2), and Secondary Plant Control (CC3) - Unit 1
7.7-19[a]	Arrangement of Control Console Nuclear Instrumentation System (CC1), Primary Plant Control (CC2), and Secondary Plant Control (CC3) - Unit 2
7.7-20[a]	Arrangement of Main Control Board - Engineered Safety Systems (VB1) - Unit 1
7.7-21[a]	Arrangement of Main Control Board - Engineered Safety Systems (VB1) - Unit 2
7.7.22[a]	Arrangement of Main Control Board - Primary Plant Systems (VB2) – Unit 1
7.7.23[a]	Arrangement of Main Control Board - Primary Plant Systems (VB2) – Unit 2
7.7.24[a]	Arrangement of Main Control Board - Steam and Turbine (VB3) - Unit 1
7.7.25[a]	Arrangement of Main Control Board - Steam and Turbine (VB3) - Unit 2
7.7.26[a]	Arrangement of Main Control Board - Auxiliary Equipment and Diesel (VB4) - Unit 1
7.7.27[a]	Arrangement of Main Control Board - Auxiliary Equipment and Diesel (VB4) - Unit 2
7.7.28[a]	Arrangement of Main Control Board - Station Electric (VB5) - Unit 1
7.7.29[a]	Arrangement of Main Control Board - Station Electric (VB5) - Unit 2
7.7-30[a]	Arrangement of Hot Shutdown Remote Control Panel

FIGURES (Continued)

Figure	Title
7.7-31[a]	Arrangement of Auxiliary Building Control Panel

NOTE:

[a] This figure corresponds to a controlled engineering drawing that is incorporated by reference into the FSAR Update. See Table 1.6-1 for the correlation between the FSAR Update figure number and the corresponding controlled engineering drawing number.

Chapter 7

INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

This chapter presents the various plant instrumentation and control systems by relating the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter emphasizes those instruments and associated equipment that constitute the protection system as defined in IEEE 279-1971(Reference 1).

The primary purpose of the instrumentation and control systems is to provide automatic protection against unsafe and improper reactor operation during steady state and transient power operations (Conditions I, II, and III) and to provide initiating signals to mitigate the consequences of faulted conditions (Condition IV). For a discussion of the four conditions, refer to Chapter 15. The information presented in this chapter emphasizes those instrumentation and control systems necessary to ensure that the reactor can be operated to produce power in a manner that ensures no undue risk to the health and safety of the public.

It is shown that the applicable criteria and codes, such as the U.S. Atomic Energy Commission's (AECs) General Design Criteria (GDC) and IEEE standards, concerned with the safe generation of nuclear power are met by these systems. Table 7.1-1 provides a summary of the applicable design basis criteria for each section within Chapter 7.

The classification of instrumentation is described in Section 3.2.2.5.

7.1.1 DEFINITIONS

The definitions below establish the meaning of certain terms in the context of their use in Chapter 7.

(1) Actuation Accuracy - Synonymous with trip accuracy, but used where the word "trip" may cause ambiguity.

(2) Channel - An arrangement of components, modules and software as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single action signals are combined.

(3) Channel Accuracy (an element of trip accuracy) - Includes accuracy of the primary element, transmitter, and rack-mounted electronics, but does not include indication accuracy.

(4) Cold Shutdown Condition - When the reactor is subcritical by an amount greater than the margin specified in the applicable Technical Specification and Tavg is less than or equal to the temperature specified in the applicable Technical Specification. Section 15.1 defines this as MODE 5.

(5) Components - Items from which the system is assembled (such as resistors, capacitors, wires, connectors, transistors, tubes, switches, and springs).

(6) Degree of Redundancy - The difference between the number of channels monitoring a variable and the number of channels that, when tripped, will cause an automatic system trip.

(7) Hot Shutdown Condition - When the reactor is subcritical by an amount greater than the margin specified in the applicable Technical Specification and Tavg is within the temperature range specified in the applicable Technical Specification. Section 15.1 defines this as MODE 4.

(8) Hot Shutdown Panel – The hot shutdown panel, which is the alternate control location in the event that the main control room is rendered uninhabitable, is provided with a mode switch, control switch and status for each of the pumps required to bring the plant to a safe shutdown condition.

(9) Hot Standby Condition - When the reactor is subcritical by an amount greater than the margin specified in the Technical Specification and the Tavg is greater than or equal to the temperature specified in the applicable Technical Specification. Section 15.1 defines this as MODE 3.

(10) Indication Accuracy - The tolerance band containing the highest expected value of the difference between: (a) the value of a process variable read on an indicator or recorder, and (b) the actual value of that process variable. An indication must fall within this tolerance band. It includes channel accuracy, accuracy of readout devices, and rack environmental effects but not process effects such as fluid stratification.

(11) Minimum Degree of Redundancy - The degree of redundancy below which operation is prohibited or otherwise restricted by the Technical Specifications.

(12) Module - Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit. A module can be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

(13) Phase A Containment Isolation - Closure of all nonessential process lines that penetrate containment. Initiated by high containment pressure, pressurizer low pressure (LP), low steamline pressure, or manual actuation.

(14) Phase B Containment Isolation - Closure of remaining process lines. Initiated by containment high-high pressure signal (process lines do not include engineered safety features [ESFs] lines) or manual actuation.

(15) Protective Action - A protective action can be at the channel or the system level. A protective action at the channel level is the initiation of a signal by a single channel when the variable sensed exceeds a limit. A protective action at the system level is the initiation of the operation of a sufficient number of actuators to effect a protective function.

(16) Protective Function - A protective function is the sensing of one or more variables associated with a particular generating station condition, signal processing, and the initiation and completion of the protective action at values of the variable established in the design bases.

(17) Reproducibility - This term may be substituted for "accuracy" in the above definitions for those cases where a trip value or indicated value need not be referenced to an actual process variable value, but rather to a previously established trip or indication value; this value is determined by test.

(18) Safe Shutdown - This term is defined as hot standby (MODE 3). Refer to Table 3.9-9, Note (a) for additional Diablo Canyon Power Plant (DCPP) safe shutdown definitions.

(19) Single Failure - Any single event that results in a loss of function of a component or components of a system. Multiple failures resulting from a single event shall be treated as a single failure.

(20) Trip Accuracy - The tolerance band containing the highest expected value of the difference between (a) the desired trip point value of a process variable, and (b) the actual value at which a comparator trips (and thus actuates some desired result). This is the tolerance band within which a comparator must trip. It includes comparator accuracy, channel accuracy for each input, and environmental effects on the rack-mounted electronics. It comprises all instrumentation errors; however, it does not include any process effects such as fluid stratification.

(21) Type Tests - Tests made on one or more units to verify adequacy of design of that type of unit.

7.1.2 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

The instrumentation and control systems and supporting systems discussed in Chapter 7 that are required to function to achieve the system responses assumed in the safety evaluations, and those needed to shut down the plant safely are:

(1) Reactor trip system (RTS)

(2) Engineered safety features actuation system (ESFAS)

(3) Instrumentation and control power supply system (refer to Section 8.3.1.1.5)

(4) Remote shutdown panel controls and instrumentation

The RTS and the ESFAS are functionally defined systems. The functional descriptions of these systems are provided in Sections 7.2 and 7.3. The trip functions identified in Section 7.2, Reactor Trip System, are provided by the following:

(1) Process instrumentation and control system (References 3 and 10)

(2) Nuclear instrumentation system (NIS) (Reference 4)

(3) Solid-state logic protection system (Reference 5)

(4) Reactor trip switchgear (Reference 5)

(5) Manual actuation circuitry

The actuation functions identified in Section 7.3 are provided by the following:

(1) Process instrumentation and control system (References 3 and 10)

(2) Solid-state logic protection system (Reference 5)

(3) ESF test cabinet (Reference 6)

(4) Manual actuation circuitry

WCAP-7671 (Reference 3) describes the instrumentation and instruments systems that are safety-related as defined in the scope of IEEE 279-1971 (Reference 1).

The original Hagan/Westinghouse process control system (PCS) was replaced with a programmable logic controller (PLC) based system (DDP 1000000237 and 1000000501).

The PCS converts physical plant parameters such as temperature, pressure, level, and flow into electrical signals during normal operation. These signals are used for plant control, remote process indication, and computer monitoring. The PCS also provides signals to components located in the Hot Shutdown Panel. The PCS comprises Control Racks 17-32, panels PIA, PIB, PIC, and the Instrument Rack (RI Rack).

The sixteen Control Racks are divided into four Control Sets. Control Set I comprises Racks 17-20. Control Set II comprises Racks 21-24. Control Set III comprises Racks 25-27. Control Set IV comprises Racks 28-32. The Control Sets and the associated Class 1E 120-Vac power sources are physically separated. Each Control Set contains two sub-systems based on a PLC platform. One PLC sub-system contains PG&E Design Class I components and functions. The other PLC sub-system contains PG&E Design Class II components and functions. The two PLC sub-systems are separated within the Control Racks. The PG&E Design Class I sub-system in each Control Set receives Class 1E 120-Vac power from an independent Class 1E 120-Vac power source. The PG&E Design Class II sub-system in each Control Set receives non-Class 1E 120-Vac power from two separate sources; one of which is inverter backed. Circuit separation and isolation is maintained for Class 1E power sources to the Control Racks.

Instrument Panels PIA, PIB, and PIC are physically separated from each other and contain Class 1E power sources. These instrument panels receive 120-Vac power from Class 1E 120-Vac power supplies.

The RI Rack contains PG&E Design Class II related components and functions that are processed by a PLC. The RI Rack receives 120-Vac power from two non-Class 1E sources.

7.1.3 IDENTIFICATION OF SAFETY CRITERIA

7.1.3.1 Design Bases

The design bases and functional performance for the PG&E Design Class I systems described in this chapter are provided in Sections 7.2 (RTS), 7.3 (ESFAS), and 8.3.1.1.5 (Instrumentation and Control Power Supply System). Table 7.1-1 provides a summary of the applicable design basis criteria for each section within Chapter 7.

The design bases for the ESF are discussed in Chapter 6; specifically, Section 6.2 for containment systems and Section 6.3 for emergency core cooling system (ECCS).

7.1.3.2 Independence of Redundant Safety-Related Systems

Separation and independence for individual channels of the RTS and ESFAS are discussed in Sections 7.2 and 7.3, respectively. Separation of protection and control

systems is discussed in Section 7.7. Refer to Section 8.3 for a discussion of separation and independence of Class 1E electrical systems.

For separation requirements for control board wiring, refer to Section 7.7.

Separation criteria for circuits entering the containment structure are met by providing separate electrical penetrations as follows:

(1) *Reactor Protection Instrumentation* - Each of the Eagle 21 protection sets (I, II, III, and IV) utilizes one or more penetrations dedicated to that protection set.

(2) *Isolation Valves (solenoid-operated)* - Each isolation valve inside the containment structure is connected to its respective ESF dc bus, and circuits are run through associated 480-V bus penetrations. All isolation valves inside the containment structure receive train A signals. Redundant isolation valves outside the containment receive train B signals.

(3) *Isolation Valves (motor-operated)* - Each isolation valve utilizes a penetration dedicated to the 480-V ESF bus that provides power to the valve.

(4) *Fan Coolers* - One penetration for each fan cooler motor.

(5) *Nuclear Instrumentation (out-of-core)* - Four separate penetrations are provided for out-of-core nuclear instrumentation.

The installation of other cable complies with the criteria presented in Chapter 8.

7.1.3.3 Physical Identification of Safety-Related Equipment

There are four separate process protection system rack sets. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks to the redundant trains in the protection logic racks. Redundant process channels are separated by locating the electronics in different rack sets. A color-coded nameplate on each rack is used to differentiate between different protective sets. The color coding of the nameplates is:

Protection Set	Color Coding
I	Red with white lettering
II	White with black lettering
III	Blue with white lettering
IV	Yellow with black lettering

Each field wire termination point is tagged to assist identification. However, these tags are not color-coded.

All nonrack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure that houses them.

Post-accident monitoring instruments and controls are identified "PAMS" as required by Regulatory Guide 1.97, Revision 3.

For further details of the process protection system, refer to Sections 7.2, 7.3, and 7.7.

There are identification nameplates on the input panels of the logic system. For details of the logic system, refer to Sections 7.2 and 7.3.

7.1.3.4 Conformance with IEEE Standards

The PG&E Design Class I control and instrumentation systems comply with the following IEEE standards, only as discussed in the appropriate sections. However, because the IEEE standards were issued after much of the design and testing had been completed, the equipment documentation may not meet the format requirements of the standards.

(1) IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

(2) IEEE 308-1971, "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations."

(3) IEEE 317-1971, "IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations."

(4) IEEE 323-1971, "IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations."

(5) IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

(6) IEEE 334-1971, "Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations."

(7) IEEE 336-1971, "Installation, Inspection, and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations."

DCPP is in conformance with IEEE 336-1971, with the following exceptions:

Paragraph 2.4 - "Data sheets shall contain an evaluation of acceptability." The evaluation of acceptability is indicated on the results and data sheets by the approval signature.

Paragraph 3(4) - "Visual examination of contact corrosion." No visual examination for contact corrosion is made on breaker and starter contacts unless there is evidence of water damage or condensation. Contact resistance tests are made on breakers rated at 4 kV and above. No contact resistance test is made of lower voltage breakers or starters.

Paragraph 6.2.2 - "Demonstrate freedom from unwanted noise." No system test incorporates a noise measurement. If the system under test meets the test criteria, then noise is not a problem.

(8) IEEE 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems."

(9) IEEE 344-1971, "Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations."

(10) IEEE 344-1975, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

(11) IEEE 384-1974, "Criteria for Independence of Class 1E Equipment and Circuits"

(12) IEEE 603-1980, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

(13) ANSI/IEEE-ANS-7-4.3.2-1982, “Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations,” 1982 (ANSI/IEEE-ANS-7-4.3.2-1982, expands and amplifies the requirements of IEEE 603-1980).

7.1.4 REFERENCES

1. IEEE Standard, 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

2. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

3. J. A. Nay, Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, WCAP-7671, April 1971.

4. J. B. Lipchak and R. A. Stokes, Nuclear Instrumentation System, WCAP-7669, April 1971.

5. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

6. J. T. Haller, Engineered Safeguards Final Device or Activator Testing, WCAP-7705, February 1973.

7. Deleted

8. Deleted

9. Deleted

10. Summary Report EAGLE 21 Process Protection System Upgrade for Diablo Canyon Power Plant Units 1 and 2, WCAP-12813, Revision 3, June 1993.

7.2 REACTOR TRIP SYSTEM

This section provides a system description and the design bases for the reactor trip system (RTS).

The RTS automatically keeps the reactor operating within a safe region by tripping the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations such as mechanical and hydraulic limitations on equipment, and heat transfer phenomena. Therefore, the RTS keeps surveillance on process variables that are directly related to equipment mechanical limitations such as pressure, pressurizer water level (to prevent water discharge through safety valves and uncovering heaters), and also on variables that directly affect the heat transfer capability of the reactor (e.g., flow and reactor coolant temperatures). Other parameters utilized in the RTS are calculated from various process variables. In any event, whenever a direct process or a calculated variable exceeds a setpoint, the reactor will be shut down to protect against either gross damage to fuel cladding or loss of system integrity that could lead to release of radioactive fission products into the containment.

7.2.1 Design Bases

7.2.1.1 General Design Criterion 2, 1967 – Performance Standards

The reactor trip system (RTS) is designed to withstand the effects of or is protected against natural phenomena, such as earthquakes, tornadoes, flooding, winds, tsunamis, and other local site effects.

7.2.1.2 General Design Criterion 11, 1967 – Control Room

The RTS is designed to or contains instrumentation and controls that support actions to maintain the safe operational status of the plant from the control room or from an alternate location if control room access is lost due to fire or other causes.

7.2.1.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

Instrumentation and controls are provided as required to monitor and maintain the RTS variables within prescribed operating ranges. The RTS is provided to receive plant instrumentation signals and automatically trip the reactor as prescribed limits are approached or reached.

7.2.1.4 General Design Criterion 14, 1967 – Core Protection Systems

The RTS is designed to act automatically to prevent or to suppress conditions that could result in exceeding acceptable fuel damage limits.

7.2.1.5 General Design Criterion 19, 1967 – Protection Systems Reliability

The RTS is designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

7.2.1.6 General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence

Redundancy and independence are designed into the RTS sufficient to assure that no single failure or removal from service of any component or channel of a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served. Different principles are used where necessary to achieve true independence of redundant instrumentation components.

7.2.1.7 General Design Criterion 21, 1967 – Single Failure Definition

The RTS is designed to remain operable after sustaining a single failure. Multiple failures resulting from a single event are treated as a single failure.

7.2.1.8 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

The RTS is designed such that protection systems are separated from control instrumentation systems to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels.

7.2.1.9 General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems

The RTS is designed such that the effects of adverse conditions to which redundant channels or RTS might be exposed in common, either under normal conditions or those of an accident will not result in loss of the reactor trip function.

7.2.1.10 General Design Criterion 24, 1967 – Emergency Power for Protection Systems

The RTS is designed such that in the event of loss of all offsite power, sufficient alternate sources of power are provided to permit the required functioning of the RTS.

7.2.1.11 General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems

The RTS includes the means for testing the RTS while the reactor is in operation to demonstrate that no failure or loss of redundancy has occurred.

7.2.1.12 General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design

The RTS is designed, with noted exceptions, to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or adverse environments (e.g., extreme heat or cold, fire, steam, or water) are experienced.

7.2.1.13 General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction

The RTS is designed to prevent exceeding acceptable fuel damage limits by limiting reactivity transients resulting from any single malfunction in the reactivity control systems, such as, unplanned continuous withdrawal (not ejection) of a control rod.

7.2.1.14 General Design Criterion 49, 1967 – Containment Design Basis

The RTS instrumentation circuits routed through containment electrical penetrations are designed so that the containment structure can accommodate, without exceeding the design leakage rate, pressures and temperatures resulting from the largest credible energy release following a loss-of-coolant accident (LOCA).

7.2.1.15 Reactor Trip System Safety Function Requirements

(1) <u>Protection from Missiles</u>

The RTS is designed to be protected against the effects of missiles which may result from plant equipment failure and from events and conditions outside the plant.

(2) <u>Protection Against High Energy Pipe Rupture Effects</u>

The RTS is designed and located to accommodate the dynamic effects of a postulated high-energy pipe failure to the extent necessary to assure that a safe shutdown condition of the reactor can be accomplished and maintained.

(3) <u>Protection from Moderate Energy Pipe Rupture Effects – Outside Containment</u>

The RTS system portion located outside containment is designed to be protected against the effects of moderate energy pipe failure

(4) Protection from Jet Impingement – Inside Containment

The RTS system portion located inside containment is designed to be protected against the effects of jet impingement which may result from high energy pipe rupture.

(5) Protection from Flooding Effects – Outside Containment

The RTS system portion located outside containment is to be protected from the effects of internal flooding.

7.2.1.16 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The RTS electric components that require environmental qualification are qualified to the requirements of 10 CFR 50.49.

7.2.1.17 Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions

The RTS is periodically tested to provide assurance that the system will operate as designed and will be available to function properly. The testing program conforms to Safety Guide 22, February 1972.

7.2.1.18 NUREG-0737 (Items II.K.3.10 and II.K.3.12), November 1980 – Clarification of TMI Action Plan Requirements

Item II.K.3.10 – Proposed Anticipatory Trip Modification: The setpoint for the anticipatory reactor trip on turbine trip bypass (P-9) cannot be raised above 10% reactor power until it has been shown that the probability of a small-break loss-of-coolant accident (LOCA) resulting from a stuck-open power-operated relief valve (PORV) is substantially unaffected by the modification.

Item II.K.3.12 – Anticipatory Reactor Trip upon Turbine Trip: The RTS includes an anticipatory reactor trip upon turbine trip.

7.2.1.19 Generic Letter 83-28 (Actions 4.3 and 4.5), July 1983 – Required Actions Based on Generic Implications of Salem ATWS Events

Action 4.3 – RTS Reliability (Automatic Actuation of Shunt Trip Attachment for Westinghouse and B&W Plants): The RTS provides actuation of the breaker shunt trip attachments. The shunt trip attachment is considered Class 1E.

Action 4.5 – RTS Reliability (System Functional Testing): On-line functional testing of the RTS, including independent testing of the diverse trip features, is performed.

7.2.2 System Description

The RTS uses sensors that feed the process circuitry consisting of two to four redundant channels, which monitor various plant parameters. The RTS also contains the logic circuitry necessary to automatically open the reactor trip breakers. The logic circuitry consists of two redundant logic trains that receive input from the protection channels.

Each of the two logic trains, A and B, is capable of opening a separate and independent reactor trip breaker (52/RTA and 52/RTB). Logic train A opens reactor trip breaker 52/RTA and bypass breaker 52/BYB. Logic train B opens reactor trip breaker 52/RTB and bypass breaker 52/BYA. The two trip breakers in series connect three-phase ac power from the rod drive motor generator sets to the rod drive power bus, as shown in Figure 7.2-1, Sheets 3 and 4. For reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker. Additionally, an undervoltage trip auxiliary relay provides a trip signal to the shunt trip coil that trips open the breaker in the unlikely event of an undervoltage coil malfunction. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall by gravity into the core. The rods cannot be withdrawn until an operator resets the trip breakers. The trip breakers cannot be reset until the bistable, which initiated the trip, reenergizes. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed below.

The RTS design was evaluated in detail with respect to common mode failure and is presented in References 1 and 11. Preoperational testing was performed on RTS components and systems to determine equipment readiness for startup. This testing served as a further evaluation of the system design.

Analyses of the results of Conditions I, II, III, and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load reduction and turbine trip is identified in Section 7.4.2 and Section 10.2.2.

7.2.2.1 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the RTS reaches a preset level. In addition to redundant channels and trains, the design approach provides an RTS that monitors numerous system variables, thereby providing RTS functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in Reference 1.

Table 7.2-1 provides a list of reactor trips that are described below.

7.2.2.1.1 Nuclear Overpower Trips

The specific trip functions generated are:

(1) *Power Range High Nuclear Power Trip* - The power range high nuclear power trip circuit trips the reactor when two of the four power range channels exceed the trip setpoint. There are two independent bistables each with its own trip setting (a high and a low setting). The high trip setting provides protection during normal power operation and is always active. The low trip setting, which provides protection during startup, can be manually blocked when two of the four power range channels read above approximately 10 percent power (P-10). This trip function is automatically reinstated when three of the four power range channels decrease below 10 percent power. Refer to Table 7.2-2 for a listing of all protection system interlocks.

(2) *Intermediate Range High Neutron Flux Trip* - The intermediate range high neutron flux trip circuit trips the reactor when one of the two intermediate range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two of the four power range channels are above approximately 10 percent power (P-10). This trip function is automatically reinstated when three of the four power range channels decrease below 10 percent power. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

(3) *Source Range High Neutron Flux Trip* - The source range high neutron flux trip circuit trips the reactor when one of the two source range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup and plant shutdown, can be manually blocked when one of the two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below the P-6 value. This trip is also automatically bypassed by two-out-of-four logic from the power range interlock (P-10). This trip function can also be reinstated below P-10 by an administrative action requiring manual actuation of two control board-mounted switches. Each switch will reinstate the trip function in one of the two protection logic trains. The source range trip point is set between the P-6 setpoint (source range cutoff flux level) and the maximum source range flux level. The channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

(4) *Power Range High Positive Nuclear Power Rate Trip* - This circuit trips the reactor when an abnormal rate of increase in nuclear power occurs in two

of the four power range channels. This trip provides protection against rod ejection and rod withdrawal accidents of low worth from middle to low power conditions and is always active.

Figure 7.2-1, Sheets 5 and 6, shows the logic for all of the nuclear overpower and rate trips. A detailed functional description of the equipment associated with this function is provided in Reference 2.

7.2.2.1.2 Core Thermal Overpower Trips

The specific trip functions generated are:

(1) *Overtemperature ΔT Trip* - This trip protects the core against DNB and trips the reactor on coincidence, as listed in Table 7.2-1, with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by process protection circuitry for each loop by solving the following equation:

$$\Delta Ti\frac{(1+\tau_4 s)}{(1+\tau_5 s)} \le \Delta Ti^{\circ}\left\{K_1 - K_2\frac{(1+\tau_1 s)}{(1+\tau_2 s)}\left[Tavg_i - Tavg_i^{\circ}\right] + K_3(P - P^{\circ}) - f_1(\Delta I)\right\} \qquad (7.2\text{-}1)$$

where:

ΔTi° = indicated ΔT at rated thermal power from loop i, °F

$Tavg_i^{\circ}$ = Indicated Tavg at rated thermal power from loop i, °F

P° = 2235 psig (indicated RCS nominal operating pressure)

Th_{ij} = jth narrow range Thot input signal from loop i

$T^f h_{ij}$ = $Th_{ij}\ (1/(1+\tau_6 s))$

$\frac{1}{1+\tau_6 s}$ = Lag compensator on measured Thot

$Thave_i$ = $\sum(T^f h_{ij})/3$ for j = 1 - 3 for each loop, i = 1 - 4

Note: A 3-input redundant sensor algorithm (RSA) eliminates $T^f h_{ij}$ values that result from known bad inputs or that fail a consistency check. The RSA also determines a quality code for $Thave_i$, depending on the quality and consistency of the individual $T^f h_{ij}$ values. (Refer to Section 7.2.2.3)

Tc_{ij} = jth narrow-range Tcold input signal from loop i

$T^f c_{ij}$ = Tc_{ij} $(1/(1+\tau_7 s))$

$\frac{1}{1+\tau_7 s}$ = Lag compensator on measured Tcold

τ_6; τ_7 = Time constants utilized in the lag compensator for Thot and Tcold: τ_6 = 0 secs; τ_7 = 0 secs

$Tcave_i$ = $\sum (T^f c_{ij})/2$ for j = 1 - 2 for each loop, i = 1 - 4

Note: A 2-input RSA determines a quality code and a value for $Tcave_i$, depending on the quality and consistency of the individual $T^f c_{ij}$ values. (Refer to Section 7.2.2.3)

ΔTi = $(Thave_i - Tcave_i)$ for each loop, i = 1 - 4, °F

$\bar{T}avg_i$ = $(Thave_i + Tcave_i)/2$ for each loop, i = 1 - 4, °F

$\frac{1+\tau_4 s}{1+\tau_5 s}$ = The function generated by the lead-lag controller for ΔT dynamic compensation

τ_4; τ_5 = Time constants utilized in the lead-lag controller for ΔT: τ_4 = 0 sec; τ_5 = 0 sec

P = pressurizer pressure signal, psig

$\frac{1+\tau_1 s}{1+\tau_2 s}$ = the function generated by the lead-lag controller for $Tavg_i$ dynamic compensation

τ_1 ; τ_2 = time constants utilized in the lead-lag controller for Tavg:
τ_1 = 30 sec;
τ_2 = 4 sec

s = Laplace transform operator, sec^{-1}

K_1 = (*)

K_2 = (*)

K_3 = (*)

f_1 (ΔI) = a function of the indicated difference between top and bottom detectors of the power range nuclear ion chambers, with grains to be selected based on measured instrument response during plant startup tests such that:

(a) for $q_t - q_b$ between (*) and (*), f_1 (ΔI) = 0
(where q_t and q_b are percent rated thermal power in the top and bottom halves of the core respectively, and $q_t + q_b$ is total thermal power in percent of rated thermal power)

(b) for each percent that the magnitude of ($q_t - q_b$) exceeds (*), the ΔT trip setpoint shall be automatically reduced by (*) of its value at rated thermal power

(c) for each percent that the magnitude of ($q_t - q_b$) exceeds (*), the ΔT trip setpoint shall be automatically reduced by (*) of its value at rated thermal power

Note: The channel's maximum trip point shall not exceed its computed trip point by more than (*).

(*) Refer to Technical Specifications for current values to be used.

One power range channel separately feeds each overtemperature ΔT trip channel.

Changes in f_1 (ΔI) can only lead to a decrease in the trip setpoint; refer to Figure 7.2-2.

The single pressurizer pressure parameter required per loop is obtained from separate sensors that are connected to three pressure taps at the top of the pressurizer. The four pressurizer pressure signals are obtained from the three taps by connecting one of the taps to two pressure transmitters. Refer to Section 7.2.2.1.3 for analysis of this arrangement. Figure 7.2-1, Sheets 9 and 10, shows the logic for the overtemperature ΔT trip function.

(2) *Overpower ΔT Trip* - This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7.2-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation:

$$\Delta Ti\frac{(1+\tau_4 s)}{(1+\tau_5 s)} \le \Delta Ti^{\circ}\left\{K_4 - K_5\frac{\tau_3 s}{1+\tau_3 s}Tavg_i - K_6\left[Tavg_i - Tavg_i^{\circ}\right] - f_2(\Delta I)\right\} \qquad (7.2\text{-}2)$$

where:

$Tavg_i$ = As defined for overtemperature ΔT trip

ΔT_i	=	As defined for overtemperature ΔT trip
$Tavg_i^o$	=	As defined for overtemperature ΔT trip
ΔT_i^o	=	As defined for overtemperature ΔT trip
$\frac{1+\tau_4 s}{1+\tau_5 s}$	=	The function generated by the lead-lag controller for measured ΔT
τ_4; τ_5	=	Time constants used in the lead-lag controller for measured ΔT: τ_4 = 0 sec; τ_5 = 0 sec
K_4	=	(*)
K_5	=	(*)/°F for increasing average temperature; 0 for decreasing average temperature
K_6	=	(*) for $Tavg_i > Tavg_i^o$; K6 = 0 for $Tavg_i \leq Tavg_i^o$
$\frac{\tau_3 s}{1+\tau_3 s}$	=	the function generated by the rate-lag controller for $Tavg_i$ dynamic compensation
τ_3	=	time constants utilized in the rate-lag controller for Tavg τ_3 = 10 sec
s	=	Laplace transform operator, sec^{-1}
f_2 (ΔI)	=	0 for all ΔI

Note: The channel's maximum trip point shall not exceed its computed trip point by more than (*).

(*) Refer to Technical Specifications for current values.

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant ΔT setpoint is compared to the same ΔT. Figure 7.2-1, Sheets 9 and 10, shows the logic for this trip function.

7.2.2.1.3 Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are:

(1) *Pressurizer Low-Pressure Trip* - The purpose of this trip is to protect against low pressure that could lead to departure from nucleate boiling (DNB), and to limit the necessary range of protection afforded by the overtemperature ΔT trip. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7, the reactor is tripped when the dynamically compensated pressurizer pressure measurements fall below preset limits. This trip is blocked below P-7 to permit startup. The trip logic and interlocks are provided in Table 7.2-1.

The trip logic is shown in Figure 7.2-1, Sheets 11 and 12.

(2) *Pressurizer High-Pressure Trip* - The purpose of this trip is to protect the reactor coolant system (RCS) against system overpressure.

The same sensors and transmitters used for the pressurizer low-pressure trip are used for the high-pressure trip except that separate comparators are used for the trip. These comparators trip when nondynamically compensated pressurizer pressure signals exceed preset limits on coincidence, as listed in Table 7.2-1. There are no interlocks or permissives associated with this trip function.

The logic for this trip is shown in Figure 7.2-1, Sheets 11 and 12.

(3) *Pressurizer High Water Level Trip* - This trip is provided as a backup to the pressurizer high-pressure trip and prevents the pressurizer from becoming water solid during low worth and low power rod withdrawal accidents. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of the pressurizer high water level signals are provided in Table 7.2-1.

The trip logic for this function is shown in Figure 7.2-1, Sheets 11 and 12.

7.2.2.1.4 Reactor Coolant System Low-Flow Trips

These trips protect the core from DNB in the event of a loss of coolant flow situation. The means of sensing the loss of coolant are:

(1) *Reactor Coolant Low-Flow Trip* - The parameter sensed is reactor coolant flow. Three elbow taps in each coolant loop are used as flow devices that indicate the status of reactor coolant flow. The basic function of these devices is to provide information as to whether or not a reduction in flow has occurred. An output signal from two out of the three comparators in a loop would indicate a low flow in that loop. The trip logic for this function is shown in Figure 7.2-1, Sheets 9 and 10. The coincidence logic and interlocks are shown in Table 7.2-1.

(2) *Reactor Coolant Pump Breakers Open Trip* - Opening of two reactor coolant pump breakers or redundant overcurrent protection breakers above the P-7 interlock setpoint, which is indicative of an imminent loss of coolant flow, also causes a reactor trip.

One set of auxiliary contacts on each pump breaker serves as the input signal to the trip logic. The trip logic for this function is shown in Figure 7.2-1, Sheets 9 and 10. The coincident logic and interlocks are shown in Table 7.2-1.

(3) *Reactor Coolant Pump Bus Undervoltage Trip* - This trip is required to protect against low flow that can result from loss of voltage to the reactor coolant pumps. Time delays are incorporated in the undervoltage trip relays to prevent spurious reactor trip from momentary electrical power transients. The maximum external time delay is determined to be 0.6 seconds. This allows the total time delay for reactor UV trip to stay within the limits specified in Equipment Control Guidelines and also within the limit established in the accident analysis, Section 15.1.5. (The nominal time delay will be 0.5 seconds, with a tolerance of +/- 0.05 seconds.) There are two undervoltage sensors on each of the two buses. A one-out-of-two undervoltage signal on both buses trips the reactor if above the P-7 setpoint and starts the turbine-driven auxiliary feedwater pump at any reactor power level. The trip logic for this function is shown in Figure 7.2-1, Sheets 9 and 10.

(4) *Reactor Coolant Pump Bus Underfrequency Trip* - This trip is required to protect against low flow resulting from bus underfrequency, which might result from a major power grid frequency disturbance.

There are three underfrequency sensors on each of two buses. A two-out-of-three underfrequency signal on either bus trips the reactor if above the P-7 setpoint. The logic scheme is arranged so that a two-out-of-three underfrequency signal on bus 1 trips the breakers to reactor coolant pumps 1 and 2 only, and a two-out-of-three underfrequency signal on bus 2 will trip the breakers to reactor coolant pumps 3 and 4 only. The trip logic for this function is shown in Figure 7.2-1, Sheets 9 and 10.

7.2.2.1.5 Low-Low Steam Generator Water Level Trip (Including Trip Time Delay)

This trip protects the reactor from loss of heat sink in the event of a loss of feedwater to one or more steam generators or a major feedwater line rupture. This trip is actuated on two out of three low-low water level signals occurring in any steam generator. If a low-low water level condition is detected in one steam generator, signals shall be generated to trip the reactor and start the motor-driven auxiliary feedwater pumps. If a

low-low water level condition is detected in two or more steam generators, a signal is generated to start the turbine-driven auxiliary feedwater pump as well.

The signals to actuate reactor trip and start auxiliary feedwater pumps are delayed through the use of a Trip Time Delay (TTD) system for reactor power levels below 50 percent of RTP. Low-low water level in any protection set in any steam generator will generate a signal that starts an elapsed time trip delay timer. The allowable trip time delay is based upon the prevailing power level at the time the low-low level trip setpoint is reached. If power level rises after the trip time delay setpoints have been determined, the trip time delay is redetermined (i.e., decreased) according to the increase in power level. However, the trip time delay is not changed if the power level decreases after the delay has been determined. The use of this delay allows added time for natural steam generator level stabilization or operator intervention to avoid an inadvertent protection system actuation.

The logic is shown in Figure 7.2-1, Sheets 13 and 14.

Steam generator water level low-low trip time delay:

$$TD = B1(P)^3 + B2(P)^2 + B3(P) + B4 \qquad (7.2\text{-}3)$$

where:

P = RCS loop ΔT equivalent to power (% rated thermal power (RTP)); $P \leq 50\%$ RTP

TD = time delay for steam generator water level low-low reactor trip (in seconds)

B1, B2, B3, and B4 are constants:

B1 = -0.007128
B2 = +0.8099
B3 = -31.40
B4 = +464.1

7.2.2.1.6 Turbine Trip-Reactor Trip

The turbine trip-reactor trip is actuated by two-out-of-three logic from low autostop oil pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-9.

Other turbine trips are discussed in Chapter 10.

The logic for this trip is shown in Figure 7.2-1, Sheets 3, 7, 19, 31 and Sheets 4, 8, 20, 32.

The analog portion of the trip shown in Figure 7.2-1, Sheets 31 and 32, is represented by dashed lines. When the turbine is tripped, turbine autostop oil pressure drops, and the pressure is sensed by three pressure sensors. A logic output is provided from each sensor when the oil pressure drops below a preset value. These three outputs are transmitted to two redundant two-out-of-three logic matrices, either of which trips the reactor if above P-9.

The autostop oil pressure signal also dumps the emergency trip fluid, closing all of the turbine steam stop valves. When all stop valves are closed, a reactor trip signal is initiated if the reactor is above P-9. This trip signal is generated by redundant contacts in each stop valve limit switch.

7.2.2.1.7 Safety Injection Signal Actuation Trip

A reactor trip occurs when the safety injection system (SIS) is actuated. The means of actuating the SIS are described in Section 7.3.2. Figure 7.2-1, Sheets 15 and16, shows the logic for this trip.

7.2.2.1.8 Manual Trip

The manual trip consists of two switches with four outputs on each switch. Each switch provides a trip signal for both trip breakers and both bypass breakers. (Operating a manual trip switch also removes the voltage from the undervoltage trip coil.)
There are no interlocks that can block this trip. Figure 7.2-1, Sheets 5 and 6, shows the manual trip logic.

7.2.2.1.9 Seismic Trip

The seismic trip system operates to shut down reactor operations should ground accelerations exceed a preset level in any two of the three orthogonal directions monitored (one vertical, two horizontal). The preset level is indicated in the Technical Specifications (Reference 4). No credit was taken for operation of the seismic trip in the safety analysis; however, its functional capability at the specified trip settings is required to enhance the overall reliability of the reactor protection system.

Three triaxial sensors (accelerometers) are anchored to the containment base in three separate locations 120 degrees apart (Figure 7.2-6). Each senses acceleration in three mutually orthogonal directions. Output signals are generated when ground accelerations exceed the preset level. These signals, lasting from 6 to 20 seconds (adjustable), are wired directly to the Trains A and B solid state protection system (SSPS). Refer to Figure 7.2-1, Sheets 35 and 36. If two of the three sensors in any direction produce simultaneous outputs, the logic produces trains A and B reactor trip signals.

The seismic reactor trip system was designed in compliance with IEEE 279-1971 (Reference 7) and IEEE 344-1975 (Reference 21), but will not be required to function

during or following a LOCA or fire. Cables and raceways are separated in accordance with Section 8.3.1.4.1

7.2.2.1.10 Automatic Trip Logic

The general alarm system, described in Reference 5, maintains a check on each train of the solid-state logic protection system for the existence of certain undesirable conditions. Both trains are tripped if an abnormal condition occurs simultaneously in both trains. Reference 5 states that SSPS printed circuit boards (PCBs) use Motorola High Threshold Logic (MHTL). MHTL based PCBs are obsolete and have been replaced with PCBs which are not based on MHTL (Reference 33). The replacement universal logic, safeguards driver, or under voltage driver PCBs have diagnostic features that can activate a general warning alarm when there is a critical board problem.

7.2.2.2 Reactor Trip System Interlocks

7.2.2.2.1 Power Escalation Permissives

The overpower protection provided by the out-of-core nuclear instrumentation consists of three discrete, but overlapping, levels. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

A one-out-of-two intermediate range permissive signal (P-6) is required prior to source range level trip blocking and detector high voltage cutoff. Source range level trips are automatically reactivated and high voltage restored when both intermediate range channels are below the permissive (P-6) levels. There is a manual reset switch for administratively reactivating the source range level trip and detector high voltage when between the permissive P-6 and P-10 level, if required. Source range level trip block and high voltage cutoff are always maintained when above the permissive P-10 level.

The intermediate range level trip and power range (low setpoint) trip can be blocked only after satisfactory operation and permissive information are obtained from two-out-of-four power range channels. Individual blocking switches are provided so that the low range power range trip and intermediate range trip can be independently blocked. These trips are automatically reactivated when any three of the four power range channels are below the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown in Figure 7.2-1, Sheets 7 and 8. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

Refer to Table 7.2-2 for the list of protection system interlocks.

7.2.2.2.2 Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) on a low reactor coolant flow or reactor coolant pump open breaker signal in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, and pressurizer high water level on both units. Refer to Figure 7.2-1, Sheets 9, 10 and Sheets 11, 12 for permissive applications. The low power signal is derived from three-out-of-four power range neutron flux signals below the setpoint in coincidence with one-out-of-two turbine impulse chamber pressure signals below the setpoint (low plant load).

The P-8 interlock blocks a reactor trip when the plant is below a preset level specified in the Technical Specifications on a low reactor coolant flow in any one loop. The block action (absence of the P-8 interlock signal) occurs when three-out-of-four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor is allowed to operate with one inactive loop, and trip will not occur until two loops are indicating low flow. Refer to Figure 7.2-1, Sheets 7 and 8, for derivation of P-8, and Sheet 5 for the applicable logic.

The P-9 interlock blocks a reactor trip below the maximum value of 50 percent of full power on a turbine trip signal. Refer to Figure 7.2-1, Sheets 2, 7, 31 and Sheets 4, 8, 32 for the application logic. The reactor trip on turbine trip is actuated by two-out-of-three logic from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves.

Refer to Table 7.2-2 for the list of protection system blocks.

7.2.2.3 Coolant Temperature Sensor Arrangement and Calculational Methodology

The individual narrow range cold and hot leg temperature signals required for input to the reactor trip circuits and interlocks are obtained using resistance temperature detectors (RTDs) installed in each reactor coolant loop.

The cold leg temperature measurement on each loop is accomplished with a dual element narrow-range RTD mounted in a thermowell. The cold leg sensors are inherently redundant in that either sensor can adequately represent the cold leg temperature measurement. Temperature streaming in the cold leg is not a concern due to the mixing action of the reactor coolant pump.

The hot leg temperature measurement on each loop is accomplished with three dual element narrow-range RTDs mounted in thermowells spaced 120 degrees apart around the circumference of the reactor coolant pipe for spatial variations. One of the elements in each thermowell is an installed spare.

These cold and hot leg narrow-range RTD signals are input to the protection system digital electronics and processed as follows:

The two filtered cold leg temperature input signals $T^f c_j$ for each loop i are processed to determine a group average value $T^f cave_i$. The 2-input redundant sensor algorithm (RSA) calculates the group average value based on the number of good input signals.

If both input signals are BAD, the group value is set equal to the average of the two bad sensor values. If one signal is BAD and the other is DISABLED, the group value is set equal to the value of the bad sensor. The group quality is set to BAD in either case.

If one of the input signals is BAD and the other is GOOD, the group value is set equal to the GOOD value. A consistency check is not performed. The group quality is set to POOR.

If neither of the input signals is BAD, a consistency check is performed. If the deviation of these two signals is within an acceptance tolerance (±DELTAC), the group quality is set to GOOD and the group value is set equal to the average of the two inputs. If the difference exceeds ±DELTAC, the group quality is set to BAD, and the individual signal qualities are set to POOR. The group value is set equal to the average of the two inputs.

DELTAC is a fixed input parameter based on operating experience. One DELTAC value is required for each protection set.

Estimates of hot leg temperature are derived from each T_{hot} input signal as follows:

$$\overline{T}_{hestij} = T^f_{hij} - P_{B_i S^o_{ij}} \qquad (7.2\text{-}4)$$

where:

T^f_{hij} is the filtered T_{hot} signal for the jth RTD (j = 1 to 3) in the ith loop (i = 1 to 4)

P_{B_i} = power fraction being used to correct the bias value being used for any power level

$$P_{B_i} = \left(T^f_{have_i} - T^f_{cave_i}\right) / \Delta T^\circ_i \qquad (7.2\text{-}5)$$

where:

ΔT^o_i is the full power ΔT in the ith loop

S^o_{ij} = manually input bias that corrects the individual T_{hot} RTD value to the loop average.

The three hot leg temperature estimates T_{hestj} for each loop i are processed to determine a group average value T^f_{havei}. The 3-input RSA calculates the group value T^f_{havei} based on the available number of good input values.

If all three inputs are BAD, the group value is set to the average of the three input sensor values. The group value quality is set to BAD. If only one input is GOOD, the group value is set equal to the value of the good sensor. The group quality is set to BAD.

If two inputs are good, the difference between the two sensors is compared to DELTAH. If the inputs do not agree within ±DELTAH, the group quality is set to BAD and the quality of both inputs is set to POOR. If the inputs agree, the group quality is set to GOOD. The group value is set equal to the average of the two inputs in either case.

If all three inputs are good, an average of the three estimated hot leg temperatures is computed and the individual signals are checked to determine if they agree within ± DELTAH of the average value. If all of the signals agree within ± DELTAH of the average value, the group quality is set to GOOD. The group value (T^f_{havei}) is set to the average of the three estimated average hot leg temperatures.

If the signal values do not all agree within ± DELTAH of the average, the RSA will delete the signal value that is furthest from the average. The quality of this signal will be set to POOR and a consistency check will then be performed on the remaining GOOD signals. If these signals pass the consistency check, the group value will be taken as the average of these GOOD signals and the group quality will be set to POOR. However, if these signals again fail the consistency check (within ± DELTAH), then the group value will be set to the average of these two signals; but the group quality will be set to BAD. All of the individual signals will have their quality set to POOR.

DELTAH is a fixed input parameter based upon temperature fluctuation within the hot leg. One DELTAH value is required for each protection set.

Delta T and T Average are calculated as follows:

$$\Delta T_i = T^f_{have_i} - T^f_{cave_i} \qquad (7.2\text{-}6)$$

$$T_{avg_i} = (T^f_{have_i} + T^f_{cave_i})/2.0 \qquad (7.2\text{-}7)$$

The calculated values for Delta T and T_{avg} are then utilized for both the remainder of the Overtemperature and Overpower Delta T protection channel and channel outputs for control purposes.

A similar calculation of Delta T is performed for and used by the steam generator low-low level trip time delay (TTD) function.

Alarms are generated from a group status that is based on the quality of T^f_{havei} and T^f_{cavei} out of the RSA. If the quality of either group is BAD and all of the inputs for that group are not off scale low, then the group status is set to TROUBLE and RTD FAILURE. If either quality is POOR and all of its inputs are not off scale low, then the group status is set to TROUBLE. Otherwise, the group status is set to GOOD.

7.2.2.4 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap. The modification shown in Figure 7.2-4 consists of the use of a sealed reference leg instead of the conventional open column of water. Refer to Section 7.2.2.11.4 for an analysis of this arrangement.

7.2.2.5 Process Protection System

The process protection system is described in Reference 3.

With the installation of the RTD bypass elimination functional upgrade as part of the Eagle 21 process protection system upgrade, the following plant operating concerns are addressed:

(1) The possibility of loss of flow or reduced flow through the common return line of the hot and cold RTD bypass manifold, as a result of transport time of the temperature measurements for the RTD loop, affecting the design basis for the overtemperature, overpower and control channels monitoring associated with the affected RTD bypass loop is eliminated.

(2) Operator indication of the loop Tavg, Tavg, and Delta-T deviation alarms is maintained, providing the operator the same detecting signals as with the bypass loops.

(3) The potential for a failed Thot RTD affecting the loop Tavg, Tavg, and ΔT measurements is reduced due to the algorithms provided in the Eagle 21 process protection system software that automatically detect a failed RTD and eliminate the failed RTDs measurement from affecting these plant parameters

7.2.2.6 Solid State (Digital) Logic Protection

The solid-state logic protection system takes binary inputs, (voltage/no voltage) from the process and nuclear instrument channels and direct inputs corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils of the reactor trip circuit breakers and an undervoltage auxiliary relay when the necessary combination of signals occurs. The undervoltage auxiliary relay sends a trip signal (125-Vdc) to the shunt trip coils of the reactor trip breakers. The system also

sends actuation signals to engineered safety features (ESF) components (as discussed in Section 7.3), provides annunciator, status light, and computer input signals that indicate the condition of bistable input signals, partial- and full-trip functions, and the status of the various blocking, permissive, and actuation functions. In addition, the system includes means for semiautomatic testing of the logic circuits. A detailed description of this system is provided in Reference 6. Reference 6 is based on SSPS printed circuit boards (PCBs) that use Motorola High Threshold Logic (MHTL). MHTL based PCBs are obsolete and have been replaced with PCBs which are not based on MHTL (Reference 33).

7.2.2.7 Reactor Trip Breakers

The reactor trip breakers are equipped for automatic actuation of both the undervoltage trip device and the shunt trip device. The reactor trip breakers are also equipped to permit manual trip of the breakers at the switchgear cabinet.

7.2.2.8 Isolation Devices

In certain applications, it is advantageous to employ control signals derived from individual protection channels through isolation devices contained in the protection channel, as permitted by IEEE-279-1971 (Reference 7).

In all of these cases, signals derived from protection channels for nonprotective functions are obtained through isolation devices located in the process protection racks. By definition, nonprotective functions include those signals used for control, remote process indication, and computer monitoring.

Isolation devices qualification type tests are described in References 8, 9, and 32.

7.2.2.9 Energy Supply and Environmental Qualification Requirements

The energy supply for the RTS, including the voltage and frequency variations, is described in Section 8.3.1.1.5.2.1, Class 1E 120-Vac Instrument Power Supply System.

Refer to Section 8.3.1.1.5.2.1 and Section 8.3.1.1.5.3.8 for a discussion on the power supply for the RTS and compliance with IEEE 308-1971 (Reference 13).

There are no Class I motors in the RTS; therefore, IEEE 334-1971 (Reference 15) does not apply.

The environmental qualification requirements are identified in Section 3.11.

7.2.2.10 Reactor Trip System Instrumentation Trip Setpoints

While most setpoints used in the RTS are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the RTS

have been selected either on the basis of applicable engineering code requirements or engineering design studies. Methodologies for determining RTS setpoint and allowable values are presented in WCAP-11082, Technical Specification 3.3.1, or in plant procedures. The capability of the RTS to prevent loss of integrity of the fuel cladding and/or RCS pressure boundary during Condition II transients is demonstrated in Section 15.2. A reactor trip is also credited for certain Condition III and IV events as described in Sections 15.3 and 15.4. These accident analyses are carried out using those setpoints determined from results of the engineering design studies. Functions that require a reactor trip and associated setpoint limits are presented in the Technical Specifications. A discussion of the intent for each of the various reactor trips and the accident analysis (where appropriate) that utilize the trip is presented in Section 7.2.2.1. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required to allow for uncertainties and instrument errors.

The setpoints for the various functions in the RTS have been analytically determined such that the operational limits so prescribed prevent fuel rod cladding damage and loss of integrity of the RCS as a result of any Condition II incident (anticipated malfunction). As such, the RTS limits the following parameters to:

(1) Minimum DNBR = The applicable limit value (Refer to Sections 4.4.4.1 and 4.4.3.3)

(2) Maximum system pressure = 2,750 psia

(3) Total core power less than or equal to 118 percent of nominal (limits the fuel rod maximum linear power to a kW/ft., less than the value that could cause fuel centerline melt)

The accident analyses described in Section 15.2 demonstrate that the functional requirements as specified for the RTS are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (Refer to Table 15.1-2). A discussion of the safety limits associated with the reactor core and RCS, plus the limiting safety system setpoints, is presented in the Technical Specifications.

7.2.2.11 Specific Control and Protection Interactions

7.2.2.11.1 Nuclear Power

Four power range nuclear power channels are provided for overpower protection. An additional control input signal is derived by auctioneering of the four channels for automatic rod control. If any channel fails producing a low output, that channel is incapable of proper overpower protection but does not cause control rod movement because of the auctioneer. Two-out-of-four overpower trip logic ensures an overpower trip, if needed, even with an independent failure in another channel.

In addition, a deviation signal gives an alarm if any nuclear power channel deviates significantly from any of the other channels. Also, the control system responds only to rapid changes in nuclear power; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear power range channel will block manual and automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.11.2 Coolant Temperature

The accuracy of the RTD temperature measurements is demonstrated during plant startup tests by comparing temperature measurements from all RTDs with one another. The comparisons are done with the RCS in an isothermal condition. The linearity of the ΔT measurements obtained from the hot leg and cold leg RTDs as a function of plant power is also checked during plant startup tests.

The absolute value of ΔT versus plant power is not important as far as reactor protection is concerned. RTS setpoints are based on percentages of the indicated ΔT at nominal full power, rather than on absolute values of ΔT. For this reason, the linearity of the ΔT signals as a function of power is of importance rather than the absolute values of the ΔT. As part of the plant startup tests, the loop RTDs signals are compared with the core exit thermocouple signals. Note also that reactor control is based on signals derived from protection system channels after isolation by isolation devices so that no feedback effect can perturb the protection channels.

Because control is based on the average temperature of the loop having the highest average temperature, the control rods are always moved based on the most conservative temperature measurement with respect to margins to DNB. A spurious low average temperature measurement from any loop temperature control channel causes no control action. A spurious high average temperature measurement causes rod insertion (safe direction).

In addition, channel deviation signals in the control system give an alarm if any temperature channel deviates significantly from the auctioneered (highest) value. Automatic rod withdrawal blocks also occur if any two of the temperature channels indicate an overtemperature or overpower condition.

7.2.2.11.3 Pressurizer Pressure

The pressurizer pressure protection channel signals are used for high- and low-pressure protection and as inputs to the overtemperature ΔT trip protection function. Isolated output signals from these channels are used for pressure control. These are used to control pressurizer spray and heaters, and power-operated relief valves. Pressurizer pressure is sensed by fast-response pressure transmitters.

A spurious high-pressure signal from one channel can cause decreasing pressure by actuation of either spray or relief valves. Additional redundancy is provided in the low

pressurizer pressure reactor trip logic and in the logic for safety injection to ensure low-pressure protection.

The pressurizer heaters are incapable of over pressurizing the RCS. Overpressure protection is based on the positive volume surge of the reactor coolant produced as a result of turbine trip under full load, assuming the core continues to produce full power. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3 percent. Note that no credit is taken for the relief capability provided by the power-operated relief valves during this surge.

In addition, operation of any one of the power-operated relief valves can maintain pressure below the high-pressure trip point for most transients. The rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available to alert the operator to the need for appropriate action.

Two of the pressure sensors share a common tap. The other two sensors use separate taps. Redundancy is not impaired by having a shared tap because the logic for this trip is two-out-of-four. If the shared tap is plugged, the reading of the affected channels will remain static. If the impulse line bursts, the indicated pressure will drop to zero. In either case, the fault is easily detectable, and the protective function remains operable.

7.2.2.11.4 Pressurizer Water Level

Three pressurizer water level channels are used for reactor trip (two-out-of-three high level). Isolated signals from these channels are used for pressurizer water level control. A failure in the water level control system could fill or empty the pressurizer at a slow rate (on the order of 1/2 hour or more).

Experience has shown that hydrogen gas can accumulate in the upper part of the condensate pot on conventional open reference leg systems in pressurizer water level service. At RCS operating pressures, high concentrations of dissolved hydrogen in the reference leg water are possible. On sudden depressurization accidents, it has been hypothesized that rapid effervescence of the dissolved hydrogen could blow water out of the reference leg and cause a large level error, measuring higher than actual level. Accurate calculations of this effect have been difficult to obtain. To eliminate the possibility of such effects in this application, a bellows is used in a pot at the top of the reference leg to provide an interface seal and prevent dissolving the hydrogen gas into the reference leg water. Supplier tests confirmed a time response of less than 1 second for the channel.

The reference leg is uninsulated and remains at local ambient temperature. This temperature varies somewhat over the length of the reference leg piping under normal operating conditions, but does not exceed 140°F. During the extreme temperature conditions caused by a blowdown accident, any reference leg water flashing to steam is confined to the condensate steam interface in the weir at the top of the temperature barrier leg and has only a small (about 12 inches between the top of weir and bellows)

effect on the measured level. Some additional error may be expected due to effervescence of hydrogen in the temperature barrier water. However, even if complete loss of this water is assumed, the error will be less than 1 foot and will not violate a safety limit.

The sealed reference leg design has been installed in various plants since early 1970, and operational accuracy was verified by use of the sealed reference leg system in parallel with an open reference leg channel. No effects of operating pressure variations on either the accuracy or integrity of the channel have been observed.

Calibration of the sealed reference leg system is done in place, after installation, by application of known pressure to the high pressure side of the transmitter with the pressure of the height of the reference column, corrected for density, applied to the transmitter low side. The effects of static pressure variations are predictable. The largest effect is due to the density change in the saturated fluid in the pressurizer itself. The effect is typical of level measurements in all tanks with two-phase fluid and is not peculiar to the sealed reference leg technique.

In the sealed reference leg, there is a slight compression of the fill water with increasing pressure, but this is taken up by the flexible bellows. A leak of the fill water in the sealed reference leg is detectable by comparison of redundant channel readings while the plant is on-line, and by physical inspection of the reference leg while the plant is off-line. Leaks of the reference leg to atmosphere are immediately detectable by off-scale indications and alarms on the control board. A closed pressurizer level instrument shutoff valve would be detected by comparing the level indications from the redundant level channels (three channels). In addition, there are alarms on one of the three channels to indicate an error between the measured pressurizer water level and the programmed pressurizer water level. The instrument sensing lines for these level sensing instruments are designed so that no single instrument valve can affect more than one of the three level channels.

The high water level trip setpoint provides sufficient margin so that the undesirable condition of discharging liquid coolant through the safety valves is avoided. Even at full power conditions, which would produce the worst thermal expansion rates, a failure of the water level control would not lead to any liquid discharge through the safety valves. This is due to the automatic high pressurizer pressure reactor trip actuating at a pressure sufficiently below the safety valve setpoint.

For control failures that tend to empty the pressurizer, two-out-of-four logic for safety injection action low pressurizer pressure ensures that the protection system can withstand an independent failure in another channel. In addition, ample time and alarms exist to alert the operator of the need for appropriate action.

7.2.2.11.5 Signal Validation Functions

The basic function of the reactor protection circuits associated with low steam generator water level is to preserve the steam generator heat sink for removal of long-term residual heat.

Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip, preventing eventual thermal expansion and discharge of the reactor coolant through the pressurizer relief valves into the relief tank even when main feedwater pumps are incapacitated. This reactor trip acts before the steam generators are dry to reduce the required capacity and starting time requirements of these auxiliary feedwater pumps, and to minimize the thermal transient on the RCS and steam generators. Therefore, a low-low steam generator water level reactor trip is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient. It is desirable to minimize thermal transients on a steam generator for a credible loss of feedwater accident. Hence, it should be noted that a protection system failure causing control system reaction is eliminated by implementation of control system signal validation; that is, steam generator water level (SGWL) median signal selector (MSS) and steam flow arbitrator (SFA) functions in the PG&E Design Class II digital feedwater control system.

The prime objective of the signal validation functions is to prevent a single failed protection system instrument channel from causing a disturbance in the feedwater control system requiring subsequent protective action, as required by IEEE 279-1971. All three isolated narrow range water level channels for each steam generator are input to the SGWL MSS. The device selects the median value of its inputs for use by the feedwater control system, and control system action is then based on this validated signal. By rejecting the high and low signals, the control system is prevented from acting on any single, failed protection system instrument channel.

The SFA function is provided to validate the steam flow inputs. The SFA uses logic to determine an appropriate control signal output based on the two steam flow channels for each steam generator. If the two input signals agree within a specified limit, the arbitrator output is the average of the inputs. If the deviation between the input signals exceeds the specified limit, the input signal closest to the arbitration signal is selected as the output. If neither of the inputs is within a specified limit, the arbitration signal itself is selected as the output of the arbitrator. The arbitration signal is based on turbine first stage pressure.

These algorithms prevent a single input channel failure from causing a control system transient requiring protective action. This includes failure of the instrument tap that is shared between one narrow-range level channel and one steam flow channel on each steam generator. The MSS function for steam generator narrow range level and the

SFA function for steam flow satisfy the control and protection interaction requirement of IEEE 279-1971.

Since no adverse control system action may result from a single, failed protection instrument channel, a second random protection system failure (as would otherwise be required by IEEE 279-1971) need not be considered. A more detailed discussion of the SFA and MSS and their compliance with control and protection system interaction criteria is provided in Reference 27.

7.2.2.12 TESTS AND INSPECTIONS

The periodic testing of the RTS conforms to the requirements of IEEE 338-1971 (Reference 16), with the following comment:

(1) The periodic test frequency specified in the Technical Specifications was conservatively selected, using the considerations discussed in paragraph 4.3 of Reference 16, to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements.

The testability of the system is discussed in Section 7.2.4.1.10.

The minimum frequencies for checks, calibration, and testing at each of the plant's operating modes are defined in the Technical Specifications. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

7.2.2.12.1 In-Service Tests and Inspections

Periodic surveillance of the RTS is performed to ensure proper protective action. This surveillance consists of checks, calibrations, and functional testing that are summarized in the following sections.

7.2.2.12.1.1 Channel Checks

A channel check consists of a qualitative assessment of channel behavior during operation by observation. This determination shall include, where possible, comparison of the channel indication and/or status with other indications and/or status derived from independent instrument channels measuring the same parameters.

7.2.2.12.1.2 Channel Calibration

A channel calibration shall be the adjustment, as necessary, of the channel such that it responds within the required range and accuracy to known values of input. The channel calibration shall encompass the entire channel including the sensors and alarm, interlock and/or trip functions, and may be performed by any series of sequential, overlapping, or total channel steps such that the entire channel is calibrated.

7.2.2.12.1.3 Actuation Logic Test

An actuation logic test shall be the application of various simulated input combinations in conjunction with each possible interlock logic state and verification of the required logic output. The actuation logic test shall include a continuity check, as a minimum, of output devices.

7.2.2.12.1.4 Process Protection Channel Operational Test

A channel operational test shall be the injection of a simulated signal into the channel as close to the sensor as practicable to verify operability of alarm, interlock, and/or trip functions. The channel operational test shall include adjustments, as necessary, of the alarm, interlock, and/or trip setpoints such that the setpoints are within the required range and accuracy.

7.2.2.12.1.5 Trip Actuating Device Operational Test

A trip actuating device operational test shall consist of operating the trip actuating device and verifying operability of alarm, interlock, and/or trip functions. The trip actuating device operational test shall include adjustment, as necessary, of the trip actuating device such that it actuates at the required setpoint within the required accuracy.

7.2.2.12.1.6 Reactor Trip System Response Time

The RTS response time shall be the time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of stationary gripper coil voltage.

7.2.2.13 Current System Drawings

The current system drawings for the RTS and supporting systems are presented in Figures 7.2-1 through 7.2-6, and 7.3-1 through 7.3-52.

7.2.3 SAFETY EVALUATION

7.2.3.1 General Design Criterion 2, 1967 – Performance Standards

The RTS is located in the auxiliary building, which is a PG&E Design Class I structure. The auxiliary building is designed to withstand the effects of winds and tornadoes (refer to Section 3.3), floods and tsunamis (refer to Section 3.4), external missiles (refer to Section 3.5), and earthquakes (refer to Section 3.7) to protect the RTS and ensure its design function will be performed. Externally exposed equipment is evaluated in Section 3.3.2.3.2.6.

The seismic design considerations for the RTS are discussed in Section 3.10.
A discussion of the seismic testing of the RTS equipment is presented in Section 3.10.3.

The monitoring circuitry, sensors and signal electronics, for several variables that provide inputs to the RTS are not seismically qualified, and in some cases, are not seismically mounted or classified as PG&E Design Class I. Those circuits are:

(1) Source range (SR) nuclear instrumentation - sensors and electronics (PG&E Design Class I)

(2) Intermediate range (IR) nuclear instrumentation - sensors and electronics (PG&E Design Class I)

(3) Main turbine stop valve closed limit switches (PG&E Design Class II)

(4) Main turbine auto-stop oil pressure switches (PG&E Design Class II)

(5) 12-kV bus underfrequency relays, potential transformers and test switches (PG&E Design Class II)

(6) 12-kV bus undervoltage relays, potential transformers and test switches (PG&E Design Class II)

(7) 12-kV reactor coolant pump circuit breaker open position switches (PG&E Design Class II)

Analyses have been performed to assure that the lack of seismic qualification and seismic installation of these inputs will not degrade the function of the RTS. The electrical circuits that provide the inputs to the RTS from these monitoring channels all are classified as PG&E Design Class I, Class 1E circuits. These analyses are based upon the following:

(1) *SR and IR Nuclear Instrumentation* - The DCPP safety analysis does not take credit for the SR or IR nuclear instrumentation as a primary reactor trip function. The safety analysis is bounded by credit taken for the seismically qualified power range nuclear instrumentation. Although the SR and IR nuclear instrumentation sensors and electronics are not seismically qualified, the SR and IR electronics drawers that provide the inputs to the RTS are seismically mounted in a seismically qualified cabinet. Therefore, no seismically induced common mode failures of the SR or IR nuclear instrumentation drawers exist that could degrade the RTS safety function.

(2) *Main Turbine Stop Valve Closed Limit Switches* - The main turbine stop valve closed limit switches provide inputs to the RTS to signal a turbine tripped (loss of heat sink) condition. These inputs are secondary (backup) reactor trip signals. The stop valve limit switches and field termination cabinets have been seismically analyzed to confirm that the structural integrity of the limit switches and field termination cabinets are such that no

seismically induced common mode failures of the main turbine stop valve closed limit switches or field termination cabinets exist that could degrade a primary RTS safety function.

(3) *Main Turbine Auto-Stop Oil Pressure Switches* - The main turbine auto-stop oil pressure switches provide inputs to the RTS to signal a turbine tripped (loss of heat sink) condition. These inputs are secondary (backup) reactor trip signals. The auto-stop oil pressure switches and the cabinet have been seismically analyzed to confirm that the structural integrity of the pressure switches and cabinet to which they are mounted is such that no seismically induced common mode failures of the pressure switches or cabinet exist that could degrade a primary RTS safety function.

(4) *12-kV System RTS Input Signals* - The 12-kV undervoltage (UV) circuits, underfrequency (UF) circuits and breaker open position switches provide inputs from the 12-kV system to the RTS to signal a loss of reactor coolant flow condition. The UV and UF inputs are backup reactor trip signals. The breaker open position inputs are also backup reactor trip signals. These circuits individually do not meet the RTS seismic qualification or mounting requirements. The UF circuits do not meet the fail-safe criterion. However, when analyzed as a "system," the 12-kV inputs to the RTS fail in such a manner as to assure a reactor trip should the equipment be subjected to an RTS design basis seismic event. In addition, the UV, UF and breaker position switch monitoring circuits and the equipment in which they are mounted have been seismically analyzed to confirm that their structural integrity is such that no seismically induced common mode failures of the monitoring circuits or the equipment in which they are mounted exist that could degrade an RTS safety function.

7.2.3.2 General Design Criterion 11, 1967 – Control Room

Controls and instrumentation related to RTS include control room status lights, annunciator displays and RTB switches on the control board with indicating lights to display breakers' position. Additionally, the reactor trip and bypass breakers can be operated locally.

7.2.3.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The RTS keeps surveillance on process variables that are directly related to equipment mechanical limitations such as pressure, pressurizer water level (to prevent water discharge through safety valves and uncovering heaters), and also on variables that directly affect the heat transfer capability of the reactor (e.g., flow and reactor coolant temperatures). Other parameters utilized in the RTS are calculated from various process variables. In any event, whenever a direct process or a calculated variable exceeds a setpoint, the reactor will be shut down to protect against either gross damage to fuel

cladding or loss of system integrity that could lead to release of radioactive fission products into the containment.

While most setpoints used in the RTS are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the RTS have been selected either on the basis of applicable engineering code requirements or engineering design studies. Methodologies for determining RTS setpoint and allowable values are presented in WCAP-11082, Technical Specification 3.3.1, or in plant procedures. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required to allow for uncertainties and instrument errors.

7.2.3.4 General Design Criterion 14, 1967 – Core Protection Systems

The RTS, together with associated equipment, is designed to act automatically to prevent or to suppress conditions that could result in exceeding acceptable fuel damage limits.

Operation below the applicable DNBR limit could result in excessive cladding temperature because of the onset of DNB and the resultant sharp reduction in heat transfer coefficient. Fuel centerline melting occurs when the local LHR, or power peaking, in a region of the fuel is high enough to cause the fuel centerline temperature to reach the melting point of the fuel. The core safety limits are established to prevent overheating of the fuel and cladding as well as possible cladding perforation. Figure 15.1-1 presents the allowable reactor coolant loop average temperature and ΔT for the design flow and the NSSS Design Thermal Power distribution as a function of primary coolant pressure. Refer to Section 15.1 for additional information.

DNBR is not a directly measurable quantity; however, the process variables that are statistically related to DNBR are sensed and evaluated. Small isolated changes in various process variables may not individually result in violation of a core safety limit, whereas the combined variation over sufficient time may cause the overpower or overtemperature safety limit to be exceeded. The design concept of the RTS takes cognizance of this situation by providing reactor trips associated with individual process variables in addition to the overpower and overtemperature safety limit trips. The process variable trips prevent reactor operation whenever a change in the monitored value is such that a core or system safety limit is in danger of being exceeded should operation continue. Basically, the high-pressure, low-pressure, and overpower and overtemperature ΔT trips provide sufficient protection for slow transients, as opposed to such trips as low flow or high flux, which trip the reactor for rapid changes in flow or flux, respectively, that could result in fuel damage before actuation of the slower responding ΔT channels.

Therefore, the RTS has been designed to provide protection for fuel cladding and RCS pressure boundary integrity where: (a) a rapid change in a single variable or factor that will quickly result in exceeding a core or a system safety limit, and (b) a slow change in

one or more variables has an integrated effect that causes safety limits to be exceeded. Overall, the RTS offers diverse and comprehensive protection against fuel cladding failure and/or loss of RCS integrity. Technical Specification Table 3.3.1-1 lists information related to the reactor trip system instrumentation safety limits and safety system settings. The limiting safety system settings are defined in Technical Specification Table 3.3.1-1 as the Allowable Values. The capability of the RTS to prevent loss of integrity of the fuel cladding and/or RCS pressure boundary during Condition II transients is demonstrated in Section 15.2. A reactor trip is credited for certain Condition III and IV events as described in Sections 15.3. and 15.4.

7.2.3.5 General Design Criterion 19, 1967 – Protection Systems Reliability

The protection systems are designed for high functional reliability and inservice testability. Each design employs redundant logic trains and measurement and equipment diversity. Sufficient redundancy is provided to enable individual end-to-end channel tests with each reactor at power without compromise of the protective function. Built-in semiautomatic testers provide means to test the majority of system components very rapidly.

The RTS uses sensors that feed the process circuitry consisting of two to four redundant channels, which monitor various plant parameters. The RTS also contains the logic circuitry necessary to automatically open the reactor trip breakers. The logic circuitry consists of two redundant logic trains that receive input from the protection channels.

Each of the two logic trains, A and B, is capable of opening a separate and independent reactor trip breaker (52/RTA and 52/RTB).

7.2.3.6 General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence

Sufficient redundancy and independence is designed into the protection systems to ensure that neither single failure nor removal from service of any component or channel of a system will result in loss of the protection function.

Each individual channel is assigned to one of four channel designations, e.g., Channel I, II, III, or IV, refer to Figure 7.2-5. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant process equipment is separated by locating electronics in different protection rack sets. Each redundant channel is energized from a separate ac power feed.

Position Regarding Separation of Isolated Signal Outputs within Process Protection Racks

It is PG&E's position that specific physical separation is not required within the process protection racks between the protection circuits and isolated nonprotection circuits, and that the degree of electrical separation plus the physical separation associated with the insulation on the wires is sufficient to meet the requirements of IEEE 279-1971.

The justification for this position is that IEEE 279-1971 covers this situation in three paragraphs quoted below:

> 4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required.
>
> 4.6 Channel Independence. Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.
>
> 4.7.2 Isolated Devices. The transmission of signals from protection system equipment for control system use shall be through isolation devices, which shall be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design base.
>
> Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible ac and dc potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the protection system.

The intent of 4.2 and 4.6 with regard to protection signals is handled through a combination of electrical and physical separation. The electrical separation is handled by supplying each protection rack set with separate independent sources of power. Physical separation is provided by locating redundant channels in separate racks sets. Thus separation, both electrical and physical, outside the rack is ensured. The intent of 4.7.2 is met within the process protection racks by the provision of qualified isolators that have been tested and verified to perform properly under the credible failures listed in 4.7.2. The isolator is designed to be an electrical barrier between protection and nonprotection and, as such, the degree of physical separation provided within the modules is that which is consistent with the voltages involved.

The question of whether or not specific physical separation is required is best addressed by reviewing the potential hazards involved. There are three general categories of

hazards that must be protected against. These are missiles, electrical faults, and fire. Missiles external to the rack can be ruled out on the basis that the racks are located in general plant areas where it is not credible to assume missiles capable of penetrating the steel rack. (Refer to Section 3.5) Missiles within the rack can be ruled out on the basis that there is no mechanism within the racks for the generation of missiles with sufficient energy to cause damage to the hardware or wiring.

Electrical faults within a rack constitute a single failure. Since there is no internal mechanism capable of simultaneously causing such a failure in more than one protection set, the result is acceptable. The plant remains safe with three out of the four protection sets remaining in operation. A few very specific electrical faults, external to the protection racks, on the signals derived from protection channels may have access to the outputs of all protection sets simultaneously. However, the isolators have been shown to prevent these disturbances from entering the protection circuits; thus the results are acceptable.

Fire external to the racks is a potential hazard; however, fire retardant paint and wiring, fire barriers at the rack entrances, and adequate separation external to the racks provide a satisfactory defense against the hazard. For further discussions on fire protection, refer to Sections 8.3.1.2 and 9.5.1. A potential cause of fire within more than one protection set is an electrical fault involving the nonprotection outputs from these sets; however, it has been verified during the isolator tests that the fault current is terminated by the failure of certain components with no damage occurring in the wiring leading to the module. Thus, a fire within a rack set due to high current igniting or otherwise damaging the wiring is not possible.

The remaining source of fire within the racks - a short circuit within the protection wiring-effects only one protection set and thus is acceptable since three of the four protection sets remain.

It is thus established that no credible failure associated with the isolator output wiring violates the single failure criterion; therefore, the present method of rack wiring is entirely adequate.

7.2.3.7 General Design Criterion 21, 1967 – Single Failure Definition

The protection system is designed to provide two, three, or four instrumentation channels for each protective function and redundant (two) logic trains. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required.

To prevent the occurrence of common mode failures, such additional measures as functional diversity, testing, as well as administrative control during design, production, installation, and operation are employed, as discussed in Reference 11, for protection logic. Standard reliability engineering techniques were used to assess the likelihood of

trip failure due to random component failures. Common mode failures were also qualitatively investigated. It was concluded from the evaluation that the likelihood of no trip following initiation of Condition II events is extremely small (2×10^{-7} derived for random component failures). The solid-state protection system design has been evaluated by the same methods as used for the relay system and the same order of magnitude of reliability is provided.

7.2.3.8 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

The protection system is designed to be independent of the control system. In certain applications, the control signals and other nonprotective functions are derived from individual protective channels through isolation devices. The isolation devices are classified as part of the protection system and are located in the process protection racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation devices are designed so that a short circuit, open circuit, or the application of 118-Vac or 140-Vdc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation devices are never returned to the protective racks.

A detailed discussion of the design and testing of the isolation devices is provided in References 8, 9, and 32. These reports include the results of applying various malfunction conditions on the output portion of the isolation devices. The results show that no significant disturbance to the isolation devices input signal occurred.

To provide additional assurance that the electrical wiring to and from the isolators, as installed, would not permit control-side faults to enter the protection system through input-output electrical coupling, tests were conducted at DCPP using voltages of 118-Vac, 250-Vdc, 460-Vac, 580-Vac and electrical noise. A description of these tests is provided in References 8, 12, and 32.

Where failure of a protection system component can cause a process excursion that requires protective action, the protection system can withstand another independent failure without loss of protective action. The steam generator low-low water level protective function relies upon two-out-of-three (2/3) trip logic. The digital feedwater control system (DFWCS) uses the same steam generator level sensors as the steam generator low-low water level protective function. The DFWCS includes the median signal selector (MSS) and the Steam Flow Arbitrator (SFA). The installation of the MSS and SFA eliminates the possibility that failure of the instrument tap shared between one narrow-range level channel and one steam flow channel on each steam generator will cause a transient that would require protective action by any of the level channels. The MSS prevents the resulting failed high narrow range level signal from causing a level transient via the level portion of the DFWCS. The SFA prevents the resulting failed low steam flow signal from causing a level transient via the feed forward mass balance portion of the DFWCS. (Refer to Section 7.2.2.11.5) For details refer to Reference 27.

7.2.3.9 General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems

Physical separation and electrical isolation of redundant channels and subsystems are employed in the RTS as defenses against functional failure through exposure to common causative factors.

Information from both logic trains is transmitted to the plant control boards and computer using a multiplex system. To ensure separation of the signals from each train, each signal is passed through an optically-coupled isolator. Verification tests on these isolators using voltages of 118-Vac and 250-Vdc are described in Reference 12.

To provide physical separation between input and output circuits in the solid-state protection system racks, physical barriers have been provided to separate input and output wire bundles.

Independence of the logic trains is discussed in Reference 6. Two reactor trip breakers are actuated by two separate logic matrices that interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all control rod drive mechanisms, permitting the rods to free-fall into the core. The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in Reference 1. Generally, two or more diverse protection functions would terminate the accident conditions before intolerable consequences could occur.

For a discussion of the tests made to verify the performance requirements, refer to Section 3.11.

7.2.3.10 General Design Criterion 24, 1967 – Emergency Power for Protection Systems

The instrumentation and controls portions of the protection systems are supplied initially from the station batteries and subsequently from the emergency diesel generators. A single failure of any one component will not prevent the required functioning of the RTS.

7.2.3.11 General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems

The RTS is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to ensure complete system operation. The process protection equipment is designed to permit any channel to be maintained in a bypassed condition and, when required, tested during power operation without initiating a protective action at

the system level. This is accomplished without lifting electrical leads or installing temporary jumpers.

If a protection channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room.

The operability of the process sensors is ascertained by comparison with redundant channels monitoring the same process variables or those with a fixed known relationship to the parameter being checked. The in-containment process sensors can be calibrated during plant shutdown, if required.

Surveillance testing of the process protection system is performed with the use of a Man Machine Interface (MMI) test system. The MMI is used to enter instructions to the installed test processor in the process protection rack being tested which then generates the appropriate test signals to verify proper channel operation. The capability is provided to test in either partial trip mode or bypass mode where the channel comparators are maintained in the not-tripped state during the testing. Testing in bypass is allowed by the plant Technical Specifications. The bypass condition is continuously indicated in the control room via an annunciator.

The power range channels of the nuclear instrumentation system are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, because the power range channel logic is two-out-of-four, bypass of this reactor trip function is not required. Note, however, that the source and intermediate-range high neutron flux trips must be bypassed during testing.

To test a power range channel, a TEST-OPERATE switch is provided to require deliberate operator action. Operation of the switch initiates the CHANNEL TEST annunciator in the control room. Bistable operation is tested by increasing the test signal level up to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights.

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bistable trips. No provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation system detector. A nuclear instrumentation system channel that causes a reactor trip through one-out-of-two protection logic (source or intermediate range) is provided with a bypass function, which prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing testing. These bypasses initiate an alarm in the control room.

For a detailed description of the nuclear instrumentation system, refer to Reference 2.

The logic trains of the RTS are designed to be capable of complete testing at power, except for those trips listed in Section 7.2.3.17. Annunciation is provided in the control room to indicate when a train is in test, when a reactor trip is bypassed, and when a reactor trip breaker is bypassed. Details of the logic system testing are provided in Reference 6.

The reactor coolant pump breakers cannot be tripped at power without causing a plant upset by loss of power to a coolant pump. However, the reactor coolant pump breaker trip logic and continuity through the shunt trip coil can be tested at power. Manual trip cannot be tested at power without causing a reactor trip, because operation of either manual trip switch actuates both trains A and B. Note, however, that manual trip could also be initiated from outside the control room by manually tripping one of the reactor trip breakers. Initiating safety injection cannot be done at power without upsetting normal plant operation. However, the logic for these trips is testable at power.

7.2.3.12 General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design

The PPS channels are designed so that upon loss of electrical power to any channel, the output of that channel is a trip signal. The following exceptions to GDC 26, 1967 are applicable to DCPP:

1. The RCP bus underfrequency trip channels are an exception to the fail-safe design requirement. The RCP bus underfrequency trip function, in conjunction with the RCP bus undervoltage function, provides a fail-safe protective function.

2. The seismic trip channels are an exception to the fail-safe design. Since no credit is taken in accident analyses for the seismic trip, the seismic trip channels are designed energize-to-actuate to eliminate the possibility of spurious trips.

7.2.3.13 General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction

The RTS and its function, reactor shutdown by RCCA insertion, is completely independent of the normal control function, since the trip breakers interrupt power to the drive mechanisms regardless of existing control signals. The protection system is designed to limit reactivity transients so that DNBR will exceed the applicable limit value (refer to Sections 4.4.4.1 and 4.4.3.3) for any single malfunction in either reactor control system.

The analysis presented in Chapter 15 shows that for postulated dilution during refueling, startup, or manual or automatic operation at power, the operator has ample time to determine the cause of dilution, terminate the source of dilution, and initiate reboration before the shutdown margin is lost. The facility reactivity control systems are discussed further in Chapter 7, and analyses of the effects of the other possible malfunctions are

discussed in Chapter 15. The analyses show that acceptable fuel damage limits are not exceeded in the event of a single malfunction of either system.

7.2.3.14 General Design Criterion 49, 1967 – Containment Design Basis

The RTS instrumentation circuits routed through containment electrical penetrations are designed to support the containment design basis as described in Section 7.2.4.2.

7.2.3.15 Reactor Trip System Safety Function Requirements

(1) Protection from Missiles

The provisions taken to protect the RTS from missiles resulting from plant equipment failures and from events and conditions outside the plant are discussed in Section 3.5.

(2) Protection Against High Energy Pipe Rupture Effects

The provisions taken to protect the RTS from damage that might result from dynamic effects associated with a postulated rupture of high-energy piping are discussed in Section 3.6.

(3) Protection from Moderate Energy Pipe Rupture Effects – Outside Containment

The provisions taken to provide protection of the RTS system portion located outside containment from the effects of moderate energy pipe failure are discussed in Section 3.6.

(4) Protection from Jet Impingement – Inside Containment

The provisions taken to provide protection of the RTS system portion located inside containment from the effects of jet impingement which may result from high energy pipe rupture are discussed in Section 3.6.

(5) Protection from Flooding Effects – Outside Containment

The provisions taken to provide protection of the RTS system portion located outside containment from flooding that might result from the effects associated with a postulated rupture of piping are discussed in Section 3.6.

7.2.3.16 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The Class 1E RTS instrument cables required to function in harsh environments under accident conditions are qualified to the applicable environmental conditions to ensure that they will continue to perform their safety functions. Section 3.11 describes the DCPP EQ program and the requirements for the environmental design of the electrical

and related mechanical equipment. The affected components are listed on the EQ Master List.

7.2.3.17 Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions

Periodic testing of the RTS actuation functions, as described, complies with AEC Safety Guide 22, February 1972 (Reference 22). Under the present design, there are protection functions that are not tested at power. These are:

(1) Generation of a reactor trip by tripping the reactor coolant pump breakers

(2) Generation of a reactor trip by tripping the turbine

(3) Generation of a reactor trip by use of the manual trip switch

(4) Generation of a reactor trip by actuating the safety injection system

(5) Generation of a reactor trip by general warning circuitry (both redundant trains)

(6) Generation of a reactor trip by closing both reactor trip bypass breakers

The actuation logic for the functions listed is tested as described in Section 7.2.2.12. As required by Safety Guide 22, February 1972, where equipment is not tested during reactor operation, it has been determined that:

(1) There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant.

(2) The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation.

(3) The equipment can be routinely tested when the reactor is shut down.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the train in test. Test circuitry does not allow two trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.

7.2.3.18 NUREG-0737 (Items II.K.3.10 and II.K.3.12), November 1980 – Clarification of TMI Action Plan Requirements

Item II.K.3.10 – Proposed Anticipatory Trip Modification: The setpoint for the anticipatory reactor trip on turbine trip bypass (P-9) cannot be raised above 10% reactor power until it has been shown that the probability of a small-break loss-of-coolant accident (LOCA) resulting from a stuck-open power-operated relief valve (PORV) is substantially unaffected by the modification. DCPP raised P-9 to 50% with prior approval of the NRC after meeting this requirement. Refer also to Section 7.2.2.2.2.

Item II.K.3.12 – Anticipatory Reactor Trip upon Turbine Trip: The RTS includes an anticipatory reactor trip upon turbine trip for DCPP Unit 1 and Unit 2.

7.2.3.19 Generic Letter 83-28 (Actions 4.3 and 4.5), July 1983 – Required Actions Based on Generic Implications of Salem ATWS Events

Action 4.3 -- RTS Reliability (Automatic Actuation of Shunt Trip Attachment for Westinghouse and B&W Plants). The shunt trip was added to the reactor trip and bypass breakers.

Action 4.5 – RTS Reliability (System Functional Testing). The RTS is designed to allow on-line functional testing of the reactor trip system and this on-line testing includes independent testing of the undervoltage and shunt trip attachments of the reactor trip breakers. The intervals for on-line testing of the RTS are consistent with achieving high RTS availability.

7.2.4 COMPLIANCE WITH IEEE STANDARDS

7.2.4.1 Compliance with IEEE 279-1971

The RTS meets the requirements of IEEE 279-1971 as indicated below. SSPS was designed prior to IEEE 279-1971; however, its design has been approved by the NRC.

7.2.4.1.1 General Functional Requirement

The following are the generating station conditions requiring reactor trip:

(1) DNBR approaching the applicable limit value (Refer to Sections 4.4.4.1 and 4.4.3.3)

(2) Power density (kilowatts per foot) approaching rated value for Condition II faults (Refer to Sections 4.2.1, 4.3.2 and 4.4.2 for fuel design limits)

(3) RCS overpressure creating stressing approaching the limits specified in Sections 5.2 and 5.5

For a discussion of energy supply and environmental variations, refer to Sections 8.3.1.1.5 and 3.11.

The following is a list of the malfunctions, accidents, or other unusual events that could physically damage RTS components or cause environmental changes. The UFSAR sections noted with each item present discussions on the provisions made to retain the necessary protective action.

(1) Loss-of-coolant accident (Refer to Sections 15.3.1, 15.3.4, and 15.4.1)

(2) Steam breaks (Refer to Sections 15.3.2 and 15.4.2)

(3) Earthquake (Refer to Sections 2.5, 3.2, 3.7, and 3.8)

(4) Fire (Refer to Section 9.5)

(5) Explosion (hydrogen buildup inside containment; refer to Sections 6.2 and 15.4)

(6) Missiles (Refer to Section 3.5)

(7) Flood (Refer to Sections 2.4 and 3.4)

(8) Wind (Refer to Section 3.3)

The performance requirements are:

(1) System Response Times

The RTS response time shall be the time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of stationary gripper coil voltage. The RTS response times shall be demonstrated as required by the Technical Specifications.

Maximum allowable time delays in generating the reactor trip signal are identified in the Equipment Control Guidelines.

(2) Reactor trip setpoint allowable values are provided in the Technical Specifications.

(3) RTS ranges:

RTS range is the output range for a device that provides input to the RTS. It is defined as the range for which the device is calibrated and verified to be operable. As described in Sections 7.2.2.10 and 7.2.3.3, methodologies for determining RTS setpoint and allowable values are

presented in WCAP-11082, Technical Specification 3.3.1 or in plant procedures. Specific device ranges are presented in plant procedures.

RTS	Range
(a) Power range nuclear power	1 to 120% rated thermal power (RTP)
(b) Neutron flux rates	+5 to +30% of full power
(c) Overtemperature ΔT	
$T_{hot\ leg}$	530 to 650°F
$T_{cold\ leg}$	510 to 630°F
T_{avg}	530 to 630°F
Pressurizer pressure	1250 to 2500 psig
ΔI	-60 to +60%
f_1 (ΔI)	1 to 3%/%ΔI
ΔT setpoint	0 to 150% power
(d) Overpower ΔT	
$T_{hot\ leg}$	530 to 650°F
$T_{cold\ leg}$	510 to 630°F
T_{avg}	510 to 630°F
ΔI	-60 to +60%
f_2 (ΔI)	1 to 3%/%ΔI
ΔT setpoint	0 to 150 % power
(e) Pressurizer pressure	1250 to 2500 psig
(f) Pressurizer water level	Entire cylindrical portion of pressurizer (0 - 100 %)
(g) Reactor coolant flow	0 to 120% of rated flow
(h) Reactor coolant pump bus	50 to 70 Hz underfrequency
(i) Reactor coolant pump	0 to 150 Vac bus voltage
(j) Low-low steam generator water level	0 to 45% of narrow-range span

7.2.4.1.2 Single Failure Criterion

Refer to Section 7.2.3.7 for a discussion regarding the single failure criterion for RTS.

7.2.4.1.3 Quality of Components and Modules

For a discussion on the quality assurance program for the components and modules used in the RTS, refer to Chapter 17 and Section 3.1.2.1.

7.2.4.1.4 Equipment Qualification

Portions of the RTS are designated PG&E Design Class I. Refer to Sections 7.2.3.15 and 3.11 for a discussion on Class 1E electrical equipment environmental qualification and compliance to IEEE 323-1971 (Reference 14). Documentation of the Environmental and Seismic qualification of the process protection system is provided in References 23, 24, 25, 26 and 34.

7.2.4.1.5 Channel Integrity

The RTS channels are designed to maintain necessary functional capability under extremes of conditions related to environment, (refer to Section 7.2.3.1), energy supply (refer to Section 7.2.3.10), malfunctions (refer to Section 7.2.3.7), and accidents (refer to Section 7.2.4.1.1).

7.2.4.1.6 Channel Independence

Refer to Section 7.2.3.6 for a discussion regarding RTS channel independence.

7.2.4.1.7 Control and Protection System Interaction

Refer to Section 7.2.2.11 for a discussion regarding RTS control and protection interaction.

7.2.4.1.8 Derivation of System Inputs

The following are the variables required to be monitored in order to provide reactor trips (refer to Figure 7.2-1 and Table 7.2-1):

(1) Neutron flux

(2) Reactor coolant temperature

(3) RCS pressure (pressurizer pressure)

(4) Pressurizer water level

(5) Reactor coolant flow

(6) Reactor coolant pump operational status (bus voltage and frequency, and breaker position)

(7) Steam generator water level

(8) Turbine operational status (autostop oil pressure and stop valve position)

Reactor coolant temperature is a spatially dependent variable. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot leg and electronically averaging these samples in the process protection system.

7.2.4.1.9 Capability for Sensor Checks

The RTS provides a means for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation. This is accomplished by channel checks as described in Section 7.2.2.12.1.1, Channel Checks.

7.2.4.1.10 Capability for Test and Calibration

The reactor protection system is capable of testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals. Testing of the logic trains of the reactor protection system includes a check of the input relays and a logic matrix check. The following sequence is used to test the system:

(1) Check of Input Relays - During testing of the process instrumentation system and nuclear instrumentation system comparators, each channel comparator is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. The contact that creates the reactor trip also causes a status lamp and an annunciator on the control board to operate. Either train A or B input relay operation lights the status lamp and sounds the annunciator.

Each train contains a multiplexing test switch. This switch is normally configured such that train A is in the A+B position, while train B is in the Normal position. Administrative controls are used to control this configuration and may be changed to other configurations as necessary to meet plant conditions. The A+B position alternately allows information to be transmitted from the two trains to the control board. A steady-status lamp and annunciator indicates that input relays in both trains have been deenergized. A flashing lamp means that both input relays in the two trains did not deenergize. Contact inputs to the logic protection system, such as

reactor coolant pump bus underfrequency relays, operate input relays that are tested by operating the remote contacts as previously described and using the same indications as those provided for bistable input relays.

Actuation of the input relays provides the overlap between the testing of the logic protection system and the testing of those systems supplying the inputs to the logic protection system. Test indications are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two-out-of-four channels trip becomes a one-out-of-three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

(2) Check of Logic Matrices - Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. Details of semiautomatic tester operation are provided in Reference 6. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is tripped or is verified in the tripped state to check closure of the input error inhibit switch contacts.

With the exception of the P-8 blocking function, the logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same points electrically that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature should not respond mechanically.

Because the P-8 block of the one of four RCS low flow trip is not connected to the semiautomatic tester, it is tested using the manual input function pushbuttons. The P-8 block function is verified in accordance with the Surveillance Frequency Control Program.

Test indications that are provided are an annunciator in the control room indicating that reactor trips from the train have been blocked and that the train is being tested, and green and red lamps on the semiautomatic tester to indicate a good or bad logic matrix test. Protection capability provided during this portion of the test is from the train not being tested.

The general design features and details of the testability of the logic system are described in Reference 6.

(3) Testing of Reactor Trip Breakers - Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers, thereby eliminating the need to bypass them during the testing, although the associated bypass breaker is closed to preclude an inadvertent reactor trip and to allow reactor trip breaker testing. The following procedure describes the method used for testing the trip breakers:

(a) Bypass breaker 52/BYB is racked to test position and closed

(b) With bypass breaker 52/BYA racked out (test position), manually close and trip it to verify its operation

(c) Rack in and close 52/BYA (bypasses 52/RTA)

(d) While blocking 52/RTA shunt trip, manually trip 52/RTA and 52/BYB through a protection system logic matrix

(e) Reset 52/RTA

(f) Manually trip 52/RTA using the shunt trip coil only with the shunt trip test push button

(g) Reset 52/RTA

(h) Rack out 52/BYB

(i) Trip and rack out 52/BYA

(j) Repeat above steps to test trip breaker 52/RTB and bypass breaker 52/BYA using bypass breaker 52/BYB to bypass 52/RTB

Auxiliary contacts of the bypass breakers are connected so that if either train is placed in test while the bypass breaker of the other train is fully racked in and closed, both reactor trip breakers and the bypass breaker automatically trip.

Auxiliary contacts of the bypass breakers are also connected in such a way that if an attempt is made to fully rack in and close the bypass breaker in one train while the bypass breaker of the other train is already fully racked in and closed, both bypass breakers automatically trip. Additionally, trip

signals will be sent to both reactor trip and bypass breakers through the protection system logic.

The train A and train B alarm systems operate an annunciator in the control room. The two bypass breakers also operate an annunciator in the control room. Bypassing of a protection train with either the bypass or the test switches results in audible and visual indications.

The complete RTS is normally required to be in service. However, to permit on-line testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a Technical Specification defining the minimum number of operable channels and the minimum degree of channel redundancy has been formulated. This Technical Specification also defines the required restriction to operation in the event that the channel operability and degree of redundancy requirements cannot be met.

The RTS is designed in such a way that some components' response time tests can only be performed during shutdown. However, the safety analyses utilize conservative numbers for trip channel response times. The measured channel response times are compared with those used in the safety evaluations.

Refer to Sections 7.2.2.12, 7.2.2.12.1.2, and 7.3.4.1.5 for additional discussion.

7.2.4.1.11 Channel Bypass or Removal from Operation

The Eagle 21 process protection system is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. Use of the bypass mode disables the individual channel comparator trip circuitry that forces the associated logic input relays to remain in the non-tripped state until the "bypass" is removed. If the process protection channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room. During such operation, the process protection system continues to satisfy the single failure criterion. This is acceptable since there are 4 channels and the two-out-of-four trip logic reduces to two-out-of-three during the test. For functions that use two-out-of-three logic, it is implicitly accepted that the single failure criterion is met because of the results of the system reliability study. From the results of this it was concluded that the Eagle 21 digital system availability is equivalent to the respective analog process protection system availability even without the incorporation of the redundancy, automatic surveillance testing, self-calibration and self diagnostic features of the Eagle 21 process protection system.

The following exception to IEEE 279-1971 is applicable to DCPP:

> Technical Specifications allow a temporary relaxation, up to 4 hours, of the single failure criterion for the “one-out-of-two” function, reactor trip on SI signal, during channel bypass for surveillance testing provided the other train is operable.

7.2.4.1.12 Operating Bypasses

A listing of the operating bypasses is included in Table 7.2-2. These bypasses meet the requirement of Paragraph 4.12 of IEEE 279-1971 that the bypass will be removed automatically whenever permissive conditions are not met. The SSPS is used to achieve automatic removal of the bypass of a protective function.

> Note: The term "bypass" is defined as the meeting of the coincident permissive (interlock) logic to permit the protective logic to become enabled/disabled as required. The term "bypass," in this section is not intended to be defined as the disabling of the individual channel comparator trip circuitry during routine test or surveillance that forces the associated logic input relays to remain in the non-tripped state until the "bypass" is removed.

7.2.4.1.13 Indication of Bypasses

Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

7.2.4.1.14 Access to Means for Bypassing

The design provides for administrative control of access to the means for manually bypassing channels or protective functions. For details refer to References 23 and 24.

7.2.4.1.15 Multiple Set Points

For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protective system circuits are designed to provide positive means or administrative control to ensure that the more restrictive trip setpoint is used. The SSPS logic is used to prevent improper use of less restrictive trip settings.

7.2.4.1.16 Completion of Protective Action Once It Is Initiated

The RTS is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

7.2.4.1.17 Manual Initiation

Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment. Additionally, the reactor trip and bypass breakers can be operated locally.

7.2.4.1.18 Access to Set Point Adjustments, Calibration, and Test Points

The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, and test points. For details refer to References 23 and 34.

7.2.4.1.19 Identification of Protective Actions

The system provides annunciator, status light, and computer input signals that indicate the condition of bistable input signals, partial- and full-trip functions, and the status of the various blocking, permissive, and actuation functions.

7.2.4.1.20 Information Read-out

The RTS provides the operator with complete information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) that cause a reactor trip are either indicated or recorded for every channel including all neutron flux power range currents (top detector, bottom detector, algebraic difference, and average of bottom and top detector currents).

Any reactor trip actuates an annunciator.

Annunciators are also used to alert the operator of deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel actuates an annunciator.

7.2.4.1.21 System Repair

The RTS design features allow for recognition, location, replacement, and repair or adjustment of malfunctioning components or modules as discussed in References 3, 23 and 34.

7.2.4.1.22 Identification

The identification described in Section 7.1.3.3 provides immediate and unambiguous identification of the protection equipment.

7.2.4.2 Compliance with IEEE 317-1971

RTS instrumentation cables which are routed through containment penetrations are designed to meet IEEE 317-1971. Circuits without direct in-line redundant protection have been analyzed, which determined the available fault current is not of sufficient magnitude to damage the penetration conductor or penetration. These circuits will not adversely heat the penetrations as presently designed. (Refer to Section 8.3.1.4.8).

7.2.4.3 Evaluation of Compliance with IEEE 344-1971

The seismic testing, as discussed in Section 3.10.2, conforms to IEEE 344-1971 (Reference 17) except the format of the documentation may not meet the requirements because testing was completed prior to issuance of the standard. Documentation of the Environmental and Seismic qualification of the process protection system is provided in References 23, 24, 25, 26 and 34.

7.2.4.4 Evaluation of Compliance with IEEE 603-1980

IEEE 603-1980 (Reference 28), which is endorsed by Regulatory Guide 1.153, December 1985 (Reference 30), is applicable to the Eagle 21 Design, Verification, and Validation Plan.

7.2.4.5 Evaluation of Compliance with ANSI/IEEE-ANS-7-4.3.2-1982

ANSI/IEEE-ANS-7-4.3.2-1982 (Reference 31), which is endorsed by Regulatory Guide 1.152, November 1985 (Reference 29), is applicable to the Eagle 21 Design, Verification, and Validation Plan.

7.2.5 REFERENCES

1. T. W. T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306, April 1969.

2. J. B. Lipchak, and R.A. Stokes, Nuclear Instrumentation System, WCAP-7669, April 1971.

3. J. A. Nay, Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, WCAP-7671, April 1971.

4. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

5. D. N. Katz, Solid State Logic Protection System Description, WCAP-7488L, January 1971.

6. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

7. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers.

8. J. P. Doyle, Noise, Fault, Surge, and Radio Frequency Interference Test Report for Westinghouse Eagle-21 Process Protection Upgrade System, WCAP-11733, June 1988 (W Proprietary Class 2).

9. R. Bartholomew and J. Lipchak, Test Report, Nuclear Instrumentation System Isolation Amplifier, WCAP-7819, Rev. 1, January 1972.

10. Deleted

11. W. C. Gangloff, An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors, WCAP-7486, May 1971.

12. D. N. Katz, et al., Westinghouse Protection Systems Noise Tests, WCAP-12358, Revision 2, October 1975 (W Proprietary Class 3).

13. IEEE Standard 308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 334-1971, Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, The Institute of Electrical and Electronics Engineers Inc.

17. IEEE Standard 344-1971, Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

18. Deleted

19. Deleted

20. Deleted in Revision 15.

21. IEEE Standard 344-1975, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

22. Safety Guide 22, Periodic Testing of Protection System Actuation Functions, USAEC, February, 1972.

23. Summary Report EAGLE 21 Process Protection System Upgrade for Diablo Canyon Power Plant Units 1 and 2, WCAP-12813, Revision 3, June 1993.

24. R. B. Miller, Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety-Related Electrical Equipment, WCAP-8587, W Proprietary Class 3.

25. Equipment Qualification Data Package, WCAP-8587, Supplement 1, EQDP-SE-9A and 69B, W Proprietary Class 3.

26. Equipment Qualification Test Report, WCAP-8687, Supplement 2-E69A and 69B, W Proprietary Class 2.

27. Advanced Digital Feedwater Control System Input Signal Validation for Pacific Gas and Electric Company Diablo Canyon Units 1 and 2, WCAP-12221 W Proprietary Class 3, April 1997 (PGE-97-540) and WCAP-12222 W Proprietary Class 3, March 1989.

28. IEEE Standard 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

29. Regulatory Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems in Nuclear Plants, November 1985.

30. Regulatory Guide 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems, December 1985.

31. ANSI/IEEE-ANS 7-4.3.2, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations, 1982.

32. C. N. Nasrallah, Noise, Fault, Surge, and Radio Frequency Interference Test Report - Westinghouse Eagle-21 Digital Family as Used in QDPS, PSMS, RVLIS, and ICCM, WCAP-11340, November 1986.

33. DCP 1000000354, Allow Replacement of SSPS Printed Circuit Boards, June 2010.

34. WCAP-13423, Eric, L.E., “Topical Report Diablo Canyon Units 1 and 2 Eagle 21 Microprocessor-Based Process Protection System,” (Proprietary), October 1992.

7.2.6 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

The ESFAS senses selected plant parameters and initiates necessary safety systems to protect against violating core design limits and the RCS pressure boundary and to mitigate accidents. If the measured value of a sensed parameter exceeds a predetermined setpoint, a signal is sent into logic matrices sensitive to combinations indicative of faults described in Chapter 15. Once the required logic combination is completed, the system sends actuation signals to those ESFs components whose aggregate function best serves the requirements of the accident. Included in this section are the electrical schematic diagrams for all ESF systems circuits and supporting systems. Figure 7.3-52 shows containment electrical penetrations, cable trays, and supports.

7.3.1 DESIGN BASES

7.3.1.1 General Design Criterion 2, 1967 – Performance Standards

ESFAS is designed to withstand the effects of or is protected against natural phenomena, such as earthquakes, tornadoes, flooding, winds, tsunamis, and other local site effects.

7.3.1.2 General Design Criterion 11, 1967 – Control Room

ESFAS is designed to or contains instrumentation and controls that support actions to maintain the safe operational status of the plant from the control room.

7.3.1.3 General Design Criterion 15, 1967 – Engineered Safety Features Protection Systems

ESFAS provides instrumentation for sensing accident situations and initiating the operation of necessary ESFs.

7.3.1.4 General Design Criterion 19, 1967 – Protection Systems Reliability

ESFAS is designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

7.3.1.5 General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence

Redundancy and independence are designed into the ESFAS sufficient to assure that no single failure or removal from service of any component or channel of a system will result in loss of the protection function. The redundancy provided includes, as a minimum, two channels of protection for each protection function served.

7.3.1.6 General Design Criterion 21, 1967 – Single Failure Definition

ESFAS is designed to perform its function after sustaining a single failure. Multiple failures resulting from a single event shall be treated as a single failure.

7.3.1.7 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

ESFAS is designed such that protection functions are separated from control instrumentation functions to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels.

7.3.1.8 General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems

ESFAS is designed such that the effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of an accident, does not result in loss of the protection function.

7.3.1.9 General Design Criterion 24, 1967 – Emergency Power for Protection Systems

ESFAS is designed such that in the event of loss of all offsite power, sufficient alternate sources of power are provided to permit the required functioning of the protection systems.

7.3.1.10 General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems

ESFAS includes means for testing protection systems while the reactor is in operation to demonstrate that no failure or loss of redundancy has occurred.

7.3.1.11 General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design

The ESFAS is designed to fail into a safe state or into a state defined as tolerable on a defined basis if conditions such as disconnection of the system, loss of electric power, or adverse environments are experienced.

7.3.1.12 General Design Criterion 37, 1967 – Engineered Safety Features Basis for Design

ESFAS is designed to actuate the ESFs provided to back up the safety provided by the core design, the reactor coolant pressure boundary, and their protection systems.

7.3.1.13 General Design Criterion 38, 1967 – Reliability and Testability of Engineered Safety Features

ESFAS is designed to provide high functional reliability and ready testability.

7.3.1.14 General Design Criterion 40, 1967 – Missile Protection

ESFAS is protected against dynamic effects and missiles that might result from plant equipment failures.

7.3.1.15 General Design Criterion 48, 1967 – Testing of Operational Sequence of Emergency Core Cooling Systems

ESFAS is designed with the capability to test under conditions as close to design as practical the full operational sequence that brings the ECCS into action, including the transfer to alternate power sources.

7.3.1.16 General Design Criterion 49, 1967 – Containment Design Basis

The ESFAS circuits routed through containment electrical penetrations are designed so that the containment structure can accommodate, without exceeding the design leakage rate, the pressures and temperatures resulting from the largest credible energy release following a LOCA.

7.3.1.17 Engineered Safety Features Actuation System Safety Function Requirements

(1) Protection from Jet Impingement – Inside Containment

The ESFAS system portion located inside containment is designed to be protected against the effects of jet impingement which may result from high energy pipe rupture.

7.3.1.18 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The ESFAS electric components that require EQ are qualified to the requirements of 10 CFR 50.49.

7.3.1.19 Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions

The ESFAS are periodically tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program conforms to Safety Guide 22, February 1972.

7.3.2 SYSTEM DESCRIPTION

7.3.2.1 Functional Design

The following summarizes those generating station conditions requiring protective action:

(1) Primary system

(a) Rupture in small pipes or crack in large pipes (refer to Section 15.3.1)

(b) Rupture of a reactor coolant pipe - LOCA (refer to Section 15.4.1)

(c) SG tube rupture (refer to Section 15.4.3)

(2) Secondary system

(a) Minor secondary system pipe break resulting in steam release rates equivalent to the actuation of a single dump, relief, or safety valve (refer to Section 15.2.14)

(b) Rupture of a major secondary system pipe (refer to Section 15.4.2)

The following summarizes the generating station variables required to be monitored for the initiation of the ESF for each accident in the preceding list:

(1) Rupture in small pipes or crack in large primary system pipes

(a) Pressurizer pressure

(b) Containment pressure

(2) Rupture of a reactor coolant pipe LOCA

(a) Pressurizer pressure

(b) Containment pressure

(3) SG tube rupture

(a) Pressurizer pressure

(4) Minor or major secondary system pipe rupture

(a) Pressurizer pressure

(b) Steam line pressures

(c) Steam line pressure rate

(d) Containment pressure

7.3.2.2 Signal Computation

The ESFAS consists of two discrete portions of circuitry: (a) a process protection portion consisting of three to four redundant channels that monitor various plant parameters and containment pressures, and (b) a logic portion consisting of two redundant logic trains that receive inputs from the process protection channels and perform the needed logic to actuate the ESF. Each logic train is capable of actuating the ESF equipment required. The intent is that any single failure within the ESFAS shall not prevent system action when required.

The redundancy concept is applied to the process protection and logic portions of the system. Separation of redundant process protection channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks, terminating at the redundant groups of ESF logic racks as shown in Figure 7.3-50. This conforms to GDC 20, 1967 (refer to Section 7.3.3.5).

Section 7.2 provides further details on protection instrumentation. The same design philosophy applies to both systems and conforms to GDC 19, 1967; GDC 20, 1967; GDC 22, 1967; and GDC 23, 1967 (refer to Sections 7.3.3.4, 7.3.3.5, 7.3.3.7, and 7.3.3.8).

The variables are sensed by the process protection circuitry, as discussed in Reference 2 and in Section 7.2. The outputs from the process protection channels are combined into actuation logic as shown on Sheets 9 and 10, 11 and 12, 13 and 14, 15 and 16 of Figure 7.2-1. Tables 7.3-1 and 7.3-2 provide additional information pertaining to logic and function.

The interlocks associated with the ESFAS are outlined in Table 7.3-3. These interlocks satisfy the functional requirements discussed in Section 7.3.2.1

7.3.2.3 Devices Requiring Actuation

The following are the actions that the ESFAS initiates when performing its function:

(1) Safety injection (SI pumps, RHR pumps, charging pumps)

(2) Reactor trip

(3) Feedwater line isolation by closing all main feedwater regulating valves (MFRVs), feedwater bypass valves, main feedwater isolation valves (MFIVs) and tripping the feedwater pumps.

(4) AFW system actuation

(5) Auxiliary saltwater (ASW) pump start

(6) Automatic containment spray (spray pumps, sodium hydroxide tank)

(7) Containment isolation

(8) Containment fan coolers start

(9) EDG startup

(10) Main steam line isolation

(11) Turbine and generator trips

(12) Control room isolation

(13) Component cooling water (CCW) pump start

(14) Trip RHR pumps on low refueling water storage tank (RWST) level

Refer to Figure 7.3-50 for a complete list of actuated components.

7.3.2.4 Implementation of Functional Design

7.3.2.4.1 Process Protection Circuitry

The process protection sensors and racks for the ESFAS are covered in References 2, 17, 72 and 73. Discussed in these reports are the parameters to be measured including pressures, tank and vessel water levels, as well as the measurement and signal transmission considerations. These latter considerations include the basic current signal transmission system, transmitters, RTDs, and pneumatics. Other considerations covered are automatic calculations, signal conditioning, and location and mounting of the devices.

The sensors monitoring the primary system are located as shown on the piping schematic diagram, Figure 3.2-7, Reactor Coolant System. The secondary system sensor locations are shown on the piping schematic diagram, Figure 3.2-4, Turbine Steam Supply System.

Containment pressure is sensed by four physically separated DP transmitters mounted outside of the containment structure. The transmitters are connected to containment atmosphere by filled and sealed hydraulic transmission systems similar to the sealed

pressurizer water level reference leg described in Section 7.2.2.11.4. Refer to Section 6.2.4.4.2.2 for additional information on instrument lines penetrating containment.

Three water level instrumentation channels are provided for the RWST. Each channel provides independent indication on the main control board, thus meeting the requirements of Paragraph 4.20 of IEEE 279-1971 (Reference 4). Two-out-of-three logic is provided for RHR pump trip and low-level alarm initiation. One channel provides low-low-level alarm initiation; another channel provides a high-level alarm to alert the operator of overfill and potential spillage of radioactive material. Refer to Sections 3.10.3.5 and 6.3.3.4.4.1 for additional information on the RWST level circuits and logic relays.

7.3.2.4.2 Logic Circuitry

The ESF logic racks are discussed in detail in Reference 5. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 5 also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation, and provisions for ensuring instrument qualification. The outputs from the process protection channels are combined into ESF actuation logic, as shown on Sheets 9 and 10 (RCP bus UV), 11 and 12 (pressurizer pressure), 13 and 14 (steam pressure rate, steamline pressure, and SG level), and 15 and 16 (ESF actuation and containment pressure) of Figure 7.2-1.

To facilitate ESF actuation testing, two cabinets (one per train) are provided that enable operation, to the maximum practical extent, of safety features loads on a group-by-group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in Section 7.3.4.1.5.8.

7.3.2.4.3 Final Actuation Circuitry

The outputs of the solid-state logic protection system (the slave relays) are energized to actuate, as are most final actuators and actuated devices. These devices are:

(1) SI System Pumps and Valve Actuators - Refer to Section 6.3 for flow diagrams and additional information.

(2) Containment Isolation - Phase A - T signal isolates all nonessential (to reactor operation) process lines on receipt of SI signal; Phase B - P signal isolates remaining process lines (which do not include SI lines) on receipt of a two-out-of-four high-high containment pressure signal. For further information, refer to Section 6.2.4.

(3) Containment Fan Coolers - Refer to Section 6.2.2.3.

(4) Component Cooling Pumps and Valves - Refer to Section 9.2.2.

(5) ASW Pumps - Refer to Section 9.2.7.

(6) AFW Pumps Start - Refer to Section 6.5.5.

(7) Diesel Generators Start - Refer to Section 8.3.1.1.3.3.5.2.

(8) Feedwater Isolation - Refer to Section 10.4.7.

(9) Ventilation Isolation Valve and Damper Actuators - Refer to Section 6.2.4.

(10) Steam Line Isolation Valve Actuators - Refer to Section 10.3.2.

(11) Containment Spray Pumps and Valve Actuators - Refer to Section 6.2.2.3.

When the ESF loads are to be powered by diesel generators, they must be sequenced to prevent overloading. This sequencing is discussed in Section 8.3.1.1.3.3.5.2.

The following systems are required for support of the ESFs:

(1) ASW System - Heat removal, refer to Section 9.2.7.

(2) CCW System - Heat removal, refer to Section 9.2.2.

(3) Electrical Power Distribution Systems - Refer to Chapter 8.

7.3.2.4.4 Safety System Status Display

The following provisions have been made to automatically display the status of safety systems.

(1) Monitor light display panels are provided to verify correct system alignment for:

(a) Safety feature valves

(b) Phase A isolation system equipment

(c) SI, charging (CCP1 and CCP2), CCW, AFW, ASW, and RHR pumps

(d) Phase B isolation system equipment and containment spray pumps

(e) Containment fan coolers

(2) A partial list of annunciator displays is included in Section 7.7.2.10.1.1.1:

In addition to the status lights and annunciator displays described, system control switches on the control board are provided with indicating lights to display valve position and motor status with power potential indicating lights provided where equipment power is 480-V or higher.

The features described above, supplemented with administrative procedures, provide the operator with safety system status information, by means of which the status of bypassed or inoperable systems is available to the operator, in accordance with the intent of Regulatory Guide 1.47 (Reference 6).

7.3.2.5 Additional Design Information

The generating station conditions that require protective action are discussed in Section 7.3.2.1. The generating station variables that are required to be monitored in order to provide protective actions are also summarized in Section 7.3.2.1.

The ESFAS functional units and trip setpoints are provided in the Technical Specifications (Reference 7). The methodology for determining ESFAS setpoints and allowable values is presented in WCAP 11082 or in plant procedures.

The following is a list of the malfunctions, accidents, or other unusual events that could physically damage protection system components or could cause environmental changes. The sections noted with each item present discussions on the provisions made to retain the necessary protective action.

(1) LOCA (refer to Sections 15.3.1 and 15.4.1)

(2) Secondary System breaks (refer to Sections 15.3.2 and 15.4.2)

(3) Earthquakes (refer to Sections 2.5, 3.2, 3.7, and 3.8)

(4) Fire (refer to Section 9.5.1)

(5) Explosion (hydrogen buildup inside containment; refer to Sections 6.2 and 15.4)

(6) Missiles (refer to Section 3.5)

(7) Flood (refer to Sections 2.4 and 3.4)

(8) Wind (refer to Section 3.3)

Minimum performance requirements are:

(1) System response times

The actuation system response time is included in the overall ESF response time.

The Technical Specifications define ESF response time. Acceptance criteria for ESF response time testing is located in ECG 38.2, “Engineered Safety Features (ESF) Response Times.”

(2) System accuracies

The system actuation setpoints together with their allowable values are provided in the Technical Specifications.

(3) Ranges of sensed variables to be accommodated until conclusion of protective action is ensured

Information readouts and the ranges required in generating the required actuation signals for loss-of-coolant and secondary system pipe break protection are discussed in Section 7.5.1 and presented in Tables 7.5-1 and 7.5-2.

7.3.2.6 Current System Drawings

The schematic diagrams and logic diagrams for ESF circuits and supporting systems are presented at the end of Chapter 7 (refer to Figures 7.3-1 through 7.3-49).

7.3.3 SAFETY EVALUATION

7.3.3.1 General Design Criterion 2, 1967 – Performance Standards

The ESFAS structures, systems and components (SSCs) are contained in the auxiliary buildings that are PG&E Design Class I (refer to Section 3.8). These buildings are designed to withstand the effects of winds and tornadoes (refer to Section 3.3), floods and tsunamis (refer to Section 3.4), external missiles (refer to Section 3.5), earthquakes (refer to Section 3.7), and other natural phenomena to protect ESFAS SSCs to ensure their safety-related functions and designs will perform.

Refer to Section 7.3.2.5 for additional information.

7.3.3.2 General Design Criterion 11, 1967 – Control Room

Controls and instrumentation related to ESFAS include control room status lights, annunciator displays and system control switches on the control board with indicating lights to display valve position and motor status with power potential indicating lights provided where equipment power is 480-V or higher.

Refer to Section 7.3.2.4.4 for additional information.

7.3.3.3 General Design Criterion 15, 1967 – Engineered Safety Features Protection Systems

The ESFAS is designed to monitor plant variables and respond to the accident conditions identified in Section 7.3.2.1. If necessary, ESFAS will initiate the operation of the ESFs as described in Section 7.3.2.3.

The effectiveness of the ESFAS is evaluated in Chapter 15 based on the ability of the system to contain the effects of Conditions III and IV faults including loss of coolant and secondary system pipe rupture accidents. The ESFAS parameters are based on the component performance specifications that are provided by the manufacturer, or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The ESFAS must detect Conditions III and IV faults and generate signals that actuate the ESF. The system must sense the accident condition and generate the signal actuating the protection function reliably, and within a time determined by, and consistent with, the accident analyses in Sections 15.3 and 15.4. The ESFAS will mitigate other faults as discussed in Section 15.2.

The time required for the generation of the actuation signal of ESFAS is relatively short. The remainder of the time is associated with the actuation of the mechanical and fluid system equipment associated with ESF. This includes the time required for switching, bringing pumps and other equipment to speed, and the time required for them to take load.

7.3.3.3.1 Loss-of-Coolant Protection

By analysis of LOCA and in-system tests, it has been verified that except for very small coolant system breaks, which can be protected against by the charging pumps (CCP1 and CCP2) followed by an orderly shutdown, the effects of various LOCAs are reliably detected by the low pressurizer pressure. The ECCS is actuated in time to prevent or limit core damage.

For large coolant system breaks, the passive accumulators inject first because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active ECCS phase.

High containment pressure also actuates the ECCS, providing additional protection as a backup to actuation on low pressurizer pressure. Emergency core cooling actuation can be brought about upon sensing this other direct consequence of a primary system break; that is, the protection system detects the leakage of the coolant into the containment.

Containment spray provides containment pressure reduction and also limits fission product release, upon sensing elevated containment pressure (high-high), to mitigate the effects of a LOCA.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems.

The analyses in Chapter 15 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss of coolant.

7.3.3.3.2 Secondary System Pipe Rupture Protection

The ECCS is also actuated to protect against a secondary system line break. Analysis of secondary system pipe rupture accidents shows that the ECCS is actuated for a secondary system pipe rupture in time to limit or prevent further damage.

There is a reactor trip, but the core reactivity is further reduced by the highly borated water injected by the ECCS.

Additional protection against the effects of secondary system pipe rupture is provided by feedwater isolation that occurs upon actuation of the ECCS. Feedwater line isolation is initiated to prevent excessive cooldown of the reactor.

Additional protection against a secondary system pipe rupture accident is provided by closure of all steam line isolation valves to prevent uncontrolled blowdown of all SGs. Generation of the protection system signal is again short compared to the time to trip the fast acting steam line isolation valves that are designed to close in less than 5 seconds.

The analyses in Chapter 15 of the secondary system pipe rupture accidents and an evaluation of the protection system instrumentation and channel design show that the EFSAS are effective in preventing or mitigating the effects of a secondary system pipe rupture accident.

7.3.3.4 General Design Criterion 19, 1967 – Protection Systems Reliability

The ESFAS is designed for high functional reliability and in-service testability. The design employs redundant logic trains and measurement and equipment diversity. Sufficient redundancy is provided to enable individual end-to-end channel tests with each reactor at power without compromise of the protective function. Built-in semiautomatic testers provide means to test the majority of system components very rapidly.

Refer to Sections 7.3.4.1.5.1 and 7.2.3.11 for additional information.

7.3.3.5 General Design Criterion 20, 1967 – Protection Systems Redundancy and Independence

Sufficient redundancy and independence is designed into the protection systems to ensure that no single failure, or removal from service of any component or channel of a system will result in loss of the protection function. The minimum redundancy is exceeded in each protection function that is active with the reactor at power. Functional diversity and consequential location diversity are designed into the systems.

The ESF outputs from the solid-state logic protection cabinets are redundant, and the actuations associated with each train are energized to actuate, up to and including the final actuators, by the separate ac power supplies that power the respective logic trains. Mutually redundant ESF circuits utilize separate relays in separate racks.

The protection system is designed to provide two, three, or four instrumentation channels for each protective function and redundant (two) logic trains. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required.

Each individual channel is assigned to one of four channel designations, e.g., Channel I, II, III, or IV. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant process equipment is separated by locating electronics in different protection rack sets. Each redundant channel is energized from a separate ac power feed.

Refer to Sections 7.3.4.1.1 and 7.3.4.1.3 for additional information.

7.3.3.6 General Design Criterion 21, 1967 – Single Failure Definition

The protection system is designed to provide two, three, or four instrumentation channels for each protective function and redundant (two) logic trains. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required.

Refer to Section 7.3.4.1.1 for additional information.

7.3.3.7 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

The protection systems comply with the requirements of IEEE 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations (Reference 4), although construction permits for the DCPP units were issued prior to issuance of the 1971 version of the standard (refer to Section 7.3.4.1). Each protection system is separate and distinct from the respective control systems. The control system is dependent on the protection system in that control signals are derived from protection system measurements, where applicable. These signals are transferred to the control system by isolation amplifiers that are classified as protection system components. The adequacy of system isolation has been verified by testing or analysis under conditions of all postulated credible faults. Isolation devices that serve to protect PG&E Instrument Class IA instrument loops have all been tested. For certain applications where the isolator is protecting a PG&E Instrument Class IB instrument loop, and the isolation device is a simple linear device with no complex failure modes, the analysis was used to verify the adequacy of the isolation device. The failure or removal of any single control instrumentation system component or channel, or of those common to the control instrumentation system component or channel and protection circuitry, leaves intact a system that satisfies the requirements of the protection system.

To provide physical separation between input and output circuits in the solid-state protection system racks, physical barriers have been provided to separate input and output wire bundles.

The protection system is designed to be independent of the control system. In certain applications, the control signals and other non-protective functions are derived from individual protective channels through isolation devices. The isolation devices are classified as part of the protection system and are located in the process protection racks. Non-protective functions include those signals used for control, remote process indication, and computer monitoring. The isolation devices are designed so that a short circuit, open circuit, or the application of 118-Vac or 140-Vdc on the isolated output portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation devices are never returned to the protective racks.

7.3.3.8 General Design Criterion 23, 1967 – Protection Against Multiple Disability for Protection Systems

Physical separation and electrical isolation of redundant channels and subsystems, functional diversity of subsystems, and safe failure modes are employed in the design of the reactor's defenses against functional failure through exposure to common causative factors. The redundant logic trains, reactor trip breakers, and ESF actuation devices are physically separated and electrically isolated. Physically separate channel trays, conduits, and penetrations are maintained upstream from the logic elements of each train.

The protection system components have been qualified by testing under extremes of the normal environment. In addition, components are tested and qualified according to individual requirements for the adverse environment specific to their location that might result from postulated accident conditions.

Refer to Sections 7.3.4.1.2 and 7.3.4.3 for additional information.

7.3.3.9 General Design Criterion 24, 1967 – Emergency Power for Protection Systems

Emergency power for the instrumentation and control portions of the protection systems is provided initially from the station batteries, supplying dedicated 120-Vac inverters for each protection channel, and subsequently from the EDGs. A single failure of any one component will not prevent the required functioning of protection systems.

Refer to Section 8.3 for additional information.

7.3.3.10 General Design Criterion 25, 1967 – Demonstration of Functional Operability of Protection Systems

The ESFAS includes means for testing protection systems while the reactor is in operation to demonstrate that no failure or loss of redundancy has occurred.

Operating procedures normally require that the complete ESF actuation system be operable. However, redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the bypass/tripped mode.

Refer to Section 7.3.4.1.5.1 for additional information.

7.3.3.11 General Design Criterion 26, 1967 – Protection Systems Fail-Safe Design

In the ESF, a loss of instrument power to a specific channel/rack/or protection set will call for actuation of ESF equipment controlled by the specific channel that lost power (exceptions to the fail-safe design requirement are the containment spray and the radiation monitoring channels that initiate containment ventilation isolation). The actuated equipment in some cases must have power to comply. The power supply for the protection systems is discussed in Chapter 8. The containment spray function is energized to trip in order to avoid spurious actuation. In addition, manual containment spray requires simultaneous actuation of both manual controls. This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels, meeting the criteria in Reference 4. When the construction permits for the Diablo Canyon units were issued in April 1968 and December 1970, manual initiation at the system level was in compliance with paragraph 4.17 of IEEE 279-1968 (Reference 8). No single random failure in the

manual initiation circuits can prevent automatic initiation. Failure of manual initiation at the system level is not considered a significant safety problem because the operator can initiate operation manually at the component level.

Refer to Section 7.3.4.1.1 for additional information.

7.3.3.12 General Design Criterion 37, 1967 – Engineered Safety Features Basis for Design

ESFAS actuates the ESFs required to cope with any size reactor coolant pipe break up to and including the circumferential rupture of any pipe in that boundary assuming unobstructed discharge from both ends, and to cope with any steam or feedwater line break up to and including the main steam or feedwater headers. Limiting the release of fission products from the reactor fuel is accomplished by the ECCS, which, by cooling the core, keeps the fuel in place and substantially intact and limits the metal-water reaction to an acceptable amount.

7.3.3.13 General Design Criterion 38, 1967 – Reliability and Testability of Engineered Safety Features

A comprehensive program of testing has been formulated for all equipment and instrumentation vital to the functioning of the ESF. The program consists of startup tests of system components and integrated tests of the system. Periodic tests of the activation circuitry and system components, throughout the station lifetime, with maintenance performed as necessary, ensure that high reliability will be maintained and that the system will perform on demand. Details of the test program are provided in the Technical Specifications.

Refer to Section 7.3.4.1.5.1 for additional information.

7.3.3.14 General Design Criterion 40, 1967 – Missile Protection

The various sources of missiles that might affect the ESF have been identified, and protective measures have been implemented to minimize these effects (refer to Sections 3.5 and 8.3). Electrical raceways containing circuits for the ESF have not been installed in zones where provision against dynamic effects must be made, with a few exceptions. When routing through such zones was necessary, metallic conduits only were used, and conduits containing redundant circuits were separated physically as far as practical.

7.3.3.15 General Design Criterion 48, 1967 – Testing of Operational Sequence of Emergency Core Cooling Systems

The design provides for capability to test, to the extent practical, the full operational sequence up to design conditions, including transfer to alternative power sources for the ECCS, to demonstrate the state of readiness and capability of the system. This

functional test is performed with the RCS initially cold and at LP. The ECCS valve alignment is set to initially simulate the system alignment for plant power operation. Details of the ECCS are found in Section 6.3. Refer to Section 7.3.4.1.5.5 for a description of the initiation circuitry.

Refer to Section 7.3.4.1.5.1 for additional information.

7.3.3.16 General Design Criterion 49, 1967 – Containment Design Basis

ESFAS circuits routed through containment are analyzed for redundant overcurrent protection and available fault energy. ESFAS circuits routed through containment penetrations are installed without direct in-line protection. The available fault current is not of sufficient magnitude to damage the penetration conductor. These circuits will not adversely heat the penetrations as presently designed.

Refer to Section 8.3 for additional information.

7.3.3.17 Engineered Safety Features Actuation System Safety Function Requirements

(1) Protection from Jet Impingement – Inside Containment

The provisions taken to provide protection of the ESFAS system portion located inside containment from the effects of jet impingement which may result from high energy pipe rupture are discussed in Section 3.6.

7.3.3.18 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The Class 1E ESFAS SSCs required to function in harsh environments under accidents conditions are qualified to the applicable environmental conditions to ensure that they will continue to perform their safety functions. Section 3.11 describes the DCPP EQ program and the requirements for the environmental design of the electrical and related mechanical equipment. The affected components are listed on the EQ Master List.

7.3.3.19 Safety Guide 22, February 1972 – Periodic Testing of Protection System Actuation Functions

Periodic testing of the ESF actuation functions, as described, complies with Safety Guide 22, February 1972 (Reference 9). Under the present design, those protection functions that are not tested at power are discussed in Section 7.3.4.1.5.9.

As described by Safety Guide 22, February 1972, where actuated equipment is not tested during reactor operation, it has been determined that:

(1) There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant.

(2) The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation.

(3) The actuated equipment can be routinely tested when the reactor is shut down.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed, for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the control room by a common "ESF testing" annunciator for the train in test. Test circuitry does not allow two ESF trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.

The discussion on "bypass" in Section 7.2.4.1.11 is applicable.

Refer to Section 7.3.4.1.5.1 for additional information.

7.3.4 COMPLIANCE WITH IEEE STANDARDS

7.3.4.1 Evaluation of Compliance with IEEE 279-1971 – Criteria for Protection Systems for Nuclear Power Generating Stations

The ESFAS meets the criteria as set forth in IEEE 279-1971 (Reference 4), as follows:

7.3.4.1.1 Single Failure Criterion

The discussion presented in Section 7.2.3.7 is applicable to the ESFAS, with the following exception:

In the ESF, a loss of instrument power to a specific channel/rack/or protection set will call for actuation of ESF equipment controlled by the specific channel that lost power (exceptions to the fail-safe design requirement are the containment spray and the radiation monitoring channels that initiate containment ventilation isolation). The actuated equipment in some cases must have power to comply. The power supply for the protection systems is discussed in Chapter 8. The containment spray function is energized to trip in order to avoid spurious actuation. In addition, manual containment spray requires simultaneous actuation of both manual controls. This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels, meeting the criteria in Reference 4. When the construction permits for the Diablo Canyon units were issued in April 1968 and December 1970, manual initiation at the system level was in compliance

with paragraph 4.17 of IEEE 279-1968 (Reference 8). No single random failure in the manual initiation circuits can prevent automatic initiation. Failure of manual initiation at the system level is not considered a significant safety problem because the operator can initiate operation manually at the component level.

The design conforms to GDC 21, 1967 and GDC 26, 1967.

7.3.4.1.2 Equipment Qualification

The ability of the equipment inside the containment required to function for post-LOCA operation in the adverse environment associated with the LOCA or in-containment steam break, has been evaluated in Section 3.11.

Sensors for measurement of pressurizer pressure, are located inside the containment and will be exposed to the post-LOCA environment.

7.3.4.1.3 Channel Independence

The discussion presented in Section 7.2.3.6 is applicable. The ESFAS outputs from the solid-state logic protection cabinets are redundant, and the actuations associated with each train are energized to actuate, up to and including the final actuators, by the separate ac power supplies that power the respective logic trains. Mutually redundant ESFAS circuits utilize separate relays in separate racks.

7.3.4.1.4 Control and Protection System Interaction

The discussions presented in Section 7.3.3.7 are applicable.

7.3.4.1.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Section 7.2.4.1.10 are applicable to the sensors, analog circuitry and logic trains of the ESFAS.

The following sections cover those areas in which the testing provisions differ from those for the RTS.

7.3.4.1.5.1 Testing of Engineered Safety Features Actuation System

The ESFAS is tested to ensure that the systems operate as designed and function properly in the unlikely event of an accident. The testing program, which conforms with GDC 19, 1967; Criteria GDC 25 1967; GDC 38 1967; GDC 48 1967; and GDC 57 1967, and to Safety Guide 22, February 1972 (Reference 9), is as follows:

(1) Prior to initial plant operations, ESFAS tests will be conducted.

(2) Subsequent to initial startup, ESFAS tests will be conducted as required in the Technical Specifications.

(3) During on-line operation of the reactor, the ESFAS process and logic circuitry are fully tested. In addition, essentially all of the ESF final actuators can be fully tested. The few final actuators whose operation is not compatible with continued on-line plant operation are checked during refueling outages. Slave relays are tested on an interval defined in the Technical Specifications.

(4) During normal operation, the operability of testable final actuation devices of the ESFAS are tested by manual initiation from the test control panel.

The discussions on capability for testing, as presented in Section 7.2.2.12, are applicable.

7.3.4.1.5.2 Performance Test Acceptability Standard for the "S" (Safety Injection Signal) and the "P" (Automatic Demand Signal for Containment Spray Actuation) Actuation Signals Generation

During reactor operation, the acceptability of the ESFAS is based on the successful completion of the overlapping tests performed on the initiating system and the ESFAS. Checks of process indications verify operability of the sensors. Process checks and tests verify the operability of the process circuitry from the input of these circuits through the logic input relays and the inputs to the logic matrices. Solid-state logic testing checks the signal path through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays. Final actuator testing can be performed by operating the output slave relays and verifying the required ESF actuation. Actuators whose testing is not compatible with on-line operation are tested during refueling outages, except those actuators normally in their required positions, which will not be tested. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves have completed their travel.

The basis for acceptability for the ESFAS interlocks is receipt of proper indication upon introducing a trip.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground of signal cables in radiation environments, are based on qualification test data that identify what constitutes acceptable degradation, e.g., radiation and thermal.

7.3.4.1.5.3 Frequency of Performance of Engineered Safety Features Actuation Tests

During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed as required by the Technical

Specifications. Testing, including the sensors, is also performed during scheduled plant shutdown for refueling.

7.3.4.1.5.4 Engineered Safety Features Actuation Test Description

The following sections describe the testing circuitry and procedures for the on-line portion of the testing program. The guidelines used in developing the circuitry and procedures are:

(1) The test procedures must not involve the potential for damage to any plant equipment.

(2) The test procedures must minimize the potential for accidental tripping.

(3) The provisions for on-line testing must minimize complication of ESF actuation circuits so that their reliability is not degraded.

7.3.4.1.5.5 Description of Initiation Circuitry

Several systems comprise the total ESFAS, the majority of which may be initiated by different process conditions and reset independently of each other.

The remaining functions (listed in Section 7.3.2) are initiated by a common signal (SI), which in turn may be generated by different process conditions.

In addition, operation of all other vital auxiliary support systems, such as AFW, CCW, and ASW, is initiated via the ESF starting sequence actuated by the SI signal.

Each function is actuated by a logic circuit that is duplicated for each of the two redundant trains of ESF initiation circuits.

The output of each of the initiation circuits consists of a master relay, which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the solid-state logic protection cabinets designated trains A and B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor-operated valve contactors, solenoid-operated valves, start the EDG, etc.

7.3.4.1.5.6 Process Protection Testing

Process protection testing is identical to that used for reactor trip circuitry and is described in Section 7.2.4.1.10. Briefly, in the process protection racks, a man machine interface unit is used together with a rack mounted test panel to facilitate testing.

Section 7.2.3.11 discusses testing in bypass which is the normal method. Alternatively, administrative controls allow, during channel testing, that the channel output be put in a trip condition that de-energizes (operates) the input relays in train A and train B cabinets. Of necessity this is done on one channel at a time. Status lights and single

channel trip alarms in the main control room verify that the logic input relays have been deenergized and the channel outputs are in the trip mode. An exception to this is containment spray, which is energized to actuate two-out-of-four logic and reverts to two-out-of-three logic when one channel is in test.

7.3.4.1.5.7 Solid-State Logic Testing

After the individual process channel testing is complete, the logic matrices are tested from the trains A and B logic rack test panels. This step provides overlap between the process protection and logic portions of the test program. During this test, each of the logic inputs is actuated automatically in all combinations of trip and nontrip logic. Trip logic is not maintained long enough to permit master relay actuation - master relays are "pulsed" to check continuity. Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. Actuation of the master relays during this test applies low voltage to the slave relay coil circuits to allow continuity checking, but not slave relay actuation. During logic testing of one train, the other train can initiate the required ESF function. For additional details, refer to Reference 5.

7.3.4.1.5.8 Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. Slave relays do not operate because of reduced voltage.

In the next step, operation of the slave relays and the devices controlled by their contacts are checked. For this procedure, control switches mounted in the safeguards test cabinet near the logic rack area are provided for most slave relays. These controls require two deliberate actions on the part of the operator to actuate a slave relay. By operation of these relays one at a time through the control switches, all devices that can be operated on-line without risk to the plant are tested.

Devices are assigned to the slave relays to minimize undesired effects on plant operation. This procedure minimizes the possibility of upset to the plant and again ensures that overlap in the testing is continuous, since the normal power supply for the slave relays is utilized.

During this last procedure, close communication between the main control room operator and the person at the test panel is required. Before energizing a slave relay, the operator in the control room ensures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has energized the slave relay, the control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps, and annunciators on the control board. The test director, using a prepared check list, records all operations. The operator then resets all devices and prepares for operation of the next slave relay-actuated equipment.

By means of the procedure outlined above, all devices actuated by ESFAS initiation circuits can be operated by the test circuitry during on-line operation, with the following exceptions:

(1) Main steam isolation - During cold shutdowns, these valves are full stroke tested.

(2) Feedwater isolation - Air-operated, spring-closed regulating control valves and feedwater bypass valves are provided for each main feedwater line. Operation of these valves is continually monitored by normal operation. During cold shutdown, these valves are tested for closure times. MFIVs are also provided for each feedwater isolation line.

(3) RCP essential service isolation

(a) CCW supply and return. These valves cannot be fully tested during normal operation.

(b) Seal water return header. These valves cannot be fully testing during normal operation.

(4) Normal charging and normal letdown isolation. These valves cannot be fully tested during normal operation due to thermal and hydraulic transients induced on the lines.

(5) Sequential transfer of centrifugal charging pump (CCP1 and CCP2) suction from the volume control tank to the RWST for charging injection. These valves cannot be fully tested during normal operation due to reactivity transients associated with the swap. Additionally, restoration of normal charging and letdown following testing causes thermal and hydraulic transients.

(6) Autotransfer Class 1E buses to startup power or EDG.

(7) Containment spray additive tank outlet valves. These valves cannot be tested during normal operation without isolating the spray additive tank.

(8) Accumulator outlet valves. These valves are required by Technical Specifications to be open with power removed from their operators during normal operation to prevent their inadvertent closure by a spurious signal, and therefore are not tested (refer to Section 7.3.4.1.5.2).

(9) Main turbine trip.

(10) Main feedwater pump trip.

(11) Blocking of the non-ESF starts of ESF pumps during an SI signal to assure bus loading will be controlled by the ESF load sequencing timers. This circuitry cannot be fully tested during normal operation since slave relay contact position cannot be verified.

(12) Containment spray initiation circuit interlock from an SI signal. This circuit cannot be fully tested during normal operation since slave relay contact position cannot be verified.

(13) Other circuitry not associated with the ESF; for example, main generator trip, RCP trip, and SR block.

7.3.4.1.5.9 Actuator Blocking and Continuity Test Circuits

The limited number of components that cannot be operated on-line are assigned to slave relays separate from those assigned to components that can be operated on-line. For some of these components, additional blocking relays are provided that allow operation of the slave relays without actuation of the associated ESF devices. Interlocking prevents blocking the output of more than one slave relay at a time. The circuits provide for monitoring of the slave relay contacts, the devices control circuit cabling, control voltage, and the devices actuating solenoids. These slave relays and actuators may be tested using the blocking and continuity test circuits while the unit is on line; however, use of these circuits can increase the risk associated with testing, since failure of the blocking circuits may result in a reactor trip.

7.3.4.1.5.10 Time Required for Testing

The system design includes provisions for timely testing of both the process protection and logic sections of the system. Testing of actuated components (including those that can only be partially tested) is a function of control room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure, automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time, the redundant devices in the other trains would be functional.

7.3.4.1.5.11 Summary

The testing program and procedures described provide capability for checking completely from the process signal to the logic cabinets and from these to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those devices whose operation could affect plant or equipment operation, the same procedure provides for checking from the process signal to the logic rack. To check the final actuation device, the device itself is tested during

shutdown conditions. All testing is performed as required by the Technical Specifications.

The procedures require testing at various locations:

(1) Process channel testing and verification of setpoints are accomplished at the process protection racks. Verification of logic input relay operation is done at the control room status lights.

(2) Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel.

(3) Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the logic racks, in combination with the control room operator.

(4) Continuity testing for the circuits that cannot be operated is done at the same test panel mentioned in (3) above.

7.3.4.1.6 Testing During Shutdown

ECCS components and the system, including emergency power supplies, will be tested in accordance with the Technical Specifications.

Containment spray system tests are performed at each major fuel reloading. The tests are performed with the isolation valves in the spray supply lines at the containment and spray additive tank blocked closed, and are initiated manually or by using an actual or simulated actuation signal.

All final actuators can be tested during a refueling outage. The final actuators that cannot be tested during on-line operation are tested during each major fuel reloading. All testing is performed as required by the Technical Specifications.

7.3.4.1.7 Periodic Maintenance Inspections

Periodic maintenance on the system equipment is accomplished and documented according to the maintenance procedures contained in the Plant Manual. Refer to Section 13.5.1.

The balance of the requirements listed in Reference 4 (Paragraphs 4.11 through 4.22) is discussed in Section 7.2.4.1. Paragraph 4.20 receives special attention in Section 7.5.

7.3.4.2 Evaluation of Compliance with IEEE 308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations

The power supplies for the ESF equipment conform to IEEE 308-1971 (Reference 10).

Refer to Section 7.6 and Chapter 8, which discuss the power supply for the protection systems, for additional discussions on compliance with this criteria.

7.3.4.3 Evaluation of Compliance with IEEE 323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations

Refer to Section 3.11 for a discussion on ESF electrical equipment EQ and compliance to IEEE 323-1971 (Reference 11). Documentation of the environmental and seismic qualification of the process protection system is provided in References 18, 19, 20, and 21.

7.3.4.4 Evaluation of Compliance with IEEE 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems

The periodic testing of the ESF actuation system conforms to the requirements of IEEE 338-1971 (Reference 13), with the following comments:

(1) The periodic test frequency specified in the Technical Specifications was conservatively selected, using considerations in paragraph 4.3 of Reference 13, to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements.

(2) The test interval discussed in Paragraph 5.2 of Reference 13 is primarily developed on past operating experience, and modified, as necessary, to ensure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.

7.3.4.5 Evaluation of Compliance with IEEE 344-1971, Trial-Use Guide for Seismic Qualifications of Class I Electric Equipment for Nuclear Power Generating Stations

The seismic testing, as set forth in Section 3.10, conforms to the testing requirements of IEEE 344-1971 (Reference 14); however, because the IEEE standards were issued after much of the design and testing had been completed the equipment documentation may not meet the format requirements of the standards. Documentation of the environmental and seismic qualification of the process protection system is provided in References 18, 19, 20, and 21.

7.3.4.6 Evaluation of Compliance with IEEE 317-1971, Electric Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations

Refer to Section 7.2.4.2 for a discussion of conformance with IEEE 317-1971 (Reference 15). The same applies to penetrations for systems described in Section 7.3.

7.3.4.7 Evaluation of Compliance with IEEE 336-1971, Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations

Refer to Section 7.1.3.4 for a discussion of conformance with IEEE 336-1971 (Reference 16).

7.3.4.8 Eagle 21 and Process Control System Design, Verification, and Validation

The standards that are applicable to the Eagle 21 Design, Verification and Validation Plan (Reference 17) are IEEE-Standard 603-1980 (Reference 21), which was endorsed by Regulatory Guide 1.153, December 1985 (Reference 23), and ANSI/IEEE-ANS-7-4.3.2-1982 (Reference 24) which was endorsed by Regulatory Guide 1.152, November 1985 (Reference 22).

The following ESFAS related instrument signals are processed by the PCS:

(1) RHR Pump Trip on Low RWST Level (refer to Sections 6.3.3.4.4.1 and 7.3.2.4.1).

References 4, 10, 13, 16, and 27 through 71 were used for design, verification, validation, and qualification of all or portions of the safety related PCS hardware and software (encompassing Triconex components, manual/auto hand stations, signal converters/isolators and loop power supplies).

7.3.5 REFERENCES

1. Deleted in Revision 21.

2. J. A. Nay, Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, WCAP-7671, April 1971.

3. Safety Guide 11, Instrument Lines Penetrating Primary Reactor Containment, USAEC, March 1971.

4. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

5. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

6. Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, USAEC, May 1973.

7. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

8. IEEE Standard 279-1968, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

9. Safety Guide 22, Periodic Testing of Protection System Actuation Functions, USAEC, February 1972.

10. IEEE 308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

11. IEEE Standard 323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

12. Deleted in Revision 21.

13. IEEE Standard 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 344-1971, Trial-Use Guide for Seismic Qualifications of Class I Electric Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 317-1971, Electric Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard, 336-1971, Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

17. L. E. Erin, Topical Report Eagle 21 Microprocessor Based Process Protection System, WCAP-12374, September 1989.

18. R. B. Miller, Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment, WCAP-8587, Westinghouse Proprietary Class 3.

19. Equipment Qualification Data Package, WCAP-8587, Supplement 1, EQDP-ESE-69A and 69B, Westinghouse Proprietary Class 3.

20. Equipment Qualification Test Report, WCAP-8687, Supplement 2-E69A and 69B, Westinghouse Proprietary Class 2.

21. IEEE Standard 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

22. Regulatory Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety Related Systems in Nuclear Plants, November 1985.

23. Regulatory Guide 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems, December 1985.

24. ANSI/IEEE-ANS-7-4.3.2, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations, 1982.

25. Reliability Assessment of Potter & Brumfield MDR Relays, WCAP-13878, Revision 0, Westinghouse Proprietary Class 2C, June 1994.

26. Extension of Slave Relay Surveillance Test Intervals, WCAP-13900, Revision 0, Westinghouse Proprietary Class 3, April 1994.

27. IEEE Standard 323-2003, Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

28. IEEE Standard 344-1987, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

29. IEEE Standard 384-1974, Criteria for Independence of Class 1E Equipment and Circuits, Institute of Electrical and Electronics Engineers, Inc.

30. IEEE Standard 730-1998, Software Quality Assurance Plans, Institute of Electrical and Electronics Engineers, Inc.

31. IEEE Standard 828-1990, Software Configuration Management Plans, Institute of Electrical and Electronics Engineers, Inc.

32. IEEE Standard 829-1983, Software Test Documentation, Institute of Electrical and Electronics Engineers, Inc.

33. IEEE Standard 830-1993, Recommended Practice for Software Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

34. IEEE Standard 1008-1987, Software Unit Testing, Institute of Electrical and Electronics Engineers, Inc.

35. IEEE Standard 1012-1998, Software Verification and Validation, Institute of Electrical and Electronics Engineers, Inc.

36. IEEE Standard 1016-1987, Recommended Practice for Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

37. IEEE Standard 1016.1-1993, Guide to Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

38. IEEE Standard 1059-1993, Guide for Software Verification and Validation Plans, Institute of Electrical and Electronics Engineers, Inc.

39. IEEE Standard 1074-1995, Developing Software Life Cycle Processes, Institute of Electrical and Electronics Engineers, Inc.

40. IEEE Standard 1233-1998, Guide for Developing System Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

41. IEEE Standard C62.41-1991, Recommended Practice for Surge Voltages in Low Voltage AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

42. IEEE Standard C62.45-1992, Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000V and less) AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

43. IEEE Standard 7-4.3.2-2003, Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

44. EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications, Electric Power Research Institute, October, 1996.

45. EPRI TR-102323 Revision 3, Guidelines for Electromagnetic Interference Testing in Power Plants, Electric Power Research Institute, November 2004.

46. EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Electric Power Research Institute, December 1996.

47. EPRI TR-102348 Revision 1, Guideline on Licensing Digital Upgrades, Electric Power Research Institute, March 2002.

48. Regulatory Guide 1.100 Revision 2, Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants, USNRC, June 1988.

49. Regulatory Guide 1.105, Revision 3, Setpoints for Safety-Related

Instrumentation, USNRC, December 1999.

50. Regulatory Guide 1.152, Revision 1, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, USNRC, January 1996.

51. Regulatory Guide 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, February 2004.

52. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

53. Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

54. Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

55. Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

56. Regulatory Guide 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997

57. Regulatory Guide 1.180, Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, USNRC, October 2003.

58. Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, USNRC, February 1972.

59. Regulatory Guide 1.29, Revision 3, Seismic Design Classification, USNRC, September 1978.

60. Regulatory Guide 1.30, Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment, USNRC, August 1972.

61. Regulatory Guide 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, USNRC, November 1974.

62. Regulatory Guide 1.97, Revision 3, Instrumentation for Light-Water-Cooled

Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, USNRC, May 1983.

63. NUREG-0800, Appendix 7.0-A, Revision 5, Review Process for Digital Instrumentation and Control Systems, USNRC, March 2007.

64. BTP 7-14 Revision 5 Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

65. BTP 7-18 Revision 5, Guidance on the use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

66. MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility, USDOD, August 1999

67. ANSI/ANS-4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, American Nuclear Society, January 1980

68. NEMA ICS 1-2000, Industrial Control and Systems: General Requirements, National Electrical Manufacturers Association, December 2008

69. NFPA 70 (NEC) 2002 National Electric Code, National Fire Protection Association, January 2002

70. IEC 61131-3 1993, Programming Industrial Automations Systems, International Electrotechnical Commission, December 1993

71. ISA-S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation, International Society of Automation, January 1994

72. S.V. Andre, et. al, Summary Report Eagle 21 Process Protection System Upgrade for Diablo Canyon Power Plant Units 1 and 2, WCAP-12813-R3 (P) / WCAP-13615-R2 (NP), June 1993

73. L.E. Erin, Topical Report Diablo Canyon Units 1 and 2 Eagle 21 Microprocessor-Based Process Protection System, WCAP-13423, October 1992

7.3.6 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

The functions necessary for safe shutdown, defined as hot standby (MODE 3), are available from instrumentation channels that are associated with the major systems in both the primary and secondary sides of the plant. These channels are normally aligned to serve a variety of operational functions, including startup and shutdown, as well as protective functions. Prescribed procedures for securing and maintaining the plant in a safe shutdown condition can be instituted by appropriate alignment of selected systems. The discussion of these systems, together with the applicable codes, criteria, and guidelines, is included in other sections. In addition, the alignment of shutdown functions associated with the ESFs that are invoked under postulated limiting fault situations is discussed in Chapter 6 and Section 7.3.

The instrumentation and control functions that are required to be aligned for maintaining safe shutdown (MODE 3) of the reactor, which are discussed in this section, are the minimum number under nonaccident conditions. These functions permit the necessary operations to:

(1) Prevent the reactor from achieving criticality in violation of the Technical Specifications (Reference 2)

(2) Provide an adequate heat sink so that design and safety limits are not exceeded

Refer to Section 9.5.1 to determine instrumentation and controls required for safe shutdown in the event of fire.

7.4.1 DESIGN BASES

7.4.1.1 General Design Criterion 3, 1971 – Fire Protection

The instrumentation and control systems required for safe shutdown are designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.

7.4.1.2 General Design Criterion 11, 1967 – Control Room

The instrumentation and control systems required for safe shutdown are designed to support actions to maintain and control the safe operational status of the plant from the control room or from an alternate location if control room access is lost due to fire or other causes.

7.4.1.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The instrumentation and control systems required for safe shutdown are designed to monitor and maintain variables within prescribed operating ranges.

7.4.1.4 Safe Shutdown Systems Safety Function Requirements

(1) Protection from Missiles

The instrumentation and control systems required for safe shutdown are designed and located to be protected against the effects of missiles which may result from plant equipment failure and from events and conditions outside the plant.

(2) Protection Against High Energy Pipe Rupture Effects

The instrumentation and control systems required for safe shutdown are designed and located to accommodate the dynamic effects of a postulated high-energy pipe failure to the extent necessary to assure that a safe shutdown condition of the reactor can be accomplished and maintained.

(3) Protection from Moderate Energy Pipe Rupture Effects – Outside Containment

The outside containment instrumentation and control systems required for safe shutdown are designed to be protected against the effects of moderate energy pipe failure.

(4) Protection from Jet Impingement – Inside Containment

The inside containment instrumentation and control systems required for safe shutdown are designed to be protected against the effects of jet impingement which may result from high energy pipe rupture.

(5) Protection from Flooding Effects – Outside Containment

The outside containment instrumentation and control systems required for safe shutdown are to be protected from the effects of internal flooding.

7.4.2 DESCRIPTION

The designation of systems used for safe shutdown depends on identifying those systems that provide the following capabilities for maintaining a safe shutdown (MODE 3):

(1) Boration

(2) Adequate supply of AFW

(3) Decay heat removal

These systems are identified in the following sections, together with the associated instrumentation and controls provisions. The design basis information for these

systems, as required by IEEE 279-1971 (Reference 3), is provided in other sections herein. For convenience, cross-referencing to these other sections is provided.

In the event that safe shutdown from outside of the control room is required, remote instrumentation, controls, and transfer switches are required for the following functions to maintain safe shutdown (MODE 3):

(1) Reactor trip indication

(2) RCS pressure control

(3) Decay heat removal via the AFW system and the SG safety valves

(4) RCS inventory control via charging flow

(5) Safety support systems for the above functions, including ASW, CCW, and EDGs

Instrumentation and controls required to fulfill these functions are described in the following sections. Other instrumentation and controls provided for cold shutdown (MODE 5) and operator convenience are also identified but are not required for safe shutdown (MODE 3).

7.4.2.1 Safe Shutdown Equipment

7.4.2.1.1 Monitoring Indicators

The characteristics of the monitoring indicators that are provided inside and outside, the control room are described in Section 7.5. The necessary safe shutdown (MODE 3) indications are:

(1) Water level indications for each SG

(2) Pressure indication for each SG

(3) Pressurizer water level indication

(4) Pressurizer pressure indication

(5) Condensate storage tank level indication

(6) RCS temperature indication for loop 1 or, loop 4 hot leg and cold leg

(7) AFW flow indication

(8) Charging flow indication

(9) Reactor trip breaker indication

All indications external to the control room are provided at the hot shutdown panel except for the RCS temperature indication (which is provided at the dedicated shutdown panel) and the reactor trip breaker indication (which is provided at the trip breaker switchgear). The dedicated shutdown panel is described in Section 7.5.2.7.

In addition, other remote shutdown indications are provided for operator convenience at the hot shutdown panel (refer to Figure 7.7-30) but not required for safe shutdown (MODE 3).

7.4.2.1.2 Controls

Controls utilized for obtaining and maintaining safe shutdown (MODE 3) are addressed below.

7.4.2.1.2.1 General Considerations

(1) The turbine is tripped from the control room (note that this can also be accomplished at the turbine).

(2) The reactor is tripped from the control room (note that this can also be accomplished at the reactor trip switchgear).

(3) All automatic systems continue functioning (refer to Sections 7.2 and 7.7).

Safe shutdown (MODE 3) is a stable plant condition automatically reached following a plant shutdown. The safe shutdown condition can be safely maintained for an extended time.

In addition, the SI signal trip circuit must be defeated and the accumulator isolation valves closed.

(4) For motor-driven equipment that must be operated from outside the control room due to control room evacuation, controls are provided at the hot shutdown panel. A control transfer switch is provided at the 4.16-kV or 480-V switchgear to directly transfer control to the hot shutdown panel for some equipment. For other equipment, a control transfer switch is provided at the hot shutdown panel to transfer control to that panel. Transfer of control is interlocked with a permissive switch that is located at the motor control center. This interlock is provided to permit isolation of the hot shutdown panel to prevent spurious actions in the event of a fire in or at the hot shutdown panel.

Three methods of transfer control are employed:

(a) For one set of redundant equipment, the permissive switch is normally closed, permitting transfer of control to the hot shutdown panel when the control transfer switch is operated. Abnormal permissive switch alignment or transfer of control is annunciated in the control room.

(b) For the second set of redundant equipment, the permissive switch is normally open, permitting transfer of control by operating the transfer switch only after closing the permissive switch. Abnormal permissive switch alignment is annunciated in the control room.

(c) For the third set of redundant equipment, the transfer switch on the 4.16-kV or 480 V switchgear permits the transfer of control to the hot shutdown panel. Transfer of control is annunciated in the control room.

7.4.2.1.2.2 Pumps, Fan Coolers, and Ventilation Systems

To maintain safe shutdown (MODE 3) conditions from inside or outside of the control room, controls and transfer switches are required for the AFW pumps, centrifugal charging pumps (CCP1 and CCP2), ASW pumps and the CCW pumps. Other controls are available for "operational convenience" but are not required for safe shutdown. The controls for the required pumps and other equipment are described below.

(1) AFW Pumps - In the event of a main feedwater pump stoppage due to a loss of electric power, the motor-driven and turbine-driven AFW pumps start automatically (these pumps can also be started manually). Motor-driven AFW pump start and stop motor controls are located on the hot shutdown panel, in the 4.16-kV switchgear rooms, and in the control room (refer to Figures 7.3-8 and 7.3-17). Controls for the steam supply valve to the turbine-driven AFW pump are located on the hot shutdown panel and in the control room (refer to Figure 7.3-18).

(2) Centrifugal Charging and Boric Acid Transfer Pumps - Start and stop motor controls are provided for these pumps. The controls for the centrifugal charging pumps (CCP1 and CCP2) and the boric acid transfer pumps are located on the hot shutdown panel, as well as in the control room. Additionally, the charging pumps can be started and stopped in the 4.16-kV switchgear rooms. (For charging pumps, refer to Figures 7.3-3, 7.3-4, and 7.3-29. For boric acid transfer pumps, refer to Figures 7.3-13 and 7.3-30, Sheet 2.)

(3) ASW Pumps - These pumps restart automatically following a loss of normal electric power. Start and stop motor controls are located on the

hot shutdown panel, in the 4.16-kV switchgear rooms, as well as in the control room (refer to Figures 7.3-5 and 7.3-28).

(4) CCW Pumps - These pumps restart automatically following a loss of normal electric power. Start and stop motor controls are located on the hot shutdown panel, in the 4.16-kV switchgear rooms, as well as in the control room (refer to Figures 7.3-7 and 7.3-27).

(5) Reactor Containment Fan Cooler Units - These units restart automatically following a loss of normal electric power. Start and stop motor controls with a selector switch are provided for the fan motors. The controls are located on the hot shutdown panel, as well as in the control room (refer to Figures 7.3-6 and 7.3-31).

(6) Control Room Heating, Ventilation and Air-Conditioning System (includes fans and dampers) - A start and stop switch is located in the control room for the fan(s). Also, a control to open or close the inlet air damper(s) is located near the dampers. When placed in automatic control, the inlet air dampers are designed to position automatically to meet the requirements of the mode of operation of the system.

(7) Auxiliary Building Ventilation System - Operation of the system can be initiated from the ventilation control board in the control room. The system is designed to automatically shift to meet the requirements of the mode of operation of the system.

(8) Fuel Handling Building Ventilation System (Provides ventilation for the AFW pumps) - Operation of the system can be initiated from the control room. Normally, the system operates with one set of supply and exhaust fans. In the event of failure of an operating fan, the redundant fan is designed to start automatically.

(9) 4.16-kV Switchgear Room Ventilation System - Operation of the system can be initiated from the locally mounted control switches. The system is automatically started by a thermostat located in the associated safety-related room.

(10) 125-Vdc and 480-V Switchgear Room Ventilation System - Operation of the system can be initiated from the locally mounted control switches.

7.4.2.1.2.3 Valves

To maintain safe shutdown (MODE 3) conditions from inside or outside of the control room, control of AFW system level control valves is required. Other controls are available for "operational convenience" but are not required for safe shutdown. The

controls for the AFW valves and other remotely operated valves with controls external to the control room are described below.

(1) Letdown Orifice Isolation Valves - Open and close controls for these valves are located on the hot shutdown panel . These controls duplicate functions that are inside the control room (refer to Figure 7.3-45, Sheet 1).

(2) AFW Control Valves - Manual control is provided on the hot shutdown panel that duplicates functions inside the control room (refer to Figure 7.3-14).

(3) Condenser Steam Dump and Atmospheric Steam Relief Valves - The condenser steam dump and atmospheric relief valves are automatically controlled. In addition to local and control room control, the 10 percent atmospheric dump valves can be manually controlled at the hot shutdown panel. Manual control is provided locally as well as inside the control room for the atmospheric relief valves. Steam dump to the condenser is blocked on high condenser pressure. Cut-out switches allow de-energizing steam generator 3 and 4, 10 percent atmospheric steam dump valve solenoids if they spuriously energize in a fire.

(4) Charging Flow Control Valves - Controls for the emergency borate valve (refer to Figure 7.3-34) and charging pump discharge header flow control valves are located on the hot shutdown panel in addition to the control room. Controls for a pressurizer auxiliary spray valve are located at the dedicated shutdown panel in addition to the control room (refer to Figure 7.3-45, Sheet 1).

(5) Pressurizer Power Operated Relief Valves - Emergency close controls for these valves are provided on the hot shutdown panel in addition to control from the control room (refer to Figure 7.3-21).

(6) Chemical and Volume Control System Valves – Controls for charging line isolation valves and charging to loop 4 isolation valve are located at the hot shutdown panel in addition to the control room (refer to Figures 7.3-34 and 7.3-45).

(7) Safety Injection System Valves – Controls for RWST to charging pump suction header valve are located at the hot shutdown panel in addition to the control room (refer to Figure 7.3-33).

7.4.2.1.2.4 Pressurizer Heater Control

The pressurizer heaters are normally controlled from the control room. On-off control is provided on the hot shutdown panel for two backup heater groups. The control is grouped with the charging flow controls and duplicates functions available in the control room. These controls are for "operational convenience" but are not required for safe shutdown (MODE 3).

7.4.2.1.2.5 Diesel Generators

These units are started automatically on a SI, loss of voltage on either the offsite source or the Class 1E buses, or on degraded bus voltage on the Class 1E buses. Manual controls for diesel starting and control are provided at the main control room and also locally at the diesel generators. Additional description is provided in Section 8.3.

7.4.2.1.3 Maintenance of Safe Shutdown (MODE 3) Conditions Using Remote Shutdown Instrumentation and Controls

The normal and preferred location to operate the plant from is the control room. However, in the event that the control room becomes inaccessible, the operators can establish remote control and place the unit in safe shutdown (MODE 3). Remote Shutdown System Technical Specifications (Reference 2) have been established to ensure the operability of the remote shutdown instrumentation and controls.

To establish and maintain safe shutdown (MODE 3) conditions from outside of the control room, the reactor must be tripped, decay heat must be removed, and the RCS temperature, pressure, and inventory must be controlled. Additionally, systems required to support equipment performing these functions must be operable. The following provides a discussion of the minimum functions required to establish and maintain safe shutdown (MODE 3) conditions from outside of the control room until a cooldown is initiated or control is transferred back to the control room.

(1) Reactor Trip - Core subcriticality is achieved by tripping the reactor. The reactor can be tripped from outside the control room by opening the reactor trip breakers at the reactor trip switchgear. Reactor trip indication is provided from outside the control room by the reactor trip breaker position. The insertion of the control rods during a reactor trip provides the negative reactivity needed to establish and maintain safe shutdown (MODE 3) conditions until such time that either control is returned to the control room or a cooldown is initiated.

(2) Decay Heat Removal via the AFW System and the SG Safety Valves - Heat removal from the RCS is accomplished by transferring heat to the secondary plant through the SGs. The decay heat is then removed from the SGs via boiling and steam release through the SG code safety valves.

Indication of secondary heat sink is provided by SG pressure indication, SG wide range level indication, and AFW flow indication at the hot shutdown panel. Indication is also provided at the hot shutdown panel for steam generator 3 and 4 cold calibrated narrow range levels. The hot shutdown panel also provides indication of condensate storage tank level to allow monitoring of water available to supply the suction of the AFW pumps for extended operation at safe shutdown (MODE 3).

To ensure that SG level remains within its expected range, the AFW pump and level control valves are controllable from the hot shutdown panel. Upon initiation of a reactor trip, SG level will decrease due to shrink and the trip of the main feedwater pumps. The AFW pumps supply feedwater to the SGs to compensate for the loss of main feedwater. After the level in the SGs recovers, the feedwater supply to the SGs must be controlled to prevent the SGs from overfilling and overcooling the RCS, which could result in a SI. The feedwater flow can be controlled from the hot shutdown panel by using the AFW level control valves or by starting and stopping the AFW pumps. AFW flow indication is provided to aid in flow control.

To monitor the rate of heat removal from the core during all plant conditions, including a loss of offsite power, indications of RCS hot and cold leg temperature indication are required. Loop 1 RCS hot and cold leg temperature indication is available at the dedicated shutdown panel. Loop 4 RCS wide range hot and cold leg temperature indications are available at the hot shutdown panel.

(3) RCS Pressure Control - Indication of RCS pressure is provided by the pressurizer pressure indication located at the hot shutdown panel. An indication of RCS loop 4 hot leg pressure is also provided at the hot shutdown panel. RCS overpressure protection is provided by the pressurizer code safety valves. Although pressurizer heaters would assist in controlling RCS pressure, they are not required to maintain RCS pressure control.

(4) RCS Inventory Control via Charging Flow - Indication of RCS inventory is provided by the pressurizer level indication located at the hot shutdown panel. Level control is necessary to prevent the loss of level in the pressurizer and the subsequent loss of RCS pressure control, to prevent the RCS from achieving a solid water condition where pressure would no longer be readily controllable, and to prevent the core from being uncovered due to low level.

The hot shutdown panel contains controls to start and stop each centrifugal charging pump (CCP1 and CCP2). The charging pumps not only supply water to the RCS for pressurizer level control, but also provide water to the RCP seals. By starting and stopping the charging pumps,

pressurizer level can be controlled. During any time when the charging pumps are shut off, RCP seal degradation would be prevented by reactor coolant flowing past the thermal barrier heat exchanger (HX), which is cooled by CCW flow, and out of the RCP seals. This would also remove water injected into the RCS that may have caused an increase in pressurizer level.

(5) Safety Support Systems - In order for the above equipment to perform its intended safety function, it must have power and be cooled. Heat removal can be accomplished via the CCW and ASW systems. The CCW system removes heat from the lube oil and seals of the ESF pumps. The ASW removes heat from the CCW system and rejects it to the ultimate heat sink. Both the CCW pumps and the ASW pumps can be started from the hot shutdown panel. Although the CCW and ASW pumps are normally in operation and are designed to auto-start, pump controls at the hot shutdown panel ensure that the pumps are available in the event that they do not start automatically.

To ensure that power is available to ESF equipment, EDGs are available to supply power in the event that offsite power is unavailable. Although the EDGs should auto-start during a loss of offsite power, local manual controls for diesel starting and control provide additional assurance that power will be available to the ESF equipment required to establish and maintain hot safe shutdown
(MODE 3) conditions.

(6) Additional Controls Provided for Operational Convenience - Controls are also provided at the hot shutdown panel to manipulate charging flow, the 10 percent atmospheric dump valves, the containment fan cooler units, the pressurizer heaters, the pressurizer PORVs, and the letdown orifice isolation valves. Controls are provided at the dedicated shutdown panel for pressurizer auxiliary spray. These controls are provided as an operational convenience.

The above evaluation demonstrates that the reactor can be maintained in a safe condition.

7.4.2.1.4 Process Control System

The PCS performs the same design functions as the original PCS. Some of the instrumentation and control functions described in this chapter are processed by the PCS. References 3 through 52 were used for design, verification, validation, and qualification of all or portions of the PG&E Design Class I PCS hardware and software (encompassing Triconex components, manual/auto hand stations, signal converters/isolators and loop power supplies).

7.4.2.2 Equipment, Services, and Approximate Time Required After Incident that Requires Hot Shutdown (MODE 4)

(1) AFW pumps - required if main feedwater pumps are not operating. For loss of plant ac power, the turbine-driven AFW pump starts automatically within 1 minute (refer to Section 6.5).

(2) Reactor containment fan cooler units - within 15 minutes (refer to Chapter 6)

(3) EDGs - loaded within 1 minute (refer to Section 8.3).

(4) Lighting in the areas of plant required during this condition - immediately (refer to Section 8.3).

(5) Pressurizer heaters - within 8 hours (refer to Section 5.5.9).

(6) Communication network - to be available for prompt use between the hot shutdown panel area and the following areas:

(a) Outside telephone exchange

(b) Boric acid transfer pump

(c) EDGs

(d) Switchgear room

(e) Steam relief valves

(f) Dedicated shutdown panel

7.4.2.3 Equipment and Systems Available for Cold Shutdown (MODE 5)

(1) Reactor coolant pump (not available after loss of offsite power; refer to Section 5.5.1)

(2) Auxiliary feedwater pumps (refer to Section 6.5.3.5)

(3) Boric acid transfer pump (refer to Section 9.3.4)

(4) Charging pumps (refer to Section 9.3.4)

(5) Containment fan coolers (refer to Section 9.4.5)

(6) Control room ventilation (refer to Section 9.4.1)

(7) Component cooling pumps (refer to Section 9.2.2)

(8) Residual heat removal pumps (refer to Section 5.5.6)[a]

(9) Vital MCC and switchgear sections (refer to Section 8.3)

(10) Controlled steam release and feedwater supply (refer to Sections 7.7 and 10.4)

(11) Boration capability (refer to Section 9.3.4)

(12) Nuclear instrumentation system (source range and intermediate range; refer to Sections 7.2 and 7.7)[a]

(13) Reactor coolant inventory (charging and letdown; refer to Section 9.3.4)

(14) Pressurizer pressure control including control for pressurizer power-operated relief valves, heaters, and spray (refer to Sections 5.5.9 and 5.5.12)[a]

(15) 10 percent atmospheric dump valves (refer to Section 10.4.4)

7.4.3 SAFETY EVALUATION

7.4.3.1 General Design Criterion 3, 1971 – Fire Protection

The instrumentation and control systems required for safe shutdown (MODE 3) are designed to meet the requirements of 10 CFR 50.48(a) and (c) (refer to Section 9.5.1).

7.4.3.2 General Design Criterion 11, 1967 – Control Room

The instrumentation and control functions required for safe shutdown (MODE 3) are located in the control room. Redundant instrumentation and controls are located on the hot shutdown panel, switchgear, and on the dedicated shutdown panel for the purpose of achieving and maintaining a safe shutdown in the event an evacuation of the control room is required.

---

[a] Instrumentation and controls for these systems would require some modifications so that their functions may be performed from outside the control room. Note that the reactor plant design does not preclude attaining the cold shutdown condition from outside the control room. An assessment of plant conditions could be made on a long-term basis (a week or more) to establish procedures for making the necessary physical modifications to instrumentation and control equipment in order to attain cold shutdown. During such time, the plant could be safely maintained in the hot shutdown condition.

These controls and the instrumentation channels, together with the equipment and services that are available for both hot and cold shutdown, identify the potential capability for cold shutdown of the reactor, subsequent to a control room evacuation, through the use of suitable procedures.

In the unlikely event that access to the control room is restricted, the plant can be safely maintained at safe shutdown (MODE 3), and until the control room can be reentered, by the use of the monitoring indicators and the controls listed in Section 7.4.2. These indicators and controls are provided on the hot shutdown panel, the dedicated shutdown panel, or local area panel as well as inside the control room.

7.4.3.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The safety evaluation of the maintenance of a shutdown with the systems described in Section 7.4.2 and associated instrumentation and controls has included consideration of the accident consequences that might jeopardize safe shutdown (MODE 3) conditions. The germane accident consequences are those that would tend to degrade the capabilities for boration, adequate supply of AFW, and decay heat removal.

The results of the accident analyses are presented in Chapter 15. Of these, the following produce the most severe consequences that are pertinent:

(1) Uncontrolled boron dilution

(2) Loss of normal feedwater

(3) Loss of external electrical load and/or turbine trip

(4) Loss of all ac power to the station auxiliaries

It is shown by these analyses that safety is not adversely affected by the incidents with the associated assumptions being that the instrumentation and controls indicated in Section 7.4.2 are available to control and/or monitor shutdown. These available systems allow the maintenance of safe shutdown (MODE 3) even under the accident conditions listed above that would tend toward a return to criticality or a loss of heat sink.

A plant design evaluation was performed by PG&E to identify the safe shutdown equipment that could be susceptible to loss of function due to the environmental conditions resulting from moderate-energy line breaks. Equipment modification such as spray barriers, terminal box cover gasket, and piping enclosures were designed and installed as required to preclude any loss of function in the event of a moderate-energy line break.

Additional information concerning protection of equipment from the effects of postulated piping ruptures is presented in Section 3.6.

7.4.3.4 Safe Shutdown Systems Safety Function Requirements

(1) Protection from Missiles

The provisions taken to protect the instrumentation and control systems required for safe shutdown from missiles resulting from plant equipment failures and from events and conditions outside the plant are discussed in Section 3.5.

(2) Protection Against High Energy Pipe Rupture Effects

The provisions taken to protect the instrumentation and control systems required for safe shutdown from damage that might result from dynamic effects associated with a postulated rupture of high-energy piping are discussed in Section 3.6.

(3) Protection from Moderate Energy Pipe Rupture Effects – Outside Containment

The provisions taken to provide protection of the instrumentation and control systems required for safe shutdown located outside containment from the effects of moderate energy pipe failure are discussed in Section 3.6.

(4) Protection from Jet Impingement – Inside Containment

The provisions taken to provide protection of the instrumentation and control systems required for safe shutdown located inside containment from the effects of jet impingement which may result from high energy pipe rupture are discussed in Section 3.6.

(5) Protection from Flooding Effects – Outside Containment

The provisions taken to provide protection of the instrumentation and control systems required for safe shutdown located outside containment from flooding that might result from the effects associated with a postulated rupture of piping are discussed in Section 3.6.

7.4.4 REFERENCES

1. Deleted in Revision 21.

2. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

3. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

4. IEEE Standard 308-1971, Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

5. IEEE Standard 323-2003, Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

6. IEEE Standard 336-1971, Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities, Institute of Electrical and Electronics Engineers, Inc.

7. IEEE Standard 338-1971, Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, Institute of Electrical and Electronics Engineers, Inc.

8. IEEE Standard 344-1987, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

9. IEEE Standard 384-1974, Criteria for Independence of Class 1E Equipment and Circuits, Institute of Electrical and Electronics Engineers, Inc.

10. IEEE Standard 730-1998, Software Quality Assurance Plans, Institute of Electrical and Electronics Engineers, Inc.

11. IEEE Standard 828-1990, Software Configuration Management Plans, Institute of Electrical and Electronics Engineers, Inc.

12. IEEE Standard 829-1983, Software Test Documentation, Institute of Electrical and Electronics Engineers, Inc.

13. IEEE Standard 830-1993, Recommended Practice for Software Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 1008-1987, Software Unit Testing, Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 1012-1998, Software Verification and Validation, Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard 1016-1987, Recommended Practice for Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

17. IEEE Standard 1016.1-1993, Guide to Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

18. IEEE Standard 1059-1993, Guide for Software Verification and Validation Plans, Institute of Electrical and Electronics Engineers, Inc.

19. IEEE Standard 1074-1995, Developing Software Life Cycle Processes, Institute of Electrical and Electronics Engineers, Inc.

20. IEEE Standard 1233-1998, Guide for Developing System Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

21. IEEE Standard C62.41-1991, Recommended Practice for Surge Voltages in Low Voltage AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

22. IEEE Standard C62.45-1992, Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000V and less) AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

23. IEEE Standard 7-4.3.2-2003, Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

24. EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications, Electric Power Research Institute, October, 1996.

25. EPRI TR-102323 Revision 3, Guidelines for Electromagnetic Interference Testing in Power Plants, Electric Power Research Institute, November 2004.

26. EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Electric Power Research Institute, December 1996.

27. EPRI TR-102348 Revision 1, Guideline on Licensing Digital Upgrades, Electric Power Research Institute, March 2002.

28. Regulatory Guide 1.100 Revision 2, Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants, USNRC, June 1988.

29. Regulatory Guide 1.105, Revision 3, Setpoints for Safety-Related Instrumentation, USNRC, December 1999.

30. Regulatory Guide 1.152, Revision 1, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, USNRC, January 1996.

31. Regulatory Guide 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, February 2004.

32. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

33. Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

34. Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

35. Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

36. Regulatory Guide 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997

37. Regulatory Guide 1.180, Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, USNRC, October 2003.

38. Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, USNRC, February 1972.

39. Regulatory Guide 1.29, Revision 3, Seismic Design Classification, USNRC, September 1978.

40. Regulatory Guide 1.30, Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment, USNRC, August 1972.

41. Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, USNRC, May 1973.

42. Regulatory Guide 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, USNRC, November 1974.

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

44. NUREG-0800, Appendix 7.0-A, Revision 5, Review Process for Digital Instrumentation and Control Systems, USNRC, March 2007.

45. BTP 7-14 Revision 5 Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

46. BTP 7-18 Revision 5, Guidance on the use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

47. MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, USDOD, August 1999

48. ANSI/ANS-4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, American Nuclear Society, January 1980

49. NEMA ICS 1-2000, Industrial Control and Systems: General Requirements, National Electrical Manufacturers Association, December 2008

50. NFPA 70 (NEC) 2002 National Electric Code, National Fire Protection Association, January 2002

51. IEC 61131-3 1993, Programming Industrial Automations Systems, International Electrotechnical Commission, December 1993

52. ISA-S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation, International Society of Automation, January 1994

53. NFPA-805, Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants, 2001 Edition

7.4.5 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION

This section provides a description of the instrumentation display systems that provide information to enable the operator to perform required safety functions and post-accident monitoring.

7.5.1 DESIGN BASES

7.5.1.1 General Design Criterion 2, 1967 – Performance Standards

The PG&E Design Class I display instrumentation is designed to withstand the effects of or is protected against natural phenomena, such as earthquakes, tornadoes, flooding, winds, tsunamis, and other local site effects.

7.5.1.2 General Design Criterion 11, 1967 – Control Room

The PG&E Design Class I display instrumentation is designed to or contains instrumentation and controls that support actions to maintain the safe operational status of the plant from the control room or from an alternate location if control room access is lost due to fire or other causes.

7.5.1.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The PG&E Design Class I display instrumentation is designed to monitor and maintain variables within prescribed operating ranges.

7.5.1.4 General Design Criterion 17, 1967 – Monitoring Radioactivity Releases

The PG&E Design Class I display instrumentation is designed to provide means for monitoring the containment atmosphere, the facility effluent discharge paths, and the facility environs for radioactivity that could be released from normal operations, from anticipated transients and from accident conditions.

7.5.1.5 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The PG&E Design Class I display instrumentation that requires environmental qualification are qualified to the requirements of 10 CFR 50.49.

7.5.1.6 Regulatory Guide 1.97, Revision 3, May 1983 – Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident

The PG&E Design Class I display instrumentation is designed to provide instrumentation to monitor plant variables and systems during and following an accident.

7.5.1.7 NUREG-0737 (Items I.D.2, II.D.3, II.E.1.2, II.F.1, II.F.2, and III.A.1.2), November 1980 – Clarification of TMI Action Plan Requirements

Item I.D.2 – Plant Safety Parameter Display Console: The safety parameter display system (SPDS) is designed to display to operating personnel a minimum set of parameters which define the safety status of the plant in accordance with the guidance of NUREG-0737, Supplement 1.

Item II.D.3 – Direct indication of relief and safety valve position: The pressurizer safety valve (PSV) position indication system provides positive indication in the control room to determine valve position using acoustic monitoring in the discharge pipe.

The pressurizer PORV position indication provides positive indication in the control room to determine valve position using valve mounted limit switches.

Item II.E.1.2 – Auxiliary Feedwater System Automatic Initiation and Flow Indication: The Auxiliary Feedwater (AFW) System is designed to automatically initiate and is designed to the requirements of IEEE 279-1971. The AFW System is designed to provide a reliable indication of auxiliary feedwater system performance.

Item II.F.1 – Additional Accident Monitoring Instrumentation: The safety-related display instrumentation is designed to include the following subparts:

- Noble gas effluent radiological monitor;
- Provisions for continuous sampling of plant effluents for post-accident releases of radioactive iodines and particulates and onsite laboratory capabilities;
- Containment high-range radiation monitor;
- Containment pressure monitor;
- Containment water level monitor; and
- Containment hydrogen concentration monitor

Item II.F.2 – Instrumentation for Detection of Inadequate Core Cooling: The safety-related display instrumentation is designed to provide an unambiguous, easy-to-interpret indication of inadequate core cooling.

Item III.A.1.2 – Upgrade Emergency Support Facilities: The safety-related display instrumentation is designed to support the Technical Support Center (TSC), the Operations Support Center (OSC) and the Emergency Operations Facility (EOF) in accordance with the guidance of NUREG-0737, Supplement 1.

7.5.2 DESCRIPTION

Tables 7.5-1 and 7.5-2 list the information readouts provided to enable the operator to perform required manual safety functions and to determine the effect of manual actions taken following a reactor trip due to a Condition II, III, or IV event, as defined in Sections 15.2, 15.3, and 15.4, respectively. The tables list the information readouts required to

maintain the plant in a hot standby condition or to proceed to cold shutdown within the limits of the Technical Specifications (Reference 1). Adequate shutdown margin following Condition II and III events is verified by sampling of the reactor coolant for boron to ensure that the concentration is sufficient to maintain the reactor subcritical, as directed by emergency procedures.

Table 7.5-3 lists the information available to the operator for monitoring conditions in the reactor, the reactor coolant system (RCS), and in the containment and process systems throughout all normal operating conditions of the plant, including anticipated operational occurrences.

Table 7.5-4 lists the information available to the operator on the post-accident monitoring panels located in the control room. This information is designed to complement the information available on the control boards during post-accident conditions.

The following sections describe the monitoring systems available to the operator for assessing post-accident conditions in the RCS and the containment. Variables monitored include containment water level, hydrogen concentration and ambient pressure in the containment; RCS pressure; subcooling margin; and water level in the reactor vessel.

7.5.2.1 Post-Accident Reactor Coolant Pressure and Containment Monitors

The systems described in this section meet the following requirements:

(1) All devices must be environmentally qualified in accordance with IEEE-323-1974 (Reference 2).

(2) All devices must be seismically qualified in accordance with IEEE-344-1975 (Reference 3).

(3) Cables and raceways shall be separated in accordance with Section 8.3.1.4.1.

7.5.2.1.1 Reactor Coolant Pressure Monitors

The RCS pressure monitors consist of two mutually redundant monitors. The transmitters are mounted outside of containment and are tied to the RCS by means of sealed systems. Each sealed system consists of a bellows seal inside containment to separate the transmitter from the RCS, tubing through the penetration with a special fill fluid, and the transmitters outside of containment. The indicators for both monitors and the recorder for one of the monitors are provided in the control room.

7.5.2.1.2 Containment Pressure Monitors

The DCPP containment is a steel-lined, reinforced concrete structure designed for pressure loads and load combinations described in Section 3.8.2.1.3.2. Containment pressure transmitters with a range of -5 to 200 psig are connected to control room recorders. This instrumentation complements the reactor protection system containment pressure indicators that have a range of -5 to 55 psig.

7.5.2.1.3 Containment Water Level Monitors

The containment water level indication system consists of wide- and narrow-range monitors. Each monitor consists of two mutually redundant and separated channels that are post-accident qualified in accordance with Class 1E requirements and Regulatory Guide 1.97, Revision 3 as noted in Table 7.5-6. In addition, because of their locations, each of the wide-range monitor differential pressure transmitters has been qualified for submerged post-accident operation.

Each of the wide-range monitors is provided with a recorder that is mounted on the post-accident monitor panel in the control room.

The residual heat removal (RHR) recirculation sump water level instrumentation (the narrow-range monitor) has a level indicator mounted on the main control board. These indicators are located above the respective recirculation control switches as these indicators are used by the operator when operating pumps for recirculation.

Figure 7.5-1 represents the level indication system described above.

Figure 7.5-1B shows the Unit 2 wide-range level monitors with an installed spare transmitter in service.

7.5.2.1.4 Containment Hydrogen Monitors

The hydrogen monitoring system is described in Section 6.2.5.5.

7.5.2.1.5 High-Range Containment Radiation Monitor

Two mutually redundant high-range area radiation monitors are provided for containment monitoring. Both indication and recording of the readouts for these monitors are provided in the control room.

A detailed discussion of these monitors is presented in Section 11.4.2.1.3.1.

7.5.2.2 Instrumentation for Detection of Inadequate Core Cooling

The function of core cooling monitoring in a redundant and diverse manner is provided by the subcooling margin monitors described in Section 7.5.2.2.1 and the core exit

thermocouples described in Section 7.5.2.2.2. A supplemental source of information for use in the detection of inadequate core cooling is provided by the reactor vessel level instrumentation system described in Section 7.5.2.2.3.

7.5.2.2.1 Subcooling Meter

DCPP uses the reactor vessel level instrumentation system (RVLIS) processors to calculate RCS subcooling. Information required on the subcooled margin monitors (SCMMs) is provided in Table 7.5-5. Details of the display, calculator, and inputs are as follows:

7.5.2.2.1.1 Display

Each display (one in post-accident monitoring panel PAM3 (train A) and one in PAM4 (train B)) indicates either the temperature or pressure margin to saturation continuously on each RVLIS monitor. A one-hour trend of the temperature margin is also displayed. Train A of the SCMM provides a temperature margin output to an analog recorder. A remote digital display of the temperature margin from SCMM B is located on the main control board in the control room. The recorder is on the post-accident monitoring panel (PAM1) with other recorders to assess core cooling conditions. Each train of the SCMM provides a temperature margin analog signal to emergency response facility display system (ERFDS) for logging purposes. Refer to Section 3.10 for a discussion of the seismic qualification of the displays.

7.5.2.2.1.2 Calculator

The redundant RVLIS processors calculate the subcooled margin. The SCMM subset of RVLIS is a software program that uses RCS pressure and temperature inputs in addition to look-up steam tables to determine subcooling. The selection logic uses the highest temperature and the input pressure. Refer to Section 3.10 for a discussion of the seismic qualification of the RVLIS processor.

7.5.2.2.1.3 Inputs

(1) Temperature – Each SCMM has three temperature inputs. Four temperature signals come from each of the four hot leg wide-range resistance temperature detectors (RTDs). Hot legs 1 and 2 input to SCMM train B, and hot legs 3 and 4 input to SCMM train A. The other temperature signal into each SCMM is the hottest temperature taken from each train of core exit thermocouples. The hottest core exit thermocouple as monitored by train A inputs to SCMM A and the hottest core exit thermocouple as monitored by train B inputs to SCMM B. The temperature inputs meet Class 1E requirements and Regulatory Guide 1.97, Revision 3 as noted in Table 7.5-6.

(2) Pressure - Pressure is sensed by the wide-range reactor coolant loop pressure transmitters as described in Section 7.5.2.1.1. Each SCMM receives a pressure input from a different wide range pressure transmitter.

7.5.2.2.2 Incore Thermocouple System

Chromel-Alumel thermocouples are inserted into guide tubes that penetrate the reactor vessel head through seal assemblies and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with two primary seals, a conoseal, and a compression-type seal from conduit to head. The thermocouples are supported in guide tubes in the upper core assembly. The incore thermocouple system incorporates the installed incore thermocouples so that a complete temperature distribution can be provided.

The system consists of two redundant trains. The thermocouples are chosen so that all areas of the core are covered by each display. The number of operable thermocouples required per core quadrant is governed by the requirements provided in the Technical Specifications.

The display unit for each of the redundant trains can read out all thermocouple temperatures assigned to the train or can indicate selective incore thermocouple temperatures continuously on demand. The highest thermocouple reading in each train is recorded on the post-accident panel. The range and accuracy of these thermocouple readings are provided in Table 7.5-4.

The incore thermocouple signals are also provided as inputs to the plant computer as described in Section 7.7.2.9.1.

The incore thermocouple system is seismically and environmentally qualified. Each of the display units is powered from an independent Class 1E power source.

7.5.2.2.3 Reactor Vessel Level Instrumentation System

The reactor vessel level instrumentation system (RVLIS) uses differential pressure (DP) measuring devices to measure vessel level or relative void content of the circulating primary coolant system fluid. The system is redundant and includes automatic compensation for potential temperature variations of the impulse lines. Essential information is displayed in the main control room on the post-accident monitoring panel in a form directly usable by the operator.

The RVLIS is a microprocessor-based system. The system inputs to the microprocessor include the DP cell inputs, compensating inputs from the temperature measurements of the DP cell impulse lines, compensating temperature and pressure measurements from the RCS, and status inputs from the reactor coolant pumps. The system consists of two independent channels. Each channel utilizes three DP cells.

This DP measuring system utilizes cells of differing ranges to cover different flow behaviors with and without pump operation, as discussed below.

(1) *Reactor Vessel - Upper-Range* -- This DP cell provides a measurement of reactor vessel level above the hot leg pipe when the reactor coolant pump in the loop with the hot leg connection is not operating.

(2) *Reactor Vessel - Narrow-Range* -- This DP measurement provides a measurement of reactor vessel level from the bottom of the reactor vessel to the top of the reactor core during natural circulation conditions.

(3) *Reactor Vessel - Wide-Range* -- This DP cell provides an indication of reactor core and internals pressure drop for any combination of operating reactor coolant pumps. The comparison of the measured pressure drop with the normal single-phase pressure drop will provide an approximate indication of the relative void content or density of the circulating fluid. This instrument will monitor coolant conditions on a continuing basis during forced flow conditions.

To provide the required accuracy for the level measurement, the temperature measurements of the impulse lines to the DP cells, together with the temperature measurement of the reactor coolant and the reactor coolant system pressure, are employed to compensate the DP cell outputs for differences in system density and reference leg density. This process occurs particularly during the change in the environment inside the containment structure following an accident.

The DP cells are located outside of the containment to eliminate the potential reduction of accuracy that may result from various accident conditions. The location of the cells outside of containment makes the system operation, including calibration and maintenance, easier (Refer to Figure 7.5-2).

7.5.2.3 Plant Vent Post-Accident Radiation Monitors

The plant vent post-accident monitoring is provided by dual-path iodine and particulate grab samplers and an extended range noble gas monitoring channel. The grab sample paths can be changed remotely. The extended range noble gas detector is a beta scintillation detector operated in the current mode.

Potential release paths not using the plant vent are the atmospheric steam dumps/reliefs, the steam generator blowdown tank vent and the main condenser vacuum pump. The steam generator blowdown sample header and the steam generator blowdown tank overflow line to the discharge tunnel are continuously monitored using in-line radiation detectors. The blowdown tank is automatically isolated on a high-radiation signal from either of these monitors, and the discharge is rerouted to the equipment drain tank receiver for further processing so that the vent of the blowdown tank is not a discharge path under these conditions.

The steam lines, which provide the potential source for radiological release from the condenser vacuum pump exhaust and/or atmospheric steam dumps/reliefs during an accident, are monitored using Geiger-Mueller (GM) detectors shielded from background activity. The control room readout has direct indication, recorder output, high alarm, failure alarm, and is powered from Class 1E power supplies.

These monitors meet the requirements of Regulatory Guide 1.97, Revision 3 (Reference 6). A detailed discussion of these monitors is provided in Section 11.4.2.1.2.1.

7.5.2.4 ALARA Monitors for Post-Accident Monitor Access

The as low as is reasonably achievable (ALARA) monitors for post-accident monitors access are provided to monitor the area where the plant vent radiation monitoring post-accident systems are located. Remote indication in a low dose area is provided. Indication in the control room for RE-34 is provided by RR-34.

7.5.2.5 Radioactive Gas Decay Tank Pressure

Post-accident monitoring of the pressures in the three radioactive gas decay tanks is provided in the control room. Each pressure measurement circuit consists of a field-mounted transmitter and an indicator located on the post-accident monitoring panel. The range and accuracy of these measurements are provided in Table 7.5-4.

7.5.2.6 Auxiliary Feedwater Flow Indication

The auxiliary feedwater (AFW) flow indication is provided by a single flow indication channel for the individual AFW feed lines to each of the four steam generators. These flow channels are Class 1Eand powered from the instrument and control power supply system.

An alternative means of AFW flow indication is provided by a Class 1E steam generator water level indication for each steam generator.

7.5.2.7 Dedicated Shutdown Panel

The instrumentation on the dedicated shutdown panel provides the indication required to bring the reactor to cold shutdown from hot standby (MODE 3) in the event that all equipment in the cable spreading room, including all protection racks, are destroyed by fire. In addition to indication, control of the pressurizer auxiliary spray valve (control remote from the control room) is located in this panel. Control of vital equipment is maintained at electrical switchgear and the hot shutdown panel. Equipment is powered from the Class 1E ac instrumentation panels.

None of the instrumentation and control or electrical components in this panel are required to complete any active functions for any seismic events, or events that produce harsh environmental conditions; however, the panel and certain components within the panel are seismically and environmentally qualified for integrity of Class 1E circuits.

The following parameters are provided on the panel:

Reactor coolant system pressure
Pressurizer level
Reactor coolant system temperature
Steam generator level

Steam generator pressure is available from local indicators adjacent to the dedicated shutdown panel.

Alarms and recorders are not required for this system.

Additional information concerning the use of the dedicated shutdown panel to support remote operations is provided in Section 7.4.

7.5.2.8 Pressurizer Safety Valve Position Indication System and Power Operated Relief Valve Position Indication

The PSV position indication system provides the necessary information in the control room to determine the position (open/close) of each of the three PSVs. One acoustic monitor (piezoelectric accelerometer) per PSV is mounted inside containment on the discharge pipe in close proximity to its associated PSV. In the event of a PSV opening, the discharge from the pressurizer will induce pipe vibrations that will be sensed by the acoustic monitor associated with the opened PSV. The electric signal originating from the acoustic monitors is first amplified by charge-mode amplifiers (located inside containment) and then electronically processed (on a per channel basis) in the control room to show, in the form of a bar graph (LED lights on panel RCRM) and a digital readout (on VB2), the percent flow (0 to 100 percent) of each of the three PSVs. Additionally, a ganged annunciator will light in the event that one or more PSVs have opened.

Positive indication of PORV position is obtained by a direct, stem-mounted actuator which mechanically activates limit switches at the full-open and full-closed valve stem positions. These switches are seismically (DE, DDE, and HE) and environmentally qualified and provide an annunciator alarm in the control room if a PORV is not fully closed. These circuits are powered from a Class 1E bus for each PORV.

7.5.2.9 Emergency Response Facility Data System

The emergency response facility data system (ERFDS) is used to monitor and display plant parameters used for post-accident monitoring. The safety parameter display system (SPDS) is part of this system and is described in Section 7.5.2.10. The total ERFDS is not Class 1E nor does it meet the single failure criterion; however, it is designed to be a highly reliable system. The ERFDS is server-based with distributed desktop PCs for data displays. The ERFDS meets the criteria set forth in NUREG-0737, Supplement 1 (Reference 8). NUREG-0696, 1981 (Reference 9) is used for guidance as identified in NUREG-0737, Supplement 1.

The data storage and data retrieval functions associated with post-accident monitoring are performed by the Main Plant Historian. The Main Plant Historian is hosted on Plant Information Network (PIN) Servers in the TSC.

Each power plant unit has its own system to acquire and process data. However, Unit 1 and Unit 2 will share Technical Support Center (TSC) data display equipment. Similarly, the Alternate Technical Support Center/Operational Support Center (Alternate TSC/OSC), and Emergency Operations Facility (EOF) equipment will be shared by Unit 1 and Unit 2.

The system is divided into three subsystems as discussed in the following subsections.

7.5.2.9.1 High-Speed Data Acquisition Subsystem

The data acquisition subsystem is a high-speed, remote multiplexing system that interfaces with the plant instrumentation, converts the data to a digital form, and then transmits the data to other parts of the ERFDS.

The data acquisition subsystem provides Class 1E isolation in the remote multiplexers between the different Class 1E instrument loops, and also between the Class 1E instrument loops and the rest of the system. Remote multiplexers are located so as to minimize additional wire runs. Each remote multiplexer has a 12-bit analog to digital (A/D) converter for high accuracy. The remote multiplexers can also interface with bilevel signals. The digital information from the remote multiplexers for Unit 1 and Unit 2 is transmitted to both the Unit 1 and Unit 2 Transient Recording System (TRS) servers which host the SPDS application.

7.5.2.9.2 SPDS TRS Server Subsystem

The TRS Server Subsystem for each unit is a dedicated server that controls data transfer between the data acquisition subsystem and the different desktop PCs making up the data display subsystem. Display data is updated at 1-second intervals.

The TRS serverhosts the SPDS application. Each unit's TRS acquires ERFDS data for both units. The TRS servers transmit the data via the Plant Data Network (PDN) to the

PPC, display PCs in the control room, and the Plant Information Network (PIN) servers in the TSC. TSC, Alternate TSC/OSC and EOF displays receive data from the PIN servers via the PIN and the DCPP LAN using remote applications (Remote Desktop Services). ERDS data to the NRC is sent via a secure internet connection on the PG&E LAN.

7.5.2.9.3 Display System

The display subsystem provides the system interface for the operators and emergency personnel. The ERFDS has two categories of display devices: the ERFDS displays and the SPDS displays. The subsystem has independent functional stations in the TSC, Alternate TSC/OSC, EOF, and control room, as described below.

The TSC, Alternate TSC/OSC, and EOF display equipment includes two ERFDS Human System Interfaces (HSIs) and two SPDS-HSIs. The HSIs are connected to the DCPP LAN. A color printer connected to the DCPP LAN may be used for printouts of ERFDS, SPDS, EARS, radiation data processor, and PPC displays. The control room display equipment includes two SPDS HSIs. Additionally, SPDS screens may be displayed on a TV monitor. The displays are human-engineered with functional groupings of variables.

With the exception of an additional display monitor, the EOF portion of the display subsystem is identical to the TSC display subsystem.

7.5.2.9.4 Equipment Location

7.5.2.9.4.1 Control Room

(1) Ten remote multiplexers for each unit are located in the control room. The multiplexer location and instrument channel are specified as follows:

Multiplexer Number	Instrument Channel	Location
1	I	Main Control Board, VB1
2	II	Main Control Board, VB1
3	III	Main Control Board, VB1
4	Nonvital	Main Control Board, VB1
5	I	Main Control Board, VB4 Unit 1, (VB5, Unit 2)
6	II	Main Control Board, VB4 Unit 1, (VB5, Unit 2)
7	III	Main Control Board, VB4 Unit 1, (VB5, Unit 2)
8	IV	Main Control Board, VB4 Unit 1, (VB5, Unit 2)
9	II	Post-accident monitoring

Multiplexer Number	Instrument Channel	Location
		panel, PAM3
10	III	Post-accident monitoring panel, PAM4
11	Nonvital	Rack remote multiplexer, RM (Reference 1)

(2) Two submultiplexers are located in the main control board, VB1 of each unit.

(3) The SPDS desks are located in the control room. Each unit has an SPDS desk. The desks each house two SPDS monitors and personal computer, a TV monitor that is available to display SPDS screens and the Main Annunciator System (MAS) secondary display monitor facing the Shift Foreman's desk.

7.5.2.9.4.2 Technical Support Center

The following equipment is located in the TSC:

(1) A color printer connected to the DCPP LAN may be used to print ERFDS, SPDS, PPC, EARS, and radiation data processor displays

(2) Two SPDS HSIs

(3) Two ERFDS HSIs

(4) PDN and PIN network infrastructure, domain servers, and data/application servers.

7.5.2.9.4.3 Emergency Operations Facility

The following equipment is located in the EOF:

(1) Two SPDS HSIs

(2) Two ERFDS HSIs

(3) Network infrastructure

(4) A color printer connected to the DCPP LAN may be used to print ERFDS, SPDS, PPC, EARS, and radiation data processor displays.

7.5.2.9.4.4 Alternate TSC/OSC

The following equipment is located in the Alternate TSC/OSC:

(1) Two SPDS HSIs

(2) Two ERFDS HSIs

(3) Network infrastructure

(4) Acolor printer connected to the DCPP LAN may be used to print ERFDS, SPDS, PPC, EARS, and radiation data processor displays.

7.5.2.10 Safety Parameter Display System

The SPDS is the display subsystem of the ERFDS. The ERFDS is described in Section 7.5.2.9. The SPDS provides a display of plant parameters from which the safety status of operation may be assessed in the control room. The primary function of the SPDS is to help operating personnel in the control room make quick assessments of plant safety status.

The SPDS equipment includes HSIs with color displays.

HSIs with color displays are located in the control room, TSC, Alternate TSC/OSC, and EOF. Each control room HSI receives data from the Unit 1 or Unit 2 TRS via the PDN. TSC, Alternate TSC/OSC, and EOF HSIs receive Unit 1 and Unit 2 data from the DCPP LAN.

The SPDS has one primary display and a number of secondary displays. The primary display addresses the following important plant functions:

(1) Reactivity control

(2) Reactor core cooling and heat removal from primary system

(3) Reactor coolant system integrity

(4) Radioactivity control

(5) Containment integrity

All displays are redundant (available to both SPDS display monitors in each location). All the displays are integrated with the plant operating procedures. Magnitudes and trends can be displayed.

The SPDS displays are available in the control room, TSC, Alternate TSC/OSC, and EOF.

7.5.3 SAFETY EVALUATION

7.5.3.1 General Design Criterion 2, 1967 – Performance Standards

Seismic qualification of safety-related display instrumentation is identified in Table 7.5-6.

The post-accident reactor coolant pressure and containment monitors described in Section 7.5.2.1 are seismically qualified in accordance with IEEE-344-1975 (Reference 3).

The seismic qualification of instrumentation used for detection of inadequate core cooling is described in Sections 3.10.3.21, 3.10.3.22, and 3.10.3.31.

None of the instrumentation and control or electrical components in the dedicated shutdown panel are required to complete any active functions for any seismic events, or events that produce harsh environmental conditions; however, the panel and certain components within the panel are seismically and environmentally qualified for integrity of Class 1E circuits.

The post-accident reactor coolant pressure and containment monitors, the instrumentation used for detection of inadequate core cooling and the dedicated shutdown panel are housed in seismically qualified buildings (containment structure and auxiliary building). These buildings are PG&E Design Class I (refer to Section 3.8) and designed to withstand the effects of winds and tornadoes (refer to Section 3.3), floods and tsunamis (refer to Section 3.4), external missiles (refer to Section 3.5), earthquakes (refer to Section 3.7), and other natural phenomena to protect the safety-related display instrumentation that perform PG&E Design Class I functions.

7.5.3.2 General Design Criterion 11, 1967 – Control Room

Tables 7.5-1 and 7.5-2 list the information readouts provided to enable the operator to perform required manual safety functions and to determine the effect of manual actions taken following a reactor trip due to a Condition II, III, or IV event, as defined in Sections 15.2, 15.3, and 15.4, respectively. The tables list the information readouts required to maintain the plant in a hot standby condition or to proceed to cold shutdown within the limits of the Technical Specifications (Reference 1). Adequate shutdown margin following Condition II and III events is verified by sampling of the reactor coolant for boron to ensure that the concentration is sufficient to maintain the reactor subcritical, as directed by emergency procedures.

Table 7.5-3 lists the information available to the operator for monitoring conditions in the reactor, the reactor coolant system (RCS), and in the containment and process systems

throughout all normal operating conditions of the plant, including anticipated operational occurrences.

Table 7.5-4 lists the information available to the operator on the post-accident monitoring panels located in the control room. This information is designed to complement the information available on the control boards during post-accident conditions.

For Conditions II, III, and IV events (Refer to Tables 7.5-1 and 7.5-2), sufficient duplication of information is provided to ensure that the minimum information required will be available. The information is part of the operational monitoring of the plant that is under surveillance by the operator during normal plant operation. This is functionally arranged on the control board to provide the operator with ready understanding and interpretation of plant conditions. Comparisons between duplicate information channels or between functionally related channels enable the operator to readily identify a malfunction in a particular channel.

Refueling water storage tank level is indicated and alarmed by three independent single channel systems. Similarly, two channels of the RCS pressure (wide-range) are available for maintaining proper pressure-temperature relationships following a postulated Condition II or III event. One channel of steam generator water level (wide-range) is provided for each steam generator; this duplicates level information from steam generator water level (narrow-range) and ensures availability of level information to the operator.

The remaining safety-related display instrumentation necessary for Conditions II, III, or IV events is obtained through isolation devices from the protection system. These protection channels are described in Section 7.2.2.8.

The readouts identified in the tables were selected on the basis of sufficiency and availability during, and subsequent to, an accident for which they are necessary. Thus, the occurrence of an accident does not render this information unavailable, and the status and reliability of the necessary information is known to the operator before, during, and after an accident. No special separation is required to ensure availability of necessary and sufficient information. In fact, such separation could reduce the operator's ease of interpretation of data.

The design criteria used in the display system are listed below:

(1) Range and accuracies listed in Tables 7.5-1 and 7.5-2 are validated through the analysis of operator actions during Condition II, III, or IV events as described in Chapter 15. The display system meets the following requirements:

(a) The range of the readouts extends over the maximum expected range of the variable being measured, as listed in column 4 of Tables 7.5-1 and 7.5-2.

(b) The combined indicated accuracies are shown in column 5 of Tables 7.5-1 and 7.5-2.

(2) Power for the display instruments is obtained from the Class 1E 120-Vac Instrument Power Supply System as described in Section 8.3.1.1.5.2.1 and the non-Class 1E 120-Vac Instrument Power Supply System as described in Section 8.3.1.1.5.2.2.

(3) Those channels determined to provide useful information in charting the course of events are recorded as shown in column 6 of Tables 7.5-1 and 7.5-2.

The dedicated shutdown panel described in Section 7.5.2.7 provides information concerning indications to support remote operations if control room access is lost due to fire or other causes.

7.5.3.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

Section 7.5.2 provides a description of the instrumentation display systems that provide information to enable the operator to perform required safety functions and post-accident monitoring. They are designed to monitor and maintain variables within prescribed operating ranges.

7.5.3.4 General Design Criterion 17, 1967 – Monitoring Radioactivity Releases

The monitors for the plant vent and containment radiation are described in Section 11.4.2.1.2.1.

The post-accident monitors used for monitoring radioactivity releases are described in Section 7.5.2.3.

7.5.3.5 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

Environmental qualification of safety-related display instrumentation is identified in Table 7.5-6. The post-accident reactor coolant pressure and containment monitors described in Section 7.5.2.1 are environmentally qualified in accordance with IEEE-323-1974 (Reference 2).

7.5.3.6 Regulatory Guide 1.97, Revision 3, May 1983 – Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident

Table 7.5-6 summarizes the compliance of Diablo Canyon Power Plant with Regulatory Guide 1.97, Rev. 3. The format and content of the table are consistent with both the recommendations in Table 3 of the Regulatory Guide and the guidance provided at the March 1, 1983, NRC Regional meeting.

Post-Accident Monitoring Instruments and Controls

Post-accident monitoring instruments and controls are divided into variable Types A through E and Categories 1 through 3 as outlined in Regulatory Guide 1.97, Rev. 3. The variable types indicate whether the variable is considered to be a key variable needed for: (a) plant operation, (b) system status indication, or (c) backup or diagnosis. The three categories provide a graded approach to design, qualification, and quality requirements depending on the importance to safety of the measurement of a specific variable. The variable types and categories are as follows:

Variable Types

Type A - This variable is for components that provide primary information required to permit the control room (operating personnel) to take the specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident events. Type A variables must meet the Category 1 qualification requirements.

Type B - This variable is for components that provide information to indicate whether plant safety functions are being accomplished. Plant safety functions are (a) reactivity control, (b) core cooling, (c) maintaining reactor core coolant system integrity, and (d) maintaining containment integrity.

Type C - This variable is for components that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product release. The barriers are (a) fuel cladding, (b) primary coolant pressure boundary, and (c) containment.

Type D - This variable is for components that provide information to indicate the operation of individual safety systems and other systems important to safety.

Type E - This variable is for components that are monitored as required for use in determining the magnitude of the release of radioactive materials and for continually assessing such releases.

Categories 1 through 3:

Category 1 - Provides the most stringent design and qualification criteria and is intended for key variables.

Category 2 - Provides less stringent design, qualification, and quality criteria and generally applies to instruments and controls designated for indicating system operating status.

Category 3 - Provides design and qualification criteria that will ensure that high-quality, off-the-shelf instrumentation is obtained. Category 3 applies to backup and diagnostic instrumentation and is also used when the design requires state-of-the-art equipment, but equipment qualified to a higher category is not available.

Category 3 instrumentation is non-Class 1E.

Process Control System

The PCS processes the following post-accident monitoring channels:

(1) Auxiliary Feedwater Flow (Type A, Cat. 1)

(2) Charging Injection Header Flow (Type D, Cat. 2)

(3) Letdown Outlet Flow (Type D, Cat. 2)

(4) Makeup Flow-in (Type D, Cat. 2)

(5) RHR Flow to RCS Cold Legs Temperature (Type D, Cat. 2)

(6) RHR HX Outlet Flow (Type D, cat. 2)

(7) RHR HX Outlet to Hot Legs 1 & 2 Flow (Type D, Cat. 2)

(8) Safety Injection Pump Discharge Flow (Type D, Cat. 2)

(9) Steam Generator Wide Range Level (Type A, Cat. 1)

(10) Volume Control Tank Level Control (Type D, Cat. 2)
(11) CCW Heat Exchanger Outlet Temperature (Type D, Cat. 2)

(12) CCW Supply Headers A and B Flow (Type D, Cat. 2)

(13) Condensate Storage Tank Level (Type A, Cat. 1)

(14) Refueling Water Storage Tank Level (Type A, Cat. 1)

(15) Accumulator Tank Pressure (Type D, Cat. 3)

(16) Quench Tank (PRT) Level (Type D, Cat. 3)

(17) Quench Tank (PRT) Temperature (Type D, Cat. 3)

(18) Quench Tank (PRT) Pressure (Type D, Cat. 3)

References 6 and 10 through 58 were used for design, verification, validation, and qualification of all or portions of the PG&E Design Class I PCS hardware and software (encompassing Triconex components, manual/auto hand stations, signal converters/isolators and loop power supplies).

7.5.3.7 NUREG-0737 (Items I.D.2, II.D.3, II.E.1.2, II.F.1, II.F.2, and III.A.1.2), November 1980 – Clarification of TMI Action Plan Requirements

7.5.3.7.1 Item I.D.2 – Plant Safety Parameter Display Console

SPDS Display

The primary SPDS display was designed to provide the control room operators with a concise format of critical plant variables to aid in determining the safety status of the plant. Parameter selection was made to address the five functions as listed in Section 7.5.2.10. The major types of possible accidents were evaluated to develop the minimum number of plant variables necessary to alert the operator of an abnormal condition. The parameters selected for each function were:

(1) *Reactivity Control*

(a) Three ranges of flux indication from 120 percent full power to 1 count/second using all three ranges of nuclear instrumentation: monitors neutron flux during all modes of operation.

(b) Startup rate indication.

(c) "Control Rods In" alert, which warns the operator of a reactor trip without insertion of all control rods.

(2) *Reactor Core Cooling and Heat Removal*

(a) Subcooled margin, which is a derived variable based on RCS pressure and temperature inputs, indicates the degree of subcooling or superheat present.

(b) Highest core exit thermocouple temperature monitors core exit temperature conditions.

(c) Reactor vessel level, wide- or narrow-range depending on reactor coolant pump status, indicates lack of adequate core cooling.

(d) Narrow-range steam generator level can be used to determine heat removal capability of the secondary system.

(3) *RCS Integrity*

(a) Reactor coolant system pressure can be used to monitor high-pressure conditions against design limits and can be used with cold leg temperature to monitor plant conditions against system nil ductility transition (NDT) limits.

(b) Pressurizer level is actually used as an indication of inventory if RCS has been, or is, subcooled. However, it is an important parameter with RCS pressure for rapid determination of normal or expected plant status.

(c) Cold leg temperature can be used with RCS pressure to monitor plant status with respect to system NDT limits.

(4) *Radioactivity Control*

(a) Containment radiation monitor indicates the release of radiation from the primary system to containment.

(b) Vent gas and vent iodine monitors monitor radioactivity releases from the plant vent to the environment.

(c) Main steam monitors indicate radioactivity released to the secondary system and/or atmosphere via steam generator tube leaks or tube failures.

(5) *Containment Integrity*

(a) Containment pressure monitors monitor actual pressure against design limit.

(b) Containment Isolation Phase A and/or B alert informs the operator that a Phase A and/or B isolation signal has occurred and whether alignment of the isolation valves is complete.

SPDS Display Groupings

The parameters for the SPDS display were grouped in each of the five areas. Alarm setpoints were selected to duplicate the trip and alarm settings of the plant instrumentation, plant Technical Specification requirements, or limits specified in the plant manuals. Distinctive color coding is used on the display to alert control room personnel to an abnormal condition. If a parameter is within its normal range, the bar for that parameter on the display is green; it is displayed red if outside the specified limits.

SPDS Operation

The basis for the location of the SPDS monitors in the control room was to ensure adequate visibility by the senior control room operator and not to impede movement in the control room. Console location is indicated in Figure 7.7-16. The color coding of the SPDS display readily enables the user to determine if a parameter on the display is within normal limits. In the case of an abnormal condition, the Emergency Evaluation Coordinator will typically be the prime user of the SPDS.

SPDS Monitors

There are two (2) SPDS displays in the control room, EOF, and TSC. Each screen has the critical safety function status shown at the top.

7.5.3.7.2 Item II.D.3 – Direct indication of relief and safety valve position

The PORV position indication and PSV position indication system provide the necessary information in the control room to determine the position (open/close) of each of the three PORVs and three PSVs as described in Section 7.5.2.8.

7.5.3.7.3 Item II.E.1.2 – Auxiliary Feedwater System Automatic Initiation and Flow Indication

AFW flow indication is provided in the control room as described in Section 7.5.2.6. AFW automatic initiation is provided as described in Section 6.5.

7.5.3.7.4 Item II.F.1 – Additional Accident Monitoring Instrumentation

The safety-related display instrumentation includes the following subparts:

- Noble gas effluent radiological monitor – refer to Section 7.5.2.3;
- Provisions for continuous sampling of plant effluents for post-accident releases of radioactive iodines and particulates – refer to Section 7.5.2.3
- Onsite laboratory capabilities – refer to Sections 12.3.2 and 6.4.2.3;
- Containment high-range radiation monitor – refer to Section 7.5.2.1.5;
- Containment pressure monitor – refer to Section 7.5.2.1.2;

- Containment water level monitor – refer to Section 7.5.2.1.3; and
- Containment hydrogen concentration monitor – refer to Section 7.5.2.1.4

A discussion of each subpart is described in the indicated section.

7.5.3.7.5 Item II.F.2 – Instrumentation for Detection of Inadequate Core Cooling

The instrumentation used for detection of inadequate core cooling is described in Section 7.5.2.2.

7.5.3.7.6 Item III.A.1.2 – Upgrade Emergency Support Facilities

ERFDS is described in Section 7.5.2.9. All input parameters are routed from the Validyne data acquisition system to the Transient Recording System (TRS), which provides the data recall and storage for ERFDS. Each Unit's TRS acquires ERFDS data for both Units. The TRS servers provide data to PDN connected HSIs and PIN servers. PIN servers provide ERFDS data to DCPP LAN connected HSIs. PDN-connected HSIs with recall capability can display ERFDS data for either Unit. There are two dedicated ERFDS HSIs connected to the DCPP LAN in both the TSC and EOF. In addition, other selected DCPP LAN connected HSIs in the TSC and EOF may also view ERFDS and SPDS data. All data available on the ERFDS HSIs in the TSC and EOF is also available on the Plant Process Computer (PPC). The PPC HSIs in the TSC and EOF receive data from PIN servers via PIN and the DCPP LAN. Additional parameters available for display by the PPC are specified in Table 7.5-6. Other parameters are also available to allow post-accident monitoring and analysis via the PPC.

7.5.4 REFERENCES

1. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

2. IEEE Standard 323-1974, Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

3. IEEE Standard 344-1975, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

4. Deleted in Revision 15.

5. Deleted in Revision 15.

6. Regulatory Guide 1.97, Rev. 3 Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, USNRC, May 1983.

7. Deleted in Revision 21.

8. NUREG-0737, Supplement 1, Safety Parameter Display System Requirements for Nuclear Power Plants, USNRC, December 17, 1982.

9. NUREG-0696, Functional Criteria for Emergency Response Facilities, USNRC, February 1981.

10. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

11. IEEE Standard 308-1971, Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

12. IEEE Standard 323-2003, Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

13. IEEE Standard 336-1971, Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities, Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 338-1971, Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 344-1987, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard 384-1974, Criteria for Independence of Class 1E Equipment and Circuits, Institute of Electrical and Electronics Engineers, Inc.

17. IEEE Standard 730-1998, Software Quality Assurance Plans, Institute of Electrical and Electronics Engineers, Inc.

18. IEEE Standard 828-1990, Software Configuration Management Plans, Institute of Electrical and Electronics Engineers, Inc.

19. IEEE Standard 829-1983, Software Test Documentation, Institute of Electrical and Electronics Engineers, Inc.

20. IEEE Standard 830-1993, Recommended Practice for Software Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

21. IEEE Standard 1008-1987, Software Unit Testing, Institute of Electrical and Electronics Engineers, Inc.

22. IEEE Standard 1012-1998, Software Verification and Validation, Institute of Electrical and Electronics Engineers, Inc.

23. IEEE Standard 1016-1987, Recommended Practice for Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

24. IEEE Standard 1016.1-1993, Guide to Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

25. IEEE Standard 1059-1993, Guide for Software Verification and Validation Plans, Institute of Electrical and Electronics Engineers, Inc.

26. IEEE Standard 1074-1995, Developing Software Life Cycle Processes, Institute of Electrical and Electronics Engineers, Inc.

27. IEEE Standard 1233-1998, Guide for Developing System Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

28. IEEE Standard C62.41-1991, Recommended Practice for Surge Voltages in Low Voltage AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

29. IEEE Standard C62.45-1992, Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000V and less) AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

30. IEEE Standard 7-4.3.2-2003, Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

31. EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications, Electric Power Research Institute, October, 1996.

32. EPRI TR-102323 Rev. 3, Guidelines for Electromagnetic Interference Testing in Power Plants, Electric Power Research Institute, November 2004.

33. EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Electric Power Research Institute, December 1996.

34. EPRI TR-102348 Rev. 1, Guideline on Licensing Digital Upgrades, Electric Power Research Institute, March 2002.

35. Regulatory Guide 1.100 Rev. 2, Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants, USNRC, June 1988.

36. Regulatory Guide 1.105, Rev. 3, Setpoints for Safety-Related Instrumentation, USNRC, December 1999.

37. Regulatory Guide 1.152, Rev, 1, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, USNRC, January 1996.

38. Regulatory Guide 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, February 2004.

39. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

40. Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

41. Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

42. Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

43. Regulatory Guide 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997

44. Regulatory Guide 1.180, Rev. 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, USNRC, October 2003.

45. Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, USNRC, February 1972.

46. Regulatory Guide 1.29, Rev. 3, Seismic Design Classification, USNRC, September 1978.

47. Regulatory Guide 1.30, Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment, USNRC, August 1972.

48. Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, USNRC, May 1973.

49. Regulatory Guide 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, USNRC, November 1974.

50. NUREG-0800, Appendix 7.0-A, Rev. 5, Review Process for Digital Instrumentation and Control Systems, USNRC, March 2007.

51. BTP 7-14 Rev. 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

52. BTP 7-18 Rev. 5, Guidance on the use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

53. MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility, USDOD, August 1999

54. ANSI/ANS-4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, American Nuclear Society, January 1980

55. NEMA ICS 1-2000, Industrial Control and Systems: General Requirements, National Electrical Manufacturers Association, December 2008

56. NFPA 70 (NEC) 2002 National Electric Code, National Fire Protection Association, January 2002

57. IEC 61131-3 1993, Programming Industrial Automations Systems, International Electrotechnical Commission, December 1993

58. ISA-S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation, International Society of Automation, January 1994

7.5.5 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

7.6 ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY

This section provides a description and an analysis of: (a) residual heat removal (RHR) isolation valves, (b) the pipe break isolation system (PBIS), and (c) the anticipated transients without scram (ATWS) mitigation system actuation circuitry (AMSAC). The instrumentation and control power supply system is described and analyzed in Section 8.3.1.1.5. A discussion of the refueling interlocks is provided in Section 9.1. The fire detection and protection system is described in Section 9.5.1.

7.6.1 DESIGN BASES

7.6.1.1 General Design Criterion 2, 1967 – Performance Standards

The RHR isolation valves and the PBIS are designed to withstand the effects of or are protected against natural phenomena, such as earthquakes, tornadoes, flooding, winds, tsunamis, and other local site effects.

7.6.1.2 General Design Criterion 11, 1967 – Control Room

The RHR isolation valves, the PBIS, and the AMSAC system are designed to or contain instrumentation and controls that support actions to maintain the safe operational status of the plant from the control room.

7.6.1.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The RHR isolation valves and the PBIS have instrumentation and controls to monitor and maintain system variables within prescribed operating ranges.

7.6.1.4 Other Instrumentation Systems Safety Function Requirements

(1) Protection from Missiles

The RHR isolation valves instrumentation and the PBIS are designed and located to be protected against the effects of missiles which may result from plant equipment failure and from events and conditions outside the plant.

(2) Protection Against High Energy Pipe Rupture Effects

The RHR isolation valves instrumentation and the PBIS are designed and located to accommodate the dynamic effects of a postulated high-energy pipe failure to the extent necessary to assure that a safe shutdown condition of the reactor can be accomplished and maintained.

(3) Protection from Moderate Energy Pipe Rupture Effects – Outside Containment

The outside containment RHR isolation valves instrumentation and the PBIS are designed to be protected against the effects of moderate energy pipe failure.

(4) Protection from Jet Impingement – Inside Containment

The inside containment RHR isolation valves instrumentation and the PBIS are designed to be protected against the effects of jet impingement which may result from high energy pipe rupture.

(5) Protection from Flooding Effects – Outside Containment

The outside containment RHR isolation valves instrumentation and the PBIS are to be protected from the effects of internal flooding.

7.6.1.5 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The RHR isolation valves and associated components and PBIS components that require environmental qualification are qualified to the requirements of 10 CFR 50.49.

7.6.1.6 10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients Without Scrams (ATWS) Events for Light-Water-Cooled Nuclear Power Plants

AMSAC meets the requirement of providing a system independent of the reactor trip system to initiate auxiliary feedwater flow and turbine trip under ATWS conditions.

7.6.2 DESCRIPTION

7.6.2.1 Residual Heat Removal Isolation Valves

There are two motor-operated gate valves in series in the inlet line from the reactor coolant system (RCS) to the RHR system. They are normally closed and can only be opened for RHR after RCS pressure is reduced below approximately 390 psig. In addition, one valve cannot open until the pressurizer vapor space temperature has been reduced to approximately 475°F (refer to Sections 5.6.2 and 5.5.6 for details of the RHR system.) RHR isolation valve control and indications are as follows:

(1) One isolation valve, that nearest the RCS, is interlocked with a pressure signal to prevent its being opened whenever the RCS pressure is greater than the setpoint pressure (approximately 390 psig). This interlock is derived from one process control channel.

(2) The other valve is similarly interlocked. Control signals are derived from a second process control channel. In order to both comply with IEEE 279-1971 (Reference 1) and to provide diversity, the permissive interlock to open this valve is satisfied when the pressurizer vapor space temperature is reduced to approximately 475°F and the RCS pressure is reduced below approximately 390 psig. This temperature control signal is derived from one process instrumentation protection channel.

(3) Each isolation valve is provided with an independent alarm circuit from independent process protection channels that will actuate a common annunciator in the control room whenever the isolation valve is not 100 percent closed and RCS pressure is greater than approximately 435 psig. Procedures instruct the operators to stop RCS pressurization and close the isolation valves should this alarm condition occur during RCS pressurization with the RHR system removed from service.

(4) The RHR suction valves interlock relays are powered from the solid state protection system (SSPS) output cabinets. To maintain the ability to open the RHR suction valves when the SSPS output cabinets are de-energized in Mode 6 or defueled, jumpers are used to lock-in the RHR suction valves open permissive. This defeats the applicable RHR system overpressurization/temperature protection. Jumper installation is limited to Mode 6 and defueled only.

In the fire protection review, it was postulated that fire damage to electrical cables could cause both RHR suction line isolation valves to open. To prevent this, the power will be removed from each valve's motor operator by opening manual circuit breakers after the valves have been correctly positioned whenever RCS pressure is greater than 390 psig. Continuous indication that the RHR suction line isolation valves are in the correct position is provided for each valve. The control room valve position indicators are not disabled by opening the circuit breakers and removing power from the valves' motor operators.

RHR isolation valve control, valve position indication, and annunciation are provided in the control room.

7.6.2.2 Pipe Break Isolation System

The PBIS provides a means to detect and isolate breaks in high-energy lines in the auxiliary building. This system limits the postulated mass/energy release in affected compartments. This reduces the environmental effect on a number of PG&E Design Class I and Class 1E components in the area.

There are two postulated pipe breaks that could affect Area K of the auxiliary building: (a) chemical and volume control system (CVCS) letdown line, and (b) auxiliary steam line. The PBIS provides an alarm and automatic isolation (redundant) of a break in the

letdown line after the letdown isolation valves. An alarm and a switch for manual isolation are provided for the auxiliary steam line.

A break in a high-energy line is detected by redundant temperature sensors monitoring ambient air temperature. Alarms are provided at predetermined setpoints, based on an analysis of the postulated breaks. Annunciation is provided in the control room.

The Process Control System (PCS) processes the CVCS letdown line break temperature detector inputs and provides an output to the pipe break isolation logic. The PCS also processes the Auxiliary steam line area temperature detector inputs and provides control room indication and alarm. References 1, 2, 3 and 9 through 55 were used for design, verification, validation, and qualification of all or portions of the PG&E Design Class I PCS hardware and software (encompassing Triconex components, manual/auto hand stations, signal converters/isolators and loop power supplies).

7.6.2.3 ATWS Mitigation System Actuation Circuitry (AMSAC)

DCPP has installed an AMSAC system in both Units.

The system uses the standard Westinghouse design with the steam generator water level option. References 5 and 6 describe the generic AMSAC design. A functional logic diagram is shown in Figure 7.2-1, Sheets 33 and 34.

The AMSAC system trips the turbine, starts auxiliary feedwater, and isolates steam generator blowdown on coincidence of an AMSAC low steam generator water level signal from three out of four steam generators.

The AMSAC system performs an important safety function if the plant's primary reactor protection system fails. Accordingly, to ensure the reliability of the system, all activities that could affect the quality of non-Class 1E AMSAC equipment shall be controlled as if the equipment were Class 1E.

ATWS Mitigation System Actuation Circuitry indication is provided in the control room with annunciation windows.

7.6.3 SAFETY EVALUATION

7.6.3.1 General Design Criterion 2, 1967 – Performance Standards

The PG&E Design Class I portion of the RHR isolation valves and pipe break isolation system are seismically designed and housed in seismically qualified buildings (containment structure and auxiliary building). These buildings are Design Class I (refer to Section 3.8) and designed to withstand the effects of winds and tornadoes (refer to Section 3.3), floods and tsunamis (refer to Section 3.4), external missiles (refer to Section 3.5), earthquakes (refer to Section 3.7), and other natural phenomena to protect

the PG&E Design Class I portion of the RHR isolation valves and pipe break isolation system to ensure their safety-related functions and designs will be performed.

7.6.3.2 General Design Criterion 11, 1967 – Control Room

Controls and instrumentation related to (a) RHR Isolation Valves, (b) PBIS and (c) anticipated transients without scram (ATWS) mitigation system actuation circuitry (AMSAC) which are designed to support actions to maintain and control the safe operational status of the plant from the control room are as follows:

RHR Isolation Valves

Each RHR isolation valve is provided with an independent alarm circuit from independent process protection channels that will actuate a common annunciator in the control room whenever the isolation valve is not 100 percent closed and RCS pressure is greater than approximately 435 psig.

Continuous indication that the RHR suction line isolation valves are in the correct position is provided for each valve by control room valve position indicators that are not disabled by opening the circuit breakers and removing power from the valves' motor operators.

Pipe Break Isolation System

The PBIS provides an alarm and automatic isolation (redundant) of a break in the letdown line after the letdown isolation valves. An alarm and a switch for manual isolation are provided for the auxiliary steam line.

A break in a high-energy line is detected by redundant temperature sensors monitoring ambient air temperature. Alarms are provided at predetermined setpoints, based on an analysis of the postulated breaks.

The auxiliary steam line break isolation system provides an alarm based on any one of several high-temperature detectors. A switch is provided on the main control board to close the valves on lines that supply auxiliary steam to the auxiliary building. Since the auxiliary steam line is tied to both the Unit 1 and Unit 2 main steam lines, the crosstie through the auxiliary building to both main steam lines can be closed from either board on detection of high area temperature. Indication of area temperature is provided on the main control board to verify that isolation has occurred. Temperature indication is the only PG&E Design Class I function of the auxiliary steam line isolation system.

ATWS Mitigation System Actuation Circuitry

ATWS Mitigation System Actuation Circuitry indication is provided in the control room with annunciation windows.

7.6.3.3 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The RHR isolation valves and the PBIS have instrumentation and controls to monitor and maintain system variables within prescribed operating ranges as follows:

Residual Heat Removal Isolation Valves

Based on the scope definitions presented in IEEE-279-1971 (Reference 1) and IEEE 338-1971 (Reference 3), these criteria do not apply to the RHR isolation valve interlocks; however, in order to meet NRC requirements, and because of the possible severity of the consequences of loss of function, the requirements of IEEE-279-1971 are applied with the following comments.

(1) For the purpose of applying IEEE-279-71 (Reference 1) to this circuit, the following definitions are used:

(a) Protection System - The two valves in series in each line and all components of their interlocking and closure circuits.

(b) Protective Action - The automatic interlock of the RHR system isolation from the RCS pressure above RHR design pressure.

(2) IEEE-279-71, Paragraph 4.10: The requirement for on-line test and calibration capability is applicable only to the actuation signal and not to the isolation valves, which are required to remain closed during power operation.

(3) IEEE-279-71, Paragraph 4.15: This requirement does not apply as the setpoints are independent of mode of operation and are not changed.

Pipe Break Isolation System

The CVCS letdown line break isolation system fully complies with IEEE-279-71 (Reference 1). Three high temperature detectors are provided. Each is powered from a separate Class 1E power source. A two-out-of-three logic is used with redundant logic trains so that a single failure will not prevent system operation, while at the same time the chance of spurious operation is limited. Redundancy is carried through to the final actuation devices.

The auxiliary steam line break isolation system provides an alarm based on any one of several high-temperature detectors. A switch is provided on the main control board to close the valves on lines that supply auxiliary steam to the auxiliary building. Since the auxiliary steam line is tied to both the Unit 1 and Unit 2 main steam lines, the crosstie through the auxiliary building to both main steam lines can be closed from either board on detection of high area temperature. Indication of area temperature is provided on the main control board to verify that isolation has occurred. Temperature indication is the

only PG&E Design Class I function of the auxiliary steam line isolation system. A PG&E Design Class I backup is provided by use of the main steam line isolation system. Manual action is acceptable because of the relatively slow temperature transient that occurs due to this accident. There is sufficient time for the operator to verify that the break has been isolated before backup action is required.

7.6.3.4 Other Instrumentation Systems Safety Function Requirements

(1) Protection from Missiles

The provisions taken to protect RHR isolation valves instrumentation and the PBIS from missiles resulting from plant equipment failures and from events and conditions outside the plant are discussed in Section 3.5.

(2) Protection Against High Energy Pipe Rupture Effects

The provisions taken to protect the RHR isolation valves instrumentation and the PBIS from damage that might result from dynamic effects associated with a postulated rupture of high-energy piping are discussed in Section 3.6.

(3) Protection from Moderate Energy Pipe Rupture Effects – Outside Containment

The provisions taken to provide protection of the RHR isolation valves instrumentation and the PBIS located outside containment from the effects of moderate energy pipe failure are discussed in Section 3.6.

(4) Protection from Jet Impingement – Inside Containment

The provisions taken to provide protection of the RHR isolation valves instrumentation and the PBIS located inside containment from the effects of jet impingement which may result from high energy pipe rupture are discussed in Section 3.6.

(5) Protection from Flooding Effects – Outside Containment

The provisions taken to provide protection of the RHR isolation valves instrumentation and the PBIS located outside containment from flooding that might result from the effects associated with a postulated rupture of piping are discussed in Section 3.6.

7.6.3.5 10 CFR 50.49 – Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

The RHR isolation valves and associated components and PBIS components listed in the DCPP EQ Master List are qualified to the requirements of 10 CFR 50.49.

Environmental qualification of the valves and wiring is discussed in Section 3.11.

7.6.3.6 10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients Without Scrams (ATWS) Events for Light-Water-Cooled Nuclear Power Plants

The AMSAC system is independent and diverse from the reactor protection system. (Refer to Section 7.2 for a description of the reactor protection system). The AMSAC system trips the turbine, starts auxiliary feedwater, and isolates steam generator blowdown on coincidence of an AMSAC low steam generator water level signal from three out of four steam generators. This meets the requirements of 10 CFR 50.62.

The Westinghouse AMSAC System has been analyzed by the Westinghouse owners group, and has been shown to maintain the reactor coolant system pressure boundary within the ASME Boiler and Pressure Vessel Code (Reference 7). Level C stress limits in the event of a Condition II event as described in Section 4.2. This is documented in Westinghouse Report NS-TMA-2182 (Reference 8).

7.6.4 REFERENCES

1. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

2. IEEE Standard 308-1971, Criteria for Class IE Electric Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

3. IEEE Standard 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, Institute of Electrical and Electronics Engineers, Inc.

4. Deleted in Revision 21.

5. AMSAC Generic Design Change Package, WCAP-10858P-A, July 1987.

6. AMSAC Generic Design Package, Prescriptive Version, WCAP-11436, February 1987.

7. ASME Boiler and Pressure Vessel Code, Section III, Division I, Subsection NB-3224.

8. NS-TMA-2182, Westinghouse Letter (T. M. Anderson) to USNRC (S. H. Hanauer), ATWS Submittal, December 30, 1979.

9. IEEE Standard 323-2003, Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

10. IEEE Standard 336-1971, Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities, Institute of Electrical and Electronics Engineers, Inc.

11. IEEE Standard 344-1987, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

12. IEEE Standard 384-1974, Criteria for Independence of Class 1E Equipment and Circuits, Institute of Electrical and Electronics Engineers, Inc.

13. IEEE Standard 730-1998, Software Quality Assurance Plans, Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 828-1990, Software Configuration Management Plans, Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 829-1983, Software Test Documentation, Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard 830-1993, Recommended Practice for Software Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

17. IEEE Standard 1008-1987, Software Unit Testing, Institute of Electrical and Electronics Engineers, Inc.

18. IEEE Standard 1012-1998, Software Verification and Validation, Institute of Electrical and Electronics Engineers, Inc.

19. IEEE Standard 1016-1987, Recommended Practice for Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

20. IEEE Standard 1016.1-1993, Guide to Software Design Descriptions, Institute of Electrical and Electronics Engineers, Inc.

21. IEEE Standard 1059-1993, Guide for Software Verification and Validation Plans, Institute of Electrical and Electronics Engineers, Inc.

22. IEEE Standard 1074-1995, Developing Software Life Cycle Processes, Institute of Electrical and Electronics Engineers, Inc.

23. IEEE Standard 1233-1998, Guide for Developing System Requirements Specifications, Institute of Electrical and Electronics Engineers, Inc.

24. IEEE Standard C62.41-1991, Recommended Practice for Surge Voltages in Low Voltage AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

25. IEEE Standard C62.45-1992, Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000V and less) AC Power Circuits, Institute of Electrical and Electronics Engineers, Inc.

26. IEEE Standard 7-4.3.2-2003, Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

27. EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications, Electric Power Research Institute, October, 1996.

28. EPRI TR-102323 Rev. 3, Guidelines for Electromagnetic Interference Testing in Power Plants, Electric Power Research Institute, November 2004.

29. EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Electric Power Research Institute, December 1996.

30. EPRI TR-102348 Rev. 1, Guideline on Licensing Digital Upgrades, Electric Power Research Institute, March 2002.

31. Regulatory Guide 1.100 Rev. 2, Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants, USNRC, June 1988.

32. Regulatory Guide 1.105, Rev. 3, Setpoints for Safety-Related Instrumentation, USNRC, December 1999.

33. Regulatory Guide 1.152, Rev, 1, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, USNRC, January 1996.

34. Regulatory Guide 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, February 2004.

35. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

36. Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

37. Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

38. Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997.

39. Regulatory Guide 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used in Safety Systems of Nuclear Power Plants, USNRC, September 1997

40. Regulatory Guide 1.180, Rev. 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, USNRC, October 2003.

41. Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, USNRC, February 1972.

42. Regulatory Guide 1.29, Rev. 3, Seismic Design Classification, USNRC, September 1978.

43. Regulatory Guide 1.30, Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment, USNRC, August 1972.

44. Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, USNRC, May 1973.

45. Regulatory Guide 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, USNRC, November 1974.

46. Regulatory Guide 1.97, Rev. 3, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, USNRC, May 1983.

47. NUREG-0800, Appendix 7.0-A, Rev. 5, Review Process for Digital Instrumentation and Control Systems, USNRC, March 2007.

48. BTP 7-14 Rev. 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

49. BTP 7-18 Rev. 5, Guidance on the use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems, USNRC, March 2007.

50. MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics of Sub-systems and Equipment, USDOD, August 1999

51. ANSI/ANS-4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, American Nuclear Society, January 1980

52. NEMA ICS 1-2000, Industrial Control and Systems: General Requirements, National Electrical Manufacturers Association, December 2008

53. NFPA 70 (NEC) 2002 National Electric Code, National Fire Protection Association, January 2002

54. IEC 61131-3 1993, Programming Industrial Automations Systems, International Electrotechnical Commission, December 1993

55. ISA-S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation, International Society of Automation, January 1994

7.6.5 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

The general design objectives of the plant control systems are:

(1) To establish and maintain power equilibrium between primary and secondary systems during steady state unit operation

(2) To constrain operational transients so as to preclude unit trip and reestablish steady state unit operation

(3) To provide the reactor operator with monitoring instrumentation that indicates required input and output control parameters of the systems, and provides the operator with the capability of assuming manual control of the system

7.7.1 DESIGN BASES

7.7.1.1 General Design Criterion 11, 1967 – Control Room

The plant control systems are designed to or contain instrumentation and controls that support actions to maintain the safe operational status of the plant from the control room or from an alternate location if control room access is lost due to fire or other causes.

7.7.1.2 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The plant control systems have instrumentation and controls to monitor and maintain variables within prescribed operating ranges.

7.7.1.3 General Design Criterion 13, 1967 – Fission Process Monitors and Controls

The plant control systems are designed to monitor and maintain control over the fission process throughout core life and for all conditions that can reasonably be anticipated to cause variations in reactivity of the core, such as indication of position of control rods and concentration of soluble reactivity control poisons.

7.7.1.4 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

The plant control systems are designed such that protection functions are separated from control instrumentation functions to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels.

7.7.1.5 General Design Criterion 26, 1971 – Reactivity Control System Redundancy and Capability

Two independent reactivity control systems of different design principles are provided, each having the capability to control the rate of reactivity changes resulting from planned, normal power changes. One of the systems is capable of reliably controlling anticipated operational occurrences. In addition, one of the systems is capable of holding the reactor core subcritical under cold conditions.

7.7.1.6 General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction

The rod control system is designed such that it is capable of sustaining any single malfunction, such as, unplanned continuous withdrawal (not ejection) of a control rod, without causing a reactivity transient which could result in exceeding acceptable fuel damage limits.

7.7.2 SYSTEM DESCRIPTION

The plant control systems described in Sections 7.7.2.1 through 7.7.2.10 perform the following functions:

(1) *Reactor Control System*

(a) Enables the nuclear plant to accept a step load increase or decrease of 10 percent, and a ramp increase or decrease of 5 percent per minute, within the load range of 15 to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.

(b) Maintains reactor coolant average temperature Tavg within prescribed limits by creating the bank demand signals for moving groups of rod cluster control assemblies (RCCAs) during normal operation and operational transients. The Tavg auctioneer unit supplies signals to pressurizer water level control and steam dump control.

(2) *Rod Control System*

(a) Provides for reactor power modulation by manual or automatic control of control rod banks in a preselected sequence, and for manual operation of individual banks

(b) Provides manual control of control banks to control the power balance between the top and bottom halves of the core

(c) Provides systems for monitoring and indicating:

1. Provide alarms to alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion

2. Display control rod position

3. Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit

(3) *Plant Control Signals for Monitoring and Indicating*

(a) Provide for measurement of reactor power level, axial power imbalance, and radial power imbalance

(b) Sense and display control rod position

(c) Provide warning to the operator of excessive rod insertion

(d) Provide an alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit

(e) Provide rod bottom alarm for individual dropped rods

(4) *Plant Control System Interlocks* (refer to Table 7.7-1)

(a) Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a departure from nucleate boiling ratio (DNBR) limit or kW/ft limit

(b) Initiate automatic turbine load runback on overpower or overtemperature

(5) *Pressurizer Pressure Control* - Maintains or restores the pressurizer pressure to the nominal operating pressure ±60 psi (which is well within reactor trip and relief and safety valve action setpoint limits) following normal operation transients that induce pressure changes by control (manual or automatic) of heaters and spray in the pressurizer. It also provides steam relief by controlling the power-operated relief valves

(6) *Pressurizer Water Level Control* - Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changes induced by loading, operational, and unloading transients. Level changes required to maintain the level within prescribed limits are produced by charging flow control (manual or automatic), as well as by manual selection of letdown orifices

(7) *Steam Generator Water Level Control*

(a) Establishes and maintains the steam generator water level to within predetermined physical limits during normal operating transients

(b) Restores the steam generator water level to within predetermined limits at unit trip conditions. Regulates the feedwater flow under operational transients to maintain the proper heat sink for the reactor coolant system (RCS). Steam generator water inventory control is manual or automatic through use of the digital feedwater control system (Reference 7).

(8) *Steam Dump Control*

(a) Permits the nuclear plant to accept a sudden loss of load without incurring reactor trip. Steam is dumped to the condenser and/or the atmosphere as necessary to accommodate excess power generation in the reactor during turbine load reduction transients

(b) Ensures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no-load conditions without actuation of the steam generator safety valves

(c) Maintains the plant at no-load conditions and permits a manually controlled cooldown of the plant

(9) *Incore Instrumentation* - Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations

(10) *Control Locations* - Provide central control and monitoring locations to perform plant operations both inside and outside the control room

7.7.2.1 Reactor Control System

The reactor control system enables the nuclear plant to follow load changes automatically, including the acceptance of step load increases or decreases of 10 percent, and ramp increases or decreases of 5 percent per minute within the load range of 15 to 100 percent without reactor trip, steam dump, or pressure relief, subject to possible xenon limitations. The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time.

The reactor control system controls the reactor coolant average temperature by regulation of control rod bank position. The reactor coolant loop average temperatures are determined from hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature (T_{avg}) computed for each loop, where:

$$T_{avg_i} = \frac{T_{have_i} + T_{cave_i}}{2} \qquad (7.7\text{-}1)$$

$$i = \text{loop numbers } 1 \rightarrow 4$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure), and the highest of the average loop measured temperatures (which is then processed through a lead-lag compensation unit) from each of the reactor coolant loops, constitutes the primary control signal as shown in general in Figure 7.7-1, and in more detail on the functional diagrams shown in Figure 7.2-1, Sheets 17 and 18. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The T_{avg} auctioneer unit also supplies a signal to pressurizer level control and steam dump control, and rod insertion limit monitoring.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response. The T_{avg} and T_{ref} signals are also supplied to the plant computer for a T_{avg} vs T_{ref} deviation alarm.

7.7.2.2 Rod Control System

7.7.2.2.1 Control Rod System

The control rod system receives rod speed and direction signals from the reactor control system. The rod speed demand signal varies over the corresponding range from 5 to 45 inches per minute (8 to 72 steps/minute), depending on the magnitude of the error signal. The rod direction demand signal is determined by the positive or negative value of the error signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the AUTOMATIC mode, and rod motion is then controlled by the reactor control system. A permissive interlock C-5 (refer to Table 7.7-1), derived from measurements of turbine impulse chamber pressure, prevents automatic withdrawal when the turbine load is below 15 percent. In the AUTOMATIC mode, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment. The manual and automatic controls are further interlocked with the control interlocks (refer to Table 7.7-1).

The shutdown banks are always in the fully withdrawn position during normal operation (except as required by surveillance testing) and are moved to this position prior to criticality. A reactor trip signal causes them to fall by gravity into the core. There are four shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod cluster control assemblies (RCCAs) in a group are electrically paralleled to move simultaneously. There is individual position indication for each RCCA.

Power to rod drive mechanisms is supplied by two motor generator sets operating from two separate 480-V, three-phase buses. Each generator is the synchronous type and is driven by a 150 hp induction motor. The ac power is distributed to the rod control power cabinets through the two series-connected reactor trip breakers.

The variable speed rod control system rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed.

A summary of the RCCA sequencing characteristics is provided below:

(1) Two groups within the same bank are stepped so that the relative position of the groups will not differ by more than one step.

(2) The control banks are programmed so that withdrawal of the banks is sequenced in the following order: control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence; i.e., the last control bank withdrawn (bank D) is the first control bank inserted.

(3) The control bank withdrawals are programmed so that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank. When the first bank reaches the top of the core, it stops, while the second bank continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power. The control bank insertion sequence is the opposite.

(4) Overlap between successive control banks is adjustable between 0 to 50 percent (zero and 115 steps), with an accuracy of ± 1 step.

(5) Rod speeds for either shutdown banks or control banks are capable of being controlled between a minimum of 8 steps per minute and a maximum of 72 steps per minute.

7.7.2.3 Plant Control Signals for Monitoring and Indicating

The following sections describe the monitoring and/or indicating functions provided by:

(1) Nuclear instrumentation system (7.7.2.3.1)

(2) Rod position (7.7.2.3.2)

(3) Control bank rod insertion monitoring (7.7.2.3.3)

(4) Rod deviation alarm (7.7.2.3.4)

(5) Rod bottom alarm (7.7.2.3.5)

7.7.2.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The nuclear instrumentation system (NIS) is described below and in detail in Reference 1. However, the Reference 1, Section 3.7 Item e, Ion-Chamber-Current Recorders (NR-41 through NR-44) description does not apply.

The power range channels are important because of their use in monitoring power distribution in the core within specified safe limits. They are used to measure reactor power level, axial power imbalance, and radial power imbalance. These channels are capable of recording power excursions up to 200 percent of full power. Suitable alarms are derived from these signals as described below.

Basic power range signals are:

(1) Total current from a power range detector (four such signals from separate detectors). These detectors are vertical and have a neutron sensitive length of 10 feet

(2) Current from the upper half of each power range detector (four such signals)

(3) Current from the lower half of each power range detector (four such signals)

Derived from these basic signals are the following (including standard signal processing for calibration):

(1) Indicated nuclear power (four such)

(2) Indicated axial flux imbalance, derived from upper half flux minus lower half flux (four such)

Alarm functions derived are as follows:

(1) Deviation (maximum minus minimum of four) in indicated nuclear power

(2) Upper radial tilt (maximum to average of four) on upper half currents

(3) Lower radial tilt (maximum to average of four) on lower half currents

Axial Flux Difference (AFD) limits are found in the cycle specific COLR (Core Operating Limits Report) for each unit. Technical Specifications provide the limiting values for the QPTR (Quadrant Power Tilt Ratio) limit.

Nuclear power and axial flux imbalance are selectable for recording. Indicators are provided on the control board for nuclear power and for axial flux imbalance.

7.7.2.3.2 Rod Position Monitoring

Two separate systems are provided to sense and display control rod position as described below:

(1) *Digital Rod Position Indication System (DRPI)* - The digital rod position indication system measures the actual position of each rod using a detector that consists of 42 discrete coils mounted concentric with the rod drive pressure housing. The coils are located axially along the pressure housing on 3.75 inch spacing. They magnetically sense the entry and presence of the rod drive shaft through its centerline. The coils are interlaced into two data channels and are connected to the containment electronics (Data A and B) by separate multiconductor cables. Multiplexing is used to transmit the digital position signals from the containment electronics to the control board display unit. The digital position signal is displayed on the main control board by light emitting diodes (LEDs) for each control rod. The one LED illuminated in the column shows the position for that particular rod. By employing two separate channels of information, the digital rod position indication system can continue to function (at reduced accuracy) when one channel fails.

Included in the system is a rod-at-bottom signal that operates a local alarm and a control room annunciator.

(2) *Demand Position Indication System* - The demand position indication system counts pulses generated in the rod drive control system to provide a digital readout of the demanded bank position.

The demand position indication and digital rod position indication systems are separate systems; each serves as a backup for the other. Operating procedures require the reactor operator to compare the demand and digital (actual) readings upon recognition of any apparent malfunction.

Therefore, a single failure in rod position indication does not in itself lead the operator to take erroneous action in the operation of the reactor.

The demand position indication system is described in detail in Reference 2.

7.7.2.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by RCS loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank:

(1) The low alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the chemical and volume control system (CVCS).

(2) The low-low alarm alerts the operator to take immediate action to add boron to the RCS by any one of several alternate methods.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip, provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection, and limits rod insertion so 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 must be decreased (the rods must be withdrawn further) with increasing power. Two parameters that are proportional to power are used as inputs to the insertion monitor. These are the ΔT between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg}, which is programmed as a function of power.

The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LLi} = K_{1i}\,\Delta T_{auct} + K_{2i}\,(T_{avg\ auct} - T_{no\text{-}load}) + K_{3i} \qquad (7.7\text{-}2)$$

where:

Z_{LLi} = maximum permissible insertion limit for affected control bank

i = A, B, C, and D respectively

$(\Delta T)_{auct}$ = highest ΔT of all loops

$(T_{avg})_{auct}$ = highest T_{avg} of all loops

K_{1i} = constants chosen to maintain $Z_{LLi} \geq$ actual limit based on physics
K_{2i} calculations
K_{3i}

The control rod bank demand position Z is compared to Z_{LLi} as follows:

If $Z - Z_{LLi} \leq D$, a low alarm is actuated
If $Z - Z_{LLi} \leq E$, a low-low alarm is actuated

where:

D, E = constants as described below

Since the highest values of T_{avg} and ΔT are chosen by auctioneering, a conservatively high representation of power is used in the insertion limit calculation.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Plant procedures require the operator to add boron through the CVCS. Actuation of the low-low alarm requires the operator to initiate emergency boration procedures. The value for E is chosen so that the low-low alarm would normally be actuated before the insertion limit is reached. The value for D is chosen to allow the operator to follow normal boration procedures. Figure 7.7-2 shows a block diagram of the control rod bank insertion monitor. The monitor is shown in more detail in the functional diagrams in Figure 7.2-1, Sheets 17 and 18. In addition to the rod insertion monitor for the control banks, an alarm system is provided to warn the operator if any shutdown RCCA leaves the fully withdrawn position. Rod insertion limits are found in the cycle specific COLR for each unit and are established by:

(1) Establishing the allowed rod reactivity insertion at full power, consistent with the purposes discussed above

(2) Establishing the differential reactivity worth of the control rods when moved in normal sequence

(3) Establishing the change in reactivity with power level by relating power level to rod position

(4) Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the initial and periodic physics testing program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of coolant boron concentration. Variations in concentration during

core life provide an additional check on the reactivity status of the reactor including core depletion.

7.7.2.3.4 Rod Deviation Alarm

The demanded and measured rod position signals are displayed on the control board. They are also monitored by the plant computer that provides an indication and an alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors. Rod alignment requirements are provided in the Technical Specifications.

Figure 7.7-3 is a block diagram of the rod deviation comparator and alarm system.

7.7.2.3.5 Rod Bottom Alarm

A rod bottom signal for each rod in the digital rod position system is used to operate a control relay, which generates the ROD BOTTOM ROD DROP alarm.

7.7.2.4 Plant Control System Interlocks

The listing of the plant control system interlocks, along with the description of their derivations and functions, is presented in Table 7.7-1. It is noted that the designation numbers for these interlocks are preceded by C. The development of these logic functions is shown in the functional diagrams (Figure 7.2-1, Sheets 17 to 32).

7.7.2.4.1 Rod Stops

Rod stops are provided to prevent abnormal power conditions that could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Rod stops are the C_1, C_2, C_3, C_4, and C_5 control interlocks identified in Table 7.7-1. The C_3 rod stop derived from overtemperature ΔT, and the C_4 rod stop derived from overpower ΔT, are also used for turbine runback, which is discussed below.

7.7.2.4.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. This prevents high power operation that might lead to an undesirable condition, which, if reached, would be protected by reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal. Two-out-of-four coincidence logic is used.

A rod stop and turbine runback are initiated when:

$\Delta T > \Delta T_{rod\ stop}$

For the overtemperature condition, an overtemperature ΔT (OTΔT) turbine runback (TR) occurs when:

$$\Delta T_i \left(\frac{1+\tau_4 s}{1+\tau_5 s} \right) - OT\Delta T_{setpoint_i} > OTTR_{setpoint_i}$$

$\Delta T_i = T_{havei} - T^f c_i$

T_{havei}, $T^f c_i$, τ_4, and τ_5 are defined in Section 7.2.2.1.2

$OT\Delta T_{setpoint_i}$ = -20 to +20% (usually zero)[(a)]

$OTTR_{setpoint_i}$ = -20 to +20% (usually negative)[(a)]

For the overpower condition, an overpower ΔT (OPΔT), turbine runback occurs when:

$$\Delta T_i \left(\frac{1+\tau_4 s}{1+\tau_5 s} \right) - OP\Delta T_{setpoint_i} > OPTR_{setpoint_i}$$

$\Delta T_i = T_{havei} - T^f c_i$

T_{havei}, $T^f c_i$, τ_4, and τ_5 are defined in Section 7.2.2.1.2

$OP\Delta T_{setpoint_i}$ = -20 to +20% (usually zero)[(a)]

$OPTR_{setpoint_i}$ = -20 to +20% (usually negative)[(a)]

ΔT setpoint refers to the overtemperature ΔT reactor trip value and the overpower ΔT reactor trip value for the two conditions. The turbine runback is continued until ΔT is equal to or less than $\Delta T_{rod\ stop}$.

This function serves to maintain an essentially constant margin to trip.

(a) The measured ΔT and ΔT setpoints should be in percent of full power ΔT. During initial plant operation, the ΔT channels were calibrated to indicate 100 percent at 100 percent power such that the channels do not reflect minor flow variations between loops or minor variations from design flow. Provisions to allow this calibration must be available in each channel before the ΔT signal is used for any alarm or protection function.

7.7.2.5 Pressurizer Pressure Control

The RCS pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportional plus integral controlled to correct small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure-controlled signal demands approximately 100 percent proportional plus integral heater power.

The spray nozzles are located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Three power operated relief valves limit system pressure for large positive pressure transients. In the event of a large load reduction, not exceeding the design plant load reduction capability, the pressurizer power-operated relief valves might be actuated for the most adverse conditions; e.g., the most negative Doppler coefficient and the minimum incremental rod worth. The relief capacity of the power-operated relief valves is sized large enough to limit the system pressure to prevent actuation of high-pressure reactor trip for the above condition.

A block diagram of the pressurizer pressure control system is shown in Figure 7.7-4.

7.7.2.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam-water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the RCS is maintained by the CVCS. During normal plant operation, charging flow varies to produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the highest average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes. To control pressurizer water level during startup and shutdown operations, the charging flow is

either automatically regulated with the controller setpoint adjusted to the desired level or manually regulated from the main control room. The pressurizer water level is programmed so that the water level is above the setpoint for heater cutout (refer to Section 7.7.3.2.2).

A block diagram of the pressurizer water level control system is shown in Figure 7.7-5.

7.7.2.7 Steam Generator Water Level Control

Each steam generator is equipped with a digital feedwater flow control system that maintains a constant steam generator (SG) water level over all power ranges. The feedwater controller regulates the MFRV and the bypass feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the programmed level, and the pressure-compensated steam flow signal. The digital feedwater control system has high and low power modes, determined by the feedwater flow measurement. The mode switch will automatically occur for a given loop when the feedwater flow in the subject loop reaches a predetermined valid value. In the low power mode, wide-range steam generator level provides a feedforward index to a single element feedwater control algorithm to anticipate nuclear steam supply system (NSSS) load changes. High power mode control is three element.

In both modes, feedwater temperature adjusts the level controller gain to account for variations in steam generator level dynamics with feedwater temperature. Narrow-range level is validated in both modes as the median value of the three isolated protection system level channels on each steam generator. As explained in WCAP-12221, this median signal selection (MSS) validation scheme meets the requirements of IEEE Std 279-1971 regarding separation of control and protection functions and control/protection interaction. The MSS was implemented to reduce the frequency of unscheduled trips resulting from equipment failure or human error during surveillance testing.

The feedwater pump speed is varied to maintain a programmed pressure differential between the average of the four steam generator steam line pressures and the feed pump discharge header. The speed demand controller continuously compares the actual differential pressure (DP) with a programmed DP_{ref} that is a linear function of steam flow. The speed demand controller then provides the feedpump speed demand to the feedpump speed control system. This system opens or closes the high pressure (HP) and low pressure (LP) governor valves for each pump to match the actual pump speed to the speed demand. The system also has a feature to back down or limit pump speed if pump discharge pressure is going high, to avoid feedpump trips on high discharge pressure due to feedwater system transients.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual override of the

feedwater control system is available at all times in the absence of a main feedwater isolation signal. Refer to Reference 7 for additional details.

A block diagram of the steam generator water level control system is shown in Figures 7.7-6 and 7.7-7.

7.7.2.8 Steam Dump Control

The steam dump system was originally designed to accept a 100 percent net load loss exclusive of the station auxiliaries without reactor or turbine trip. However, as described in Section 5.2.2.1.5.1, the design basis load reduction transient has been revised to a 50 percent step load reduction.

The automatic steam dump system is able to accommodate this abnormal load reduction and to reduce the effects of the transient imposed upon the RCS. By bypassing main steam directly to the condenser, an artificial load is thereby maintained on the primary system. The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions.

If the difference between the T_{ref} based on turbine impulse chamber pressure and the lead/lag compensated auctioneered T_{avg} exceeds a predetermined amount, and the interlock mentioned below is satisfied, a demand signal will actuate the steam dump to maintain the RCS temperature within control range until a new equilibrium condition is reached.

To prevent actuation of steam dump on small load perturbations, an independent load reduction sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. The circuit is provided to unblock the dump valves when the rate of load reduction exceeds a preset value corresponding to a 10 percent step load decrease or a sustained ramp load decrease of 5 percent per minute.

A block diagram of the steam dump control system is shown in Figure 7.7-8.

7.7.2.8.1 Load Rejection Steam Dump Controller

This circuit prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the lead-lag compensated auctioneered T_{avg} and the T_{ref}, which is based on turbine impulse chamber pressure.

The T_{avg} signal is the same as that used in the reactor control system. The lead-lag compensation for the T_{avg} signal is to compensate for lags in the plant thermal response and in valve positioning. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase, thus generating an immediate demand signal for

steam dump. Since control rods are available in this situation, steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.2.8.2 Reactor Trip Steam Dump Controller

Following a reactor trip above 15 percent power, the load rejection steam dump controller is defeated and the reactor trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead-lag compensated auctioneered T_{avg} and the no-load reference T_{avg}. When the error signal exceeds a predetermined setpoint, the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude, indicating that the RCS T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the reactor trip controller to regulate the rate of removal of decay heat and thus gradually establish the equilibrium hot shutdown condition.

The error signal determines whether a group of valves is to be tripped open or modulated open. In either case, they are modulated when the error is below the trip-open setpoints.

Some documentation may refer to the “reactor trip steam dump controller” as the “plant trip steam dump controller.”

7.7.2.8.3 Steam Header Pressure Controller

The removal of residual heat from the system is maintained by the steam header pressure controller (manually selected) that controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers that are used during the initial transient following turbine/reactor trip or load reduction. This mode of operation is used during startup and cooldown (turbine not paralleled), and when operating the turbine below approximately 15 percent load.

7.7.2.9 Incore Instrumentation

The incore instrumentation system consists of Chromel-Alumel thermocouples at fixed core outlet positions, and movable miniature neutron detectors that can be positioned at the center of selected fuel assemblies anywhere along the length of the fuel assembly vertical axis. The basic system for inserting these detectors is shown in Figure 7.7-9. Sections 1 and 2 of Reference 3 outline the incore instrumentation system in more detail.

7.7.2.9.1 Thermocouples

The incore thermocouple system has been upgraded to safety-grade to qualify the system for postaccident monitoring. The upgraded system is discussed in Section 7.5.2.2.2.

The plant computer is also used to monitor and display the incore thermocouple temperatures through Class 1E isolation devices provided in the upgraded thermocouple system.

7.7.2.9.2 Movable Neutron Flux Detector Drive System

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. Flux mapping is described in Section 7.7.2.9.3 and the use of the data is described in Section 4.3.3.2. Refer to Reference 3 for neutron flux detector parameters. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless steel sheathed coaxial cable. The retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits that extend from the bottom of the reactor vessel, down through the concrete shield area, and then up to a thimble seal table.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere.

Mechanical seals between the retractable thimbles and the conduits are provided at the seal line. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal line is provided for the retraction operation.

The drive system for inserting the miniature detectors consists basically of drive assemblies, five-path rotary transfer operation selector assemblies, ten-path rotary transfer selector assemblies, and stop valves, as shown in Figure 7.7-9. These assemblies are described in Reference 3. The drive system pushes hollow helical wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small-diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor that pushes a helical, wrap-drive cable and a detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

The leakage detection and gas purge provisions are discussed in Reference 3.

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, the valve forms a 2500 psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve prior to closing the valve.

A small leak would probably not prevent access to the isolation valves and, thus, a leaking thimble could be isolated during a hot shutdown. A large leak might require cold shutdown for access to the isolation valve. Access to the lower reactor cavity is provided through a small access room located below the incore instrumentation seal

area. During normal operations and hot or cold shutdown, the access room will be pressurized as cooling air from the containment heating, ventilating, and air conditioning (HVAC) system is forced through the lower reactor cavity. A normally closed PG&E Design Class I pressure relief shutter damper in the access room may be opened manually to relieve the pressure through the damper opening into the larger containment volume, thus reducing the pressure against the entry door and facilitating personnel access to the room. This damper contains counterweight devices that permit it to be automatically forced open if the pressure in the access room rises above the maximum normal operating pressure. In the event of a loss-of-coolant accident (LOCA), this damper will open and act as one of several reactor cavity subcompartment pressure-relief flowpaths.

7.7.2.9.2.1 Flux Thimble Tube Acceptance Criteria

The acceptance criteria to address nonlinear wear include capping or replacing flux thimble tubes that:

(1) showed greater than 25 percent wear per year; or

(2) had to be repositioned more than once; or

(3) had multiple wear scars with any two that measured greater than 40 percent; or

(4) had to be repositioned more than a total of 6 inches; or

(5) can not be inspected.

For wear above 40 percent, an additional predictability allowance of 5 percent is adequate to ensure that actual nonlinear wear does not exceed projected wear.

Based on Reference 11, 80 percent acceptance criterion, including 5 percent predictability uncertainty and 10 percent for eddy current testing instrument and wear scar uncertainty, PG&E will use a net acceptance criterion of 65 percent (References 9 and 10).

7.7.2.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The thimbles are distributed nearly uniformly over the core with about the same number of thimbles in each quadrant. The control system consists of two sections, one physically mounted with the drive units, and the other contained in the control room. Limit switches in each transfer device provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One five-path operation selector is provided for each drive unit to insert the detector in one of

five functional modes of operation. A ten-path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. A common path is provided to permit cross-calibration of the detectors.

The control room contains the necessary equipment for control, position indication, and flux recording for each detector. Panels are provided to indicate the position of the detectors and to plot the flux level. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting, and gain controls.

A flux mapping consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom. Other core locations are selected and plotted in a similar manner. Each detector provides axial flux distribution data along the center of a fuel assembly. Various radial positions of detectors may then be compared to obtain a flux map for a region of the core.

Operating plant experience has demonstrated the adequacy of the incore instrumentation system in meeting the design bases stated.

7.7.2.10 Control Locations

7.7.2.10.1 Control Room

A common control room for Unit 1 and Unit 2 contains the controls and instrumentation necessary for operating each unit's reactor and turbine-generator during normal and accident conditions. The control boards for Unit 2 are physically separated from the Unit 1 control boards. The control room is continuously occupied by licensed operating personnel during all operating conditions. It is also expected to be continuously occupied during all accident conditions. In the remote case where it is not possible to occupy the control room, alternative control locations are provided. The control room for each unit is designed to normally accommodate three to five people.

Sufficient shielding, distance, and containment integrity are provided to ensure that control room personnel are not subjected to doses under postulated accident conditions that would exceed 5 rem TEDE. The doses received by the operator during both entry and exit is expected to be minimal (refer to Section 15.5 and Table 15.5-33 for detail). Control room ventilation is provided by a system capable of having a large percentage of recirculated air. The fresh air intake can be closed to limit the intake of airborne activity if monitors indicate that such action is appropriate. (A complete discussion of control room ventilation and air conditioning is presented in Chapter 9.)

Provisions are made so that plant operators can readily shut down and maintain the plant at hot standby by means of controls located outside the control room at central alternative locations, one for each unit, in the auxiliary building.

Control room arrangement is shown in Figure 7.7-16.

7.7.2.10.1.1 Main Control Boards

The control board design and layout presents all the controls, indicators, recorders, and alarms required for the safe startup, operation, and shutdown of the plant.

The control board layout is based on operator ease in relating the control board devices to the physical plant and determining, at a glance, the status of related equipment. This is referred to as providing a functional layout. Within the boundaries of a functional layout, modules are arranged in columns of control functions associated with separation trains defined for the reactor protection and Engineered Safety Features (ESF) systems. Teflon-coated wire is used within the module and between the module and the first termination point.

Modular train column wiring is formed into wire bundles and carried to metal wireways (gutters). Gutters are run into metal vertical wireways (risers). The risers are the interface between field wiring and control board wiring. Risers are arranged to maintain the separated routing of the field wire trays.

Alarms and annunciators on the control board provide warning of abnormal plant conditions that might lead to possible unsafe conditions. An annunciator terminal display and logger printer are also available in the main control room. Indicators and recorders are provided for observation of instantaneous and trend values of plant operating conditions. The charts are also used for record-keeping purposes.

The bench-vertical control boards and control console are arranged to afford the operator instant access to the continuing controllers, recorders, and indicators, while allowing easy access to all the other controls. Refer to Figure 7.7-17.

The control console houses the reactor controls, plant process computer terminals, turbine controls, and generator controls. These are arranged from left to right of an operator sitting at the console. Various trip switches and safety system indicators are also located on the console. Refer to Figures 7.7-18 and 7.7-19.

The bench-vertical board houses the indicators, recorders, and controllers for ESF, primary plant, steam generator, turbine-generator, ventilation, diesel generator, and station electrical systems. These instruments, however, do not require the immediate attention of the operator as do those located on the control console. Refer to Figures 7.7-20 through 7.7-29.

Indication provided in the control room is discussed under the description of each individual system.

A process computer is used to provide supplementary information to the operator and to effectively assist in the operation of the NSSS. However, the analog indication provides the operator with ample information for safe operation without the computer system.

The plant operator's computer panel is located on the control console for easy access to information. A plant process computer terminal display is also at this location.

7.7.2.10.1.1.1 Main Annunciator System

The function of the main annunciator system is to monitor the status of selected plant equipment, systems and components, and to alert the Plant Operations Staff when an abnormal (alarm) condition is detected. The design of the main annunciator system is described in Section 3.10.3.9.

A partial list of annunciator displays includes:

(1) Loss of power supplies

(2) SSPS trouble

(3) SSPS in test

(4) NIS detector loss

(5) NIS channel test

(6) NIS trip bypass

(7) Hot shutdown panel open

(8) Hot shutdown panel in control

(9) Heat tracing fault (boric acid systems)

(10) Radiation monitoring system failure

(11) Radiation monitoring system in test

(12) Diesel generator system

(13) NIS reactor trip bypass

(14) NIS rod stop bypass

(15) Containment high-high pressure in test

(16) Process protection system (PPS) channel in bypass

(17) PPS channel set failure

(18) PPS trouble

(19) PPS RTD failure

(20) Steam generator trip time delay timer actuated

7.7.2.10.1.2 Occupancy Requirements

The control room area that is located in the auxiliary building at elevation 140 feet is designed for safe occupancy during abnormal conditions. Adequate shielding is used to maintain acceptable radiation levels in these areas under all normal operating and accident conditions. Radiation detectors and smoke detectors are provided to monitor the air intake and to initiate appropriate alarms and modes of operation. Air conditioning is included with provisions for the air to be recirculated through charcoal filters. Emergency lighting is provided in the control room area.

Fire hazards in the control room area are limited by the following:

(1) Noncombustible materials are used in construction where possible. Structural and finish materials (including furniture) for the control room and interconnecting areas have been selected on the basis of fire-retardant characteristics. Structural floors and exterior and interior walls are of reinforced concrete. Interior partitions within the control room areas incorporate concrete blocks, metal, and gypsum drywalls on metal studs. The control room door frames and doors are metallic. Personnel doors are tight fitting and gasketed. Wood trim is not used.

(2) Control cables are provided with an individual flame-retardant insulation over each single conductor and overall flame-retardant jacket over multiconductor cables. Cables throughout the installation have an exterior jacket that meets the Insulated Power Cable Engineers Association (IPCEA) requirements. Shielded instrumentation cables are provided with fire-resistant insulation and covered with a jacket of the same material. For a more detailed discussion on insulated cable construction, refer to Appendix 8.3B and Sections 8.3.1.2 and 8.3.1.4.3.

(3) All pressure information is transmitted to the control room by electrical signals. No high-pressure fluids are piped into the control room.

(4) Combustible materials are administratively controlled in the control room area.

(5) Combustible supplies, such as logs, records, procedures, and manuals, are limited to the amounts required for current operation.

(6) Detectors, sensitive to smoke and combustibles, are located in the vicinity of equipment cabinets and in the air conditioning system ducts. Fire detection alarms are provided in the control room with indication of which detector has been actuated.

(7) All areas of the control room are readily accessible for fire extinguishing.

(8) Adequate fire extinguishers and breathing apparatus that are easily accessible are provided and are to be used in accordance with National Fire Code (NFC) and National Fire Protection Association (NFPA) requirements. This equipment is provided to control any fire that could occur.

(9) The control room is occupied at all times by an operator who has been trained in fire extinguishing techniques.

Therefore, as a result of these provisions, any fires in the control room area are expected to be of such small magnitude that they could be extinguished by the operator using a hand fire extinguisher. The resulting smoke and vapors would be removed by the air conditioning system.

The control room area is protected from infiltration of fire, smoke, or airborne radioactivity from outdoors and other areas of the auxiliary building by minimum leakage penetrations, weather-stripped doors, absence of outside windows, and the positive air pressure maintained in the area during normal and accident operation.

A smoke detection device provides warning so that the operator can take steps to minimize any hazard (refer to Section 9.4).

An area radiation detector monitors the control room for radiation content and will alert the operator to a high radioactivity level.

There are additional area radiation monitors in the auxiliary building and containment structures that provide the plant operator with a warning of unexpected high levels of radioactivity. Process monitors located in the residual heat removal exhaust ducts, component cooling water system, and liquid and gaseous radwaste systems also warn the operator of higher than expected concentrations of radioactivity. A plant vent gas process monitor is backed up by an air particulate monitor that can also sample the containment air and detect primary plant piping leaks within containment. For a complete discussion of the radiation monitoring system, refer to Section 11.4.

Should the operator be forced to leave the control room, operating procedures require that the operator first trip the reactor and turbine-generator through manual trip switches located on the console. The operator would then verify the reactor trip and the turbine

trip using approved plant procedures. After the reactor and turbine have tripped, plant controls automatically bring the plant to no-load condition after which it is necessary only to control the removal of decay heat and to maintain the water level in the pressurizer to maintain the plant in a safe condition. The operator would monitor and control these operations from the hot shutdown panel.

7.7.2.10.2 Hot Shutdown Panel

The hot shutdown panel, which is located in the auxiliary building at elevation 100 feet (refer to Figure 7.7-30), contains control stations, switches, and indicators to:

(1) Enable the operator to control water level in the steam generators with the auxiliary feedwater system (pumps and valves)

(2) Display auxiliary feedwater pump discharge pressure, auxiliary feedwater flow, auxiliary feedwater source levels, steam generator pressure and level, pressurizer pressure and level, emergency borate flow, charging flow, source range neutron flux, and Class 1E 4.16-kV bus voltages. Display RCS loop 4 wide range hot leg and cold leg temperatures.

(3) Enable the operator to manipulate the 10 percent atmospheric dump valves

(4) Start and stop:

(a) Component cooling water pumps (3)

(b) Auxiliary saltwater pumps (2)

(c) Charging pumps CCP1 and CCP2 (2)

(d) Boric acid transfer pumps (2)

(e) Containment fan coolers (5)

(5) Control:

(a) Emergency boric acid valve (1)

(b) Charging flow control valves (2)

(c) Power-operated relief valves (PORVs) for the pressurizer (close only) (3)

(d) RCP seal injection back-pressure

(e) RCP seal injection pressure

(f) RWST to charging pump suction header isolation valve (1)

(g) Charging line isolation valves (2)

(h) Charging to loop 4 isolation valve (1)

Boric acid concentration can be verified by reading the boron analyzer local indication or by sampling and analysis.

Transfer switches are located on this panel to allow the operator to activate these controls individually. Transfer switches for items (f) and (g) are in the associated vital 480V motor control center and the transfer switch for item (h) is in the associated 125 VDC inverter room. Except for motor-driven equipment, any transfer switch operation will cause annunciation in the control room. For motor-driven equipment, refer to Section 7.4.1.2.1(4).

The hot shutdown panel for plant shutdown and decay heat removal would be used only under abnormal conditions when access to the control room has been lost, and not during normal plant operation. The controls and indicators are located behind doors of the main panel and under the lids of the sub-panels to reduce the possibility of misoperation during normal operation. An alarm is initiated when a main panel door or the switch sub-panel lid or maintenance hatch is opened.

The indications and controls listed above are required for remote shutdown and/or Title 10, U.S. Code of Federal Regulations, Part 50.48(c), NFPA 805 purposes. Other indications and controls located on the hot shutdown panel are for operator convenience (additional indications and controls required for remote shutdown and NFPA 805 are located elsewhere throughout the plant.

7.7.2.10.3 Auxiliary Building Control Board

The auxiliary building control board, which is located in the auxiliary building at elevation 85 feet (refer to Figure 7.7-31), contains the controls, indicators, and alarm functions for:

(1) CVCS (Unit 1)

(2) Common panel for radioactive waste handling

(3) CVCS (Unit 2)

The control system provides a mimic for the radioactive waste handling system to aid the operator in setting up these systems.

7.7.2.10.4 Auxiliary Control Stations

Local control panels are provided for systems and components that do not require full-time operator attendance or are not used on a continuous basis. Examples of such systems are the waste disposal system and the turbine-generator hydrogen cooling system. In these cases, however, appropriate alarms are activated in the control room to alert the operator to an equipment malfunction or approach to unsafe conditions.

7.7.3 SAFETY EVALUATION

7.7.3.1 General Design Criterion 11, 1967 – Control Room

The plant is provided with a centralized control room common to both Unit 1 and Unit 2 that contains the controls and instrumentation necessary for operation of both units under normal and accident conditions. Should the operator be forced to leave the control room, operating procedures require that the operator first trip the reactor and turbine-generator through manual trip switches located on the console. Provisions are made so that plant operators can readily shut down and maintain the plant at hot standby by means of controls located outside of the control room. Refer to Section 7.7.2.10.

Proper positioning of the control rods is monitored in the control room by bank arrangements of the individual column meters for each RCCA. A rod deviation alarm alerts the operator of a deviation of one RCCA from the other rack in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each RCCA. Four out-of-core long ion chambers also detect asymmetrical flux distribution indicative of rod misalignment.

7.7.3.2 General Design Criterion 12, 1967 – Instrumentation and Control Systems

The plant control systems are designed to ensure high reliability in any anticipated operational occurrences. Equipment used in these systems is designed and constructed to maintain a high level of reliability.

7.7.3.2.1 Step Load Changes without Steam Dump

The plant control systems restore equilibrium conditions, without a trip, following a $\pm$ 10 percent step change in load demand, over the 15 to 100 percent power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10 percent. A load demand greater than full power is prohibited by the turbine control load limit devices.

The plant control systems minimize the reactor coolant average temperature deviation during the transient within a given value, and restore average temperature to the

programmed setpoint. Excessive pressurizer pressure variations are prevented by using spray and heaters and power operated relief valves in the pressurizer.

The control systems limit nuclear power overshoot to acceptable values following a 10 percent increase in load to 100 percent.

7.7.3.2.2 Loading and Unloading

Ramp loading and unloading of 5 percent per minute can be accepted over the 15 to 100 percent power range under automatic control without tripping the plant. The function of the control systems is to maintain the coolant average temperature as a function of turbine-generator load.

The coolant average temperature increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer heaters limit the resulting system pressure decrease. The pressurizer water level is programmed so that the water level is above the setpoint for heater cutout during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the overtemperature ΔT setpoint.

7.7.3.2.3 Load Reduction Furnished by Steam Dump System

When a load reduction occurs, if the difference between the required temperature setpoint of the RCS and the actual average temperature exceeds a predetermined amount, a signal will actuate the steam dump to maintain the RCS temperature within control range until a new equilibrium condition is reached.

The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic. The steam dump flow reduction is as fast as RCCAs are capable of inserting negative reactivity.

The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is nominally 40 percent of full load steam flow at full load steam pressure.

The steam dump flow reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated by the reactor coolant average temperature signal. The required number of steam dump valves can be tripped quickly to stroke full open or

modulate, depending on the magnitude of the temperature error signal resulting from loss of load.

7.7.3.2.4 Turbine-Generator Trip with Reactor Trip

Whenever the turbine-generator unit trips at an operating power level above the protection system interlock P-9 setting, the reactor also trips. The unit is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the safety valve setpoint. The thermal capacity of the RCS is greater than that of the secondary system, and because the full load average temperature is greater than the no-load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for a trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators.

The steam dump system is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the 10 percent atmospheric dump valves open, the average coolant temperature starts to reduce quickly to the no-load setpoint. A direct feedback of temperature acts to close the valves proportionally to minimize the total amount of steam that is bypassed.

Following the turbine trip, the feedwater flow is cut off when the average coolant temperature decreases below a given temperature, or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level, while ensuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) that controls the amount of steam flow to the condensers. This controller operates a portion of the same 40 percent condenser dump valves to the condensers that are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and water level fall rapidly during the transient because of coolant contraction. Following the turbine and reactor trip, the pressurizer level control follows RCS T_{avg} to its no load value. If heaters become uncovered following the trip, they are deenergized and the CVCS will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressure to normal.

The steam dump feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip to ensure adequate reactivity shutdown margin.

7.7.3.2.5 General Considerations

The plant control systems prevent an undesirable condition in the operation of the plant that, if reached, would be protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst-case failure modes of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as the following:

(1) Uncontrolled RCCA withdrawal from a subcritical condition

(2) Uncontrolled RCCA withdrawal at power

(3) RCCA misalignment

(4) Loss of external electric load and/or turbine trip

(5) Loss of all ac power to the station auxiliaries

(6) Excessive heat removal due to feedwater system malfunctions

(7) Excessive load increase

(8) Accidental depressurization of the RCS

These analyses show that a reactor trip setpoint is reached in time to protect the health and safety of the public under these postulated incidents, and that the resulting coolant temperatures produce a DNBR well above the applicable limit value (refer to Sections 4.4.4.1 and 4.4.3.3). Thus, there will be no cladding damage and no release of fission products to the RCS under the assumption of these postulated worst case failure modes of the plant control systems.

7.7.3.3 General Design Criterion 13, 1967 – Fission Process Monitors and Controls

Overall reactivity control is achieved by the combination of soluble boron and RCCAs. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes is accomplished by the plant control systems that automatically move RCCAs. This system uses input signals including neutron flux, coolant temperature, and turbine load.

7.7.3.4 General Design Criterion 22, 1967 – Separation of Protection and Control Instrumentation Systems

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation devices contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel.

Accordingly, this postulated failure mode meets the requirements of GDC 22, 1967. Test results have proved that failure of any single control system component or channel did not perceptibly disturb the protection side (input) of the devices.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action, and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Paragraph 4.7 of IEEE-279-1971 (Reference 5).

Channels of the nuclear instrumentation that are used in the protective system are combined to provide nonprotective functions, such as signals, to indicating or recording devices; the required signals are derived through isolation devices.

These isolation devices are designed so that open or short circuit conditions, as well as the application of 120-Vac or 140-Vdc to the isolation side of the circuit, will have no effect on the input, or protection, side of the circuit. As such, failures on the nonprotective side of the system will not affect the individual protection channels.

7.7.3.5 General Design Criterion 26, 1971 – Reactivity Control System Redundancy and Capability

Two independent reactivity control systems are provided for each reactor. These are RCCAs and chemical shim (boration).

Overall reactivity control is achieved by the combination of soluble boron and RCCAs. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes is accomplished by the plant control systems that automatically move RCCAs. This system uses input signals including neutron flux, coolant temperature, and turbine load.

No single electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single RCCA from the partially inserted bank at full power operation. The operator could deliberately withdraw a single RCCA in the control bank; this feature is necessary in order to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures that could result in single withdrawal, rod deviation would be displayed on the plant annunciator, and the rod position indicators would indicate the relative positions of the rods in the bank. Withdrawal of a single RCCA by operator action, whether deliberate or by a combination of errors, would result in activation of the same alarm and the same visual indications.

The control and shutdown rods are arranged as follows:

Control Shutdown

Bank A Group 1	Bank A Group 1
Bank A Group 2	Bank A Group 2
Bank B Group 1	Bank B Group 1
Bank B Group 2	Bank B Group 2
Bank C Group 1	Bank C One Group
Bank C Group 2	Bank D One Group
Bank D Group 1	
Bank D Group 2	

The rods in a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially so that the first group is always within one step of the second group in the bank. A definite schedule of actuation or deactuation of the stationary gripper, movable gripper, and lift coils of a mechanism is required to withdraw the RCCA attached to the mechanism. Since the four stationary grippers, movable grippers, and lift coils associated with the RCCAs of a rod group are driven in parallel, any single failure that could cause rod withdrawal would affect a minimum of one group of RCCAs. Mechanical failures are in the direction of insertion, or immobility.

The identified multiple failure involving the least number of components consists of open circuit failure of the proper two out of sixteen wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is 0.016 x 10-6 per hour by MIL HDBK-217A (Reference 6). These wire failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is therefore too low to have any significance.

Concerning the human element, to erroneously withdraw a single RCCA, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indications would have to be disregarded or ineffective. Such a series of errors would require a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as these. Such a number would be highly subjective.

The rod position indication provides direct visual displays of each control rod assembly position. The plant computer alarms for deviation of rods from their banks. In addition, a rod insertion limit monitor provides an audible and visual alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to follow emergency boration procedures. The facility reactivity control systems are such that acceptable fuel damage limits will not be exceeded in the event of a single malfunction of either system.

An important feature of the control rod system is that insertion is provided by gravity fall of the rods.

In all analyses involving reactor trip, the single, highest worth RCCA is postulated to remain untripped in its full out position.

One means of detecting a stuck control rod assembly is available from the actual rod position information displayed on the control board. The control board position readouts for each rod give the plant operator the actual position of the rod in steps. The indications are grouped by banks (e.g., control bank A, control bank B, etc.) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The plant computer monitors the actual position of all rods. Should a rod be misaligned from the other rods in that bank by more than 12 steps, the rod deviation alarm is actuated.

Misaligned RCCAs are also detected and alarmed in the control room via the flux tilt (QPTR) monitoring system that is independent of the plant computer.

Isolated signals derived from the NIS are compared with one another to determine if a preset amount of deviation of average power has occurred. Should such a deviation occur, the comparator output will operate a bistable unit to actuate a control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By use of individual rod position readouts, the operator can determine the deviating control rod and take corrective action. Thus, the design of the plant control systems meets the applicable requirements of GDC 12, 1967 and GDC 31, 1967.

The boron system can compensate for all xenon burnout reactivity transients without exception.

The rod system can compensate for xenon burnout reactivity transients over the allowed range of rod travel. Xenon burnout transients of larger magnitude must be accommodated by boration or by reactor trip (which eliminates the burnout).

The boron system is not used to compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes.

The rod system can compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes over the full range from full-load to no-load at the design maximum load uprate.

Automatic control of the rods is, however, limited to the range of approximately 15 to 100 percent of rating for reasons unrelated to reactivity or reactor safety.

The boron system (by the use of administrative measures) will maintain the reactor in the cold shutdown state, irrespective of the disposition of the control rods.

The overall reactivity control achieved by the combination of soluble boron and RCCAs meets the applicable requirements of GDC 27, 1967.

7.7.3.6 General Design Criterion 31, 1967 – Reactivity Control Systems Malfunction

Reactor shutdown with control rods is completely independent of the control functions since the trip breakers interrupt power to the rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. Thus, the design meets the applicable requirements of GDC 31, 1967.

7.7.4 REFERENCES

1. J. B. Lipchak and R. A. Stokes, Nuclear Instrumentation System, WCAP-7669, April 1971.

2. A. E. Blanchard, Rod Position Monitoring, WCAP-7571, March 1971.

3. J. J. Loving, In-Core Instrumentation (Flux-Mapping System and Thermocouples), WCAP-7607, July 1971.

4. Deleted in Revision 21.

5. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc.

6. MIL-HDBK-217A, Reliability Prediction of Electronic Equipment, December 1965.

7. Advanced Digital Feedwater Control System Input Signal Validation for Pacific Gas and Electric Co., Diablo Canyon Units 1 and 2, WCAP - 12221, April 1997 (W Proprietary Class 3) (PGE-97-540) and WCAP - 12222, March 1989 (W Proprietary Class 3).

8. Westinghouse Protection System Noise Tests, WCAP - 12358, Revision 2, October 1975 (W Proprietary Class 3).

9. PG&E Letter DCL-11-037, Response to Telephone Conference Calls Held on February 2 and 4, 2011, Between the U.S. Nuclear Regulatory Commission and Pacific Gas and Electric Company Concerning Responses to Requests for Additional Information Related to the Diablo Canyon Nuclear Power Plant, Units 1 and 2, License Renewal Application, dated March 25, 2011.

10. NRC Letter to PG&E, Safety Evaluation Report Related to the License Renewal of Diablo Canyon Nuclear Power Plant, Units 1 and 2, dated June 2, 2011 (Section 3.0.3.1.2).

11. Westinghouse Commercial Atomic Power (WCAP) - 12866, Bottom Mounted Instrumentation Flux Thimble Wear, January 1991

7.7.5 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

TABLE 7.1-1

APPLICABLE DESIGN BASIS CRITERIA

CRITERIA	TITLE	APPLICABILITY					
Instrumentation and Controls		Reactor Trip System (RTS)	Engineered Safety Features Actuation System (ESFAS)	Systems Required for Safe Shutdown	Safety-Related Display Instrumentation	All Other Instrumentation Systems Required for Safety	Control Systems Not Required for Safety
Section		7.2	7.3	7.4	7.5	7.6	7.7
1. General Design Criteria							
Criterion 2, 1967	Performance Standards	X	X		X	X	
Criterion 3, 1971	Fire Protection			X			
Criterion 11, 1967	Control Room	X	X	X	X	X	X
Criterion 12, 1967	Instrumentation and Control System	X		X	X	X	X
Criterion 13, 1967	Fission Process Monitors and Controls						X
Criterion 14, 1967	Core Protection Systems	X					
Criterion 15, 1967	Engineered Safety Features Protection Systems		X				
Criterion 17, 1967	Monitoring Radioactivity Releases				X		
Criterion 19, 1967	Protection Systems Reliability	X	X				
Criterion 20, 1967	Protection Systems Redundancy and Independence	X	X				
Criterion 21, 1967	Single Failure Definition	X	X				
Criterion 22, 1967	Separation of Protection Control Instrumentation Systems	X	X				X
Criterion 23, 1967	Protection Against Multiple Disability for Protection Systems	X	X				
Criterion 24, 1967	Emergency Power for Protection Systems	X	X				
Criterion 25, 1967	Demonstration of Functional Operability of Protection Systems	X	X				
Criterion 26, 1967	Protection Systems Fail-Safe Design	X	X				

TABLE 7.1-1

APPLICABLE DESIGN BASIS CRITERIA

CRITERIA	TITLE	APPLICABILITY					
Instrumentation and Controls		Reactor Trip System (RTS)	Engineered Safety Features Actuation System (ESFAS)	Systems Required for Safe Shutdown	Safety-Related Display Instrumentation	All Other Instrumentation Systems Required for Safety	Control Systems Not Required for Safety
Section		7.2	7.3	7.4	7.5	7.6	7.7
Criterion 27, 1967	Redundancy of Reactivity Control						X
Criterion 31, 1967	Reactivity Control Systems Malfunction	X					X
Criterion 37, 1967	Engineered Safety Features Basis for Design		X				
Criterion 38, 1967	Reliability and Testability of Engineered Safety Features		X				
Criterion 40, 1967	Missile Protection		X				
Criterion 48, 1967	Testing of Operational Sequence of Emergency Core Cooling Systems		X				
Criterion 49, 1967	Containment Design Basis	X	X				
2. 10 CFR Part 50							
50.49	Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants	X	X		X	X	
50.62	Requirements for Reduction of Risk from Anticipated Transients without Scrams (ATWS) Events for Light-Water-Cooled Nuclear Power Plants					X	
3. Atomic Energy Commission (AEC) Safety Guides							
Safety Guide 22, February 1972	Periodic Testing of Protection System Actuation Functions	X	X				
4. Regulatory Guides							
Regulatory Guide 1.97, Revision 3, May 1983	Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and				X		

TABLE 7.1-1

APPLICABLE DESIGN BASIS CRITERIA

CRITERIA	TITLE	APPLICABILITY					
Instrumentation and Controls		Reactor Trip System (RTS)	Engineered Safety Features Actuation System (ESFAS)	Systems Required for Safe Shutdown	Safety-Related Display Instrumentation	All Other Instrumentation Systems Required for Safety	Control Systems Not Required for Safety
Section		7.2	7.3	7.4	7.5	7.6	7.7
	Following an Accident						
5. NRC NUREG							
NUREG-0737 (Item I.D.2), November 1980	Clarification of TMI Action Plan Requirements				X		
NUREG-0737 (Item II.D.3), November 1980	Clarification of TMI Action Plan Requirements				X		
NUREG-0737 (Item II.E.1.2), November 1980	Clarification of TMI Action Plan Requirements				X		
NUREG-0737 (Item II.F.1), November 1980	Clarification of TMI Action Plan Requirements				X		
NUREG-0737 (Item II.F.2), November 1980	Clarification of TMI Action Plan Requirements				X		
NUREG-0737 (Item II.K.3.10), November 1980	Clarification of TMI Action Plan Requirements	X					
NUREG-0737 (Item II.K.3.12), November 1980	Clarification of TMI Action Plan Requirements	X					
NUREG-0737 (Item II.A.1.2), November 1980	Clarification of TMI Action Plan Requirements				X		
6. NRC Generic Letters							
Generic Letter 83-28, July 1983	Required Actions Based on Generic Implications of Salem ATWS Events	X					

TABLE 7.2-1

LIST OF REACTOR TRIPS

Reactor Trip	Coincidence Logic	Interlocks	Comments
1. Power range high nuclear power	2/4	Manual block of low setting permitted by P-10	High and low settings; manual and automatic reset of low setting by P-10
2. Intermediate range high neutron flux	1/2	Manual block permitted by P-10	Manual block and automatic reset
3. Source range high neutron flux	1/2	Manual block permitted by P-6, interlocked with P-10	Manual block and automatic reset. Automatic block above P-10
4. Power range high positive nuclear power rate	2/4	No interlocks	-
5. Deleted in Revision 20.		-	-
6. Overtemperature ΔT	2/4	No interlocks	-
7. Overpower ΔT	2/4	No interlocks	-
8. Pressurizer low pressure	2/4	Interlocked with P-7	Blocked below P-7
9. Pressurizer high pressure	2/4	No interlocks	-

TABLE 7.2-1

Reactor Trip	Coincidence Logic	Interlocks	Comments
10. Pressurizer high water level	2/3	Interlocked with P-7	Blocked below P-7
11. Reactor coolant low flow	2/3 per loop	Interlocked with P-7 and P-8	Low flow in one loop will cause a reactor trip when above P-8 and a low flow in two loops will cause a reactor trip with permissive P-7 enabled. Blocked below P-7
12. Reactor coolant pump breakers open or redundant breaker open	2/4	Interlocked with P-7	Blocked below P-7
13. Reactor coolant pump bus under-voltage	1/2 on both buses	Interlocked with P-7	Low voltage on all buses permitted below P-7
14. Reactor coolant pump bus under-frequency	2/3 on either bus	Interlocked with P-7	Underfrequency on 2/3 sensors on either bus will trip reactor if above P-7 setpoint
15. Steam generator low- low level	2/3 per loop	No interlocks	-

TABLE 7.2-1

Reactor Trip	Coincidence Logic	Interlocks	Comments
16. Safety injection signal	Coincidence with actuation of safety injection	No interlocks	(See Section 7.3 for engineered safety features actuation conditions)
17. Turbine trip-Reactor trip			
a. Low autostop oil pressure	2/3	Interlocked with P-9	Blocked below P-9
b. Turbine stop valve close	4/4	Interlocked with P-9	Blocked below P-9
18. Manual	1/2	No interlocks	Reactor trip or Safety Injection Signal Actuation
19. Seismic	2/3 per axis	No interlocks	-
20. Reactor trip/bypass breakers	2/2	No interlocks	Both trains
21. Automatic trip logic	1/2	No interlocks	Both trains
22. General warning	2/2	No interlocks	Both trains

TABLE 7.2-2

PROTECTION SYSTEM INTERLOCKS

Designation	Derivation	Function
	Power Escalation Permissives	
P-6	1/2 Neutron flux (intermediate range) above setpoint	Allows manual block of source range reactor trip
	2/2 Neutron flux (intermediate range) below setpoint	Defeats the block of source range reactor trip
P-10	2/4 Nuclear power (power range) above setpoint	Allows manual block of power range (low setpoint) reactor trip
		Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Blocks source range reactor trip (backup for P-6)
		Blocks subcooled margin monitor lo-margin alarm
	3/4 Nuclear power (power range) below setpoint	Defeats the block of power range (low set- point) reactor trip
		Defeats the block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Input to P-7
		Enables subcooled margin monitor lo-margin alarm

TABLE 7.2-2

Designation	Derivation	Function
	Blocks of Reactor Trips	
P-7	3/4 Nuclear power (power range) below setpoint (from P-10), and 2/2 turbine impulse chamber pressure below setpoint (from P-13)	Blocks reactor trip on: low flow or reactor coolant pump breakers open in more than one loop, undervoltage, underfrequency, pressurizer low pressure, and pressurizer high level
P-8	3/4 Nuclear power (power range) below setpoint	Blocks reactor trip on low flow in a single loop
P-9	3/4 Neutron Flux (power range) below setpoint	Blocks reactor trip on turbine trip
P-13	2/2 Turbine impulse chamber pressure below setpoint	Input to P-7

TABLE 7.3-1

INSTRUMENTATION OPERATING CONDITION
FOR ENGINEERED SAFETY FEATURES

No.	Functional Unit	No. of Channels	No. of Channels To Trip
1.	Safety Injection		
	a. Manual	2	1
	b. High containment pressure	3	2
	c. Pressurizer low pressure	4	2
	d. Low steam line pressure (lead/lag compensated)	12 (3/steam line)	2/3 in any steam line
2.	Containment Spray		
	a. Manual	2	2 coincident
	b. Containment pressure high-high	4	2

TABLE 7.3-2

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
INSTRUMENTATION OPERATING CONDITIONS FOR ISOLATION FUNCTIONS

No.	Functional Unit	No. of Channels	No. of Channels To Trip
1.	Containment Isolation		
	a. Safety injection (Phase A)	(See Item No. 1 of Table 7.3-1)	
	b. Containment pressure (Phase B)	(See Item No. 2b of Table 7.3-1)	
	c. Manual		
	Phase A	2	1
	Phase B	(See Item No. 2a of Table 7.3-1)	
2.	Steam Line Isolation		
	a. Low steam line pressure (lead/lag compensated)	(See Item No. 1d of Table 7.3-1)	
	b. High steam pressure rate (rate lag compensated)	12 (3/steam line)	2/3 in any steam line
	c. Containment pressure high- high 2/4	(See Item No. 2b of Table 7.3-1)	
	d. Manual	1/loop	1/loop
3.	Feedwater Line Isolation		
	a. Safety injection	(See Item No. 1 of Table 7.3-1)	
	b. Steam generator high-high level	12 (3/steam generator)	2/3 in any steam generator

TABLE 7.3-2

No.	Functional Unit	No. of Channels	No. of Channels To Trip
4.	Containment Ventilation Isolation		
	a. Safety injection	(See Item No. 1 of Table 7.3-1)	
	b. Containment exhaust detectors	2	1
	c. Containment isolation		
	1) Phase A (manual)	2	1
	2) Phase B (manual)	2	2
	3) Spray actuation (manual)	2	2
5.	Control Room Air Intake Duct Isolation		
	a. Safety injection	(See Item No. 1 of Table 7.3-1)	
	b. Control room air intake radiation monitor[a,b,c]	2	1
	c. Manual	1	1

(a) Circuitry is not part of the safeguards system.

(b) Monitors on either unit control room air intake duct will initiate the isolation of both Units' control room ventilation systems.

(c) Circuitry is not redundant.

TABLE 7.3-3

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Input	Function Performed
P-4	Reactor trip	Actuates turbine trip
		Closes all MFRVs and all main feedwater bypass valves on T_{avg} below setpoint
		Prevents opening of all MFRVs, all main feedwater bypass valves, and all MFIVs which were closed by safety injection or high steam generator water level
		Allows manual block of safety injection
	Reactor not tripped	Defeats the block of the automatic reactuation of safety injection
P-11	2/3 Pressurizer pressure below setpoint	Allows manual block of safety injection actuation on low pressurizer pressure signal
		Allows manual block of safety injection and steam line isolation on low steamline pressure. Steam line isolation on high negative rate steam line pressures is permitted when this manual block is accomplished
	2/3 Pressurizer pressure above setpoint	Defeats manual block of safety injection actuation
		Defeats manual block of safety injection and steam line isolation on low steam line pressure and defeats steam line isolation on high negative rate steam line pressure

TABLE 7.3-3

Designation	Input	Function Performed
P-12[a]	2/4 T_{avg} below setpoint	Blocks steam dump condenser valves
		Allows manual bypass of steam dump block for the cooldown condenser valves only[b]
		Blocks trip open atmospheric dump
		Blocks modulation of the dump valves according to sequence described in Sheets 19 and 20 of Figure 7.2-1
	3/4 T_{avg} above setpoint	Defeats the manual bypass of steam dump block
		Enables steam dump (all condenser dump valves except the cooldown dump valves)
		Enables steam dump (atmospheric dump valves)
P-14	2/3 Steam generator water level above setpoint in any steam generator	Closes all MFRVs, all main feedwater bypass valves, and all MFIVs
		Trips all main feedwater pumps
		Actuates turbine trip

(a) Circuitry is not part of safeguards system

(b) Operations procedures allow bypassing the P-12 interlock once the reactor is in Mode 3 and borated to cold shutdown conditions.

TABLE 7.5-1

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR (CONDITIONS II AND III EVENTS)

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
1. T_{cold} &/or T_{hot} (measured, wide-range)	1 T_{hot} or 1 T_{cold} per loop	1 T_{hot} & 1 T_{cold} any 2 operating loops	0 to 700°F	±4% of full range	All channels are recorded	Ensure maintenance of proper cooldown rate and maintenance of proper relationship between system pressure and temperature for NDT considerations
2. Pressurizer Water Level	3	2	0 to 100%	±6% span at 2250 psia	All three channels indicated; one channel is selected for recording	Ensure maintenance of proper reactor coolant inventory
3. RCS Pressure (wide-range)	2	2	0 to 3000 psig	±4% of full range	One channel indicated and one recorded	Ensure maintenance of proper relationship between system pressure and temperature for NDT considerations
4. Containment Pressure (normal-range)	4	2	-5 to +55 psig	±3.5% of full span	All 4 are indicated	Monitor containment conditions to indicate need for potential engineered safety features

TABLE 7.5-1

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
5. Steam Line Pressure	3/Loop	2/Loop	0 to 1,200 psig	±4.0% of full span	All channels are indicated	Monitor steam generator pressure conditions during hot shutdown and cooldown, and for use in recovery from steam generator tube ruptures
6. Steam Generator Water Level (wide-range)	1/Steam generator	N/A	0 to 100%	±3% span[b]	All channels recorded	Ensure maintenance of reactor heat sink
7. Steam Generator Water level (narrow-range)	3/Steam generator	2/Steam generator	0 to 100%	±3% span[b]	All channels indicated; the channels used for control are recorded	Ensure maintenance of reactor heat sink
8. Intermediate Range Flux Level	2	N/A	8 decades logarithmic 10^{-11} to 10^{-3} amps overlapping the source range by 2 decades	Indicator: -16.8% to +20.2% of input; Recorder: -24% to +30% of input[c]	Both channels indicated. All channels are recorded.	

TABLE 7.5-1

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
9. Power Range						
a. Uncompensated ion chamber current (top and bottom uncompensated ion chambers)	4	N/A	0 to 120% of full power current	±1% of full span	All 8 current signals indicated	
b. Average flux of the top and bottom ion chambers	4	N/A	0 to 120% of full power	±3% of full power for indication, ±2% for recording	All 4 channels indicated. All channels are recorded.	
c. Average flux of the top and bottom ion chambers	4	N/A	0 to 200% of full power	±2% of full power to 120% ±6% of full power to 200%	All 4 channels recorded	
d. Flux difference of the top and bottom ion chambers	4	N/A	-30 to +30%	±4%	All 4 channels indicated. All channels are recorded.	

(a) Includes channel accuracy and environmental effects during normal plant operation, but does not include post-accident environmental effects.

Changes which are within the stated accuracy band or within the reading accuracy of the indicator are not reflected in this table. Actual values are found in design documents.

The instrumentation accuracies listed are typical indicator values and are not directly comparable to the channel accuracies utilized in the Chapter 15 analysis.

TABLE 7.5-1

(b) Instrument accuracy only. The accuracy statement does not include the effect of density changes in the vessel.

(c) Does not include instrument drift allowance.

TABLE 7.5-2

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR (CONDITION IV EVENTS)

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
1. Containment Pressure (normal range)	4	2	-5 to +55 psig	±3.5% of full span	All 4 are indicated	Monitor post-LOCA containment conditions
2. Containment Sump Level (NR)	2	1	88.5 to 96.6 ft El.	±6.5% of full span[e]	Indicator	Assess recirculation mode and general conditions
3. Refueling Water Storage Tank Water Level	3	2	0 to 100% of span	±4.5% of level span	All 3 are indicated and alarmed	Ensure that water is flowing to the safety injection system after a LOCA, and determine when to shift from injection to recirculation mode
4. Steam Generator Water Level (narrow-range)	3/Steam generator	2/Steam generator	0 to 100%	±3% of level span[b][c]	All channels indicated; the channels used for control are recorded	Detect steam generator tube rupture; monitor steam generator water level following a feedwater line break

TABLE 7.5-2

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
5. Steam Generator Water Level (wide range)	1/Steam generator	N/A	0 to 100%	±3% of level span[b][c]	All channels are recorded	Detect steam generator tube rupture; monitor steam generator water level following a feedwater line break
6. Steam Line Pressure	3/Steam line	2/Steam line	0 to 1,200 psig	±4% of full scale	All channels are indicated	Monitor steam line pressures following steam generator tube rupture or steam line break
7. Steam Line Flow	2/Steam line	N/A	0 to 4.5 million pounds/hour	Within ±10% span when flow >25%	All channels are indicated; the channels used for control are recorded	Indication purposes only
8. Pressurizer Water Level	3	2	0 to 100%	Indicate that level is somewhere between 0 and 100% of span	All three channels are indicated, and one channel is selected for recording	Indicate that water has returned to the pressurizer following cooldown after steam generator tube rupture or steam line break
9. Pressurizer Pressure	4	3	1250 to 2500 psig	±3.5% of full span	All channels indicated, one channel recorded	Detect steam generator tube breaks

TABLE 7.5-2

Parameter	No. of Channels Avail.	No. of Channels Req.	Range	Available Indicated Accuracy[a]	Indicator/ Recorder	Purpose
10. Intermediate Range Flux Level	2	N/A	Logarithmic 10^{-11} to 10^{-3} amps	Indicator: -16.8% to +20.2% of input; Recorder: -24% to +30% of input[d]	Both channels indicated. All channels are recorded.	Assess rod cluster control assembly ejection
11. Power Range						
a. Un-compensated ion chamber current (top and bottom un-compensated ion chambers)	4	N/A	0 to 120% of full power current	±1% of full span	All 8 current signals indicated	Assess rod cluster control assembly ejection
b. Average flux of the top and bottom ion chambers	4	N/A	0 to 120% of full power	±3% of full power for indication, ±2% for recording	All four channels indicated. All channels are recorded.	Assess rod cluster control assembly ejection

(a) Includes channel accuracy and environmental effects for normal operation. Does not include post-accident environmental effects. The instrumentation accuracies listed are typical indicator values and are not directly comparable to the channel accuracies utilized in the Chapter 15 analysis.

Changes which are within the stated accuracy band or within the reading accuracy of the indicator are not reflected in this table. Actual values are found in design documents.

(b) For the steam break, when the water level channel is exposed to a hostile environment, the accuracy required can be relaxed. The indication need only convey to the operator that water level in the steam generator is somewhere between the narrow-range steam generator water level taps.

TABLE 7.5-2

(c) Instrument accuracy only. The accuracy statement does not include the effect of density changes in the vessel, mid-deck plate delta-P, and other process measurement or environmental uncertainties.

(d) Does not include instrument drift allowance.

(e) Stated uncertainty applied to channel safety function as it is used in accordance with the EOPs. Channel uncertainty at 100% span is within ±10% span.

TABLE 7.5-3

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
Nuclear Instrumentation						
1. Source Range						
a. Count rate	2	1 to 10^6 counts/sec	±7% of the linear full scale analog voltage	Both channels indicated. All channels are recorded.	Control console	Deenergize above P-6
b. Startup rate	2	-0.5 to 5.0 decades/min	±7% of the linear full scale analog voltage	Both channels indicated	Control console	Deenergize above P-6
2. Intermediate Range						
a. Flux level	2	8 decades logarithmic 10^{-11} to 10-3 amps overlapping the source by 2 decades	Indicator: -16.8% to +20.2% of input; Recorder: -24% to +30% of input	Both channels indicated. All channels are recorded.	Control console	
b. Startup rate	2	-0.5 to 5.0 decades/min	±7% of the linear full scale analog voltage	Both channels indicated	Control console	

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
3. Power Range						
a. Uncompensated ion chamber current (top and bottom uncompensated ion chambers)	4	0 to 5 mA	±1% of full span	All 8 current signals indicated	NIS racks in control room	
c. Average flux of the top and bottom ion chambers	4	0 to 120% of full power	±3% of full power for indication, ±2% for recording	All 4 channels indicated. All channels are recorded.	Control console	
d. Average flux of the top and bottom ion chambers	4	0 to 200% of full power	±2% of full power to 120% ±6% of full power to 200%	All 4 channels recorded	Control board	
e. Flux difference of the top and bottom ion chambers	4	-30 to +30%	±4%	All 4 channels indicated. All channels are recorded.	Control console	
Reactor Coolant System						
1. $T_{average}$ (measured)	1/Loop	530 to 630°F	±4°F	All channels indicated; auctioneered high is recorded	Control console	

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
2. ΔT (measured)	1/Loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated. One channel is selected for recording	Control console	
T_{cold} or T_{hot} (measured, wide-range)	1-T_{hot} and 1-T_{cold} per loop	0 to 700°F	±4%	Both channels recorded	Control board	
3. Overpower ΔT Setpoint	1/Loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated. One channel is selected for recording	Control board & control console	
4. Overtemperature ΔT Setpoint	1/Loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated. One channel is selected for recording	Control board & control console	
5. Pressurizer Pressure	4	1250 to 2500 psig	±3.5% of span	All channels indicated, controlling channel recorded	Control board & control console	
6. Pressurizer Level	3	0 to 100%	±6.1% span at 2250 psia[b]	All channels indicated. One channel is selected for recording	Control board & control console	Two-pen recorder used, second pen records reference level signal

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
7. Primary Coolant Flow	3/Loop	0 to 120% of rated flow	Repeatability of ±4% of full flow	All channels indicated	Control board	
8. Reactor Coolant Pump Motor Amperes	1/Loop	0 to 400 amp	±2%	All channels indicated	Control board	One channel for each motor
9. RCS Pressure Wide-range	2	0 to 3000 psig	±4%	One channel indicated and one recorded	Control board	
10. Pressurizer Safety Relief Valve Position	3	Open/closed	NA	All channels indicated	Vertical board	
Reactor Control System						
1. Demanded Rod Speed	1	8 to 72 steps/min	±2 steps/min	The one channel is indicated	Control console	
2. Auctioneered $T_{average}$	1	530 to 630°F	±4°F	The one channel is recorded	Control console	The highest of the four T_{avg} channels into the auctioneer will be passed to the recorder
3. $T_{reference}$	1	530 to 630°F	±4°F	The one channel is recorded	Control console	
4. Control Rod Position						If system not available, borate and sample accordingly

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
a. Number of steps of demanded rod withdrawal	1/group	0 to 231 steps	±1 step	Each group is indicated.	Control console	These signals are used in conjunction with the measured position signals (4b) to detect deviation of any individual rod from the demanded position. A deviation will actuate an annunciator. An alarm annunciator is actuated when the last rod control bank to be withdrawn reaches the withdrawal limit, when any rod control bank reaches the low insertion limit, and when any rod control bank reaches the low-low insertion limit
b. Full-length rod measured position	1 for each rod	0 to 228 steps	±3 steps at full accuracy, ±6 steps at 1/2 accuracy	Each rod position is indicated	Control board	
Containment System						
1. Containment Pressure (normal range)	4	-5 to +55 psig	±3.5% of full span	All 4 channels indicated	Control board	

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
2. Containment Pressure (narrow range)	1	-1 to +1.5 psig	±0.1 psi	Recorded	Control board	
Feedwater and Steam Systems						
1. Auxiliary Feedwater Flow	1/Steam generator	0 to 300 gpm	±10% of full span	All channels indicated	Control board	One channel to measure the flow to each steam generator
2. Steam Generator Level (narrow-range)	3/Steam generator	0 to 100%	±3% of ΔP span (hot) [b]	All channels indicated. The channels used for control are trended indications.	Control board & control console	
3. Steam Generator Level (wide-range)	1/Steam generator full load level	0 to 100%	±3% of ΔP span (hot) [b]	All channels recorded	Control board	
4. Programmed Steam Generator Signal	1 for 4 Steam generators	0 to 100%	±4%	One channel indicated	Control board	
5. Main Feedwater Flow	2/Steam generator	0 to 4.5 million pounds per hour	Within ±10% span when flow >25%	All channels indicated. The channels used for control are trended indications.	Control board	

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
6. Magnitude of Signal Controlling Main and Bypass Feedwater Control Valve	1/main 1/bypass	0 to 100% of valve opening	±2%	All channels indicated	Control board & control console	One channel for each main and bypass valve. OPEN/SHUT indication is provided in the control room for each main and bypass feedwater control valve
7. Steam Flow	2/Steam generator	Unit 1: 0 to 4.5 million pounds per hour Unit 2: 0 to 4.5 million pounds per hour	±10% span when flow >20%	All channels indicated. The channels used for control are trended indications.	Control board	Accuracy is equipment capability; however, absolute accuracy depends on calibration against feedwater flow
8. Steam Line Pressure	3/Loop	0 to 1,200 psig	±4.0% of full span	All channels indicated	Control board	
9. Steam Dump Demand Signal	1	0 to 100% equivalent to 0 to 85% max calculated steam flow	±2% span[c]	The one channel is indicated	Control board	OPEN/SHUT indication is provided in the control room for each steam dump valve

TABLE 7.5-3

Parameter	No. of Channels Available	Indicated Range	Indicator/ Accuracy[a]	Indicator/Recorder	Location	Notes
10. Turbine Impulse Chamber Pressure	2	0 to 110% of max calculated turbine load	±3.5% of full span	Both channels indicated	Control board	OPEN/SHUT indication is provided in the control room for each turbine stop valve
11. Condensate Storage Tank Level	1	0 to 100%	±3.5% of full span	Indicator and Recorded	Control board	
Charging and Volume Control						
1. Boric Acid Tank Level	1/Tank	0 to 100%	±3.5% of full span	Indicator	Control board	
2. Emergency Borate Flow	1	0 to 50 gpm	±4% of full span	Indicator	Control board	
3. Charging Pump Flow	1	0 to 200 gpm	±10% span when flow >60 gpm	Indicator	Control console	

(a) Includes channel accuracy and environmental effects.
Changes which are within the stated accuracy band or within the reading accuracy of the indicator are not reflected in this table. Actual values are found in design documents.

(b) Instrument accuracy only. The accuracy statement does not include the effect of density changes in the vessel.

(c) Indicator calibration tolerance.

TABLE 7.5-4

POSTACCIDENT MONITORING PANEL INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR

Parameter	No. of Channels	Indicated Range	Available Indicated Accuracy[j]	Indicator/ Recorder	Comments
1. Reactor vessel level (bottom of vessel to top)	2	0 to 120% (vessel span)	±10% of calibrated span [h]	Recorder/indicator	
2. Reactor plenum level (hot leg pipe to top of vessel)	2	60 to 120% (vessel span)	25.4% of calibrated span total error band [i]	Recorder	
3. Containment pressure (wide-range)	2	-5 to 200 psig	±4% of full span	Recorder	
4. Containment water level (wide-range)	2	64 ft to 98 ft	-8 to +5.5 ft[e]	Recorder	
5. Containment radiation (high-range)	2	1 to 10^7 R/hr	-50% to +60% reading[d]	Recorder/indicator	
6. Plant vent noble gas – normal and extended range	1	10^{-6} to 10^5 µCi/cc	±15% reading based on min. expected sample pressure[f]	Recorder[c]/indicator	
7. Containment hydrogen	2	0 to 10%	±10% of full span	Recorder	
8. Degree of subcooling	2	-40 to +200°F	< 20°F when RCS pressure >900 psig[e] and temperature ≤ 700°F	Recorder (Train A)/ Indicator (Train B)	
9. Plant vent monitor (ALARA)	1	0.1 to 10^7 mR/hr	-40% to +55% reading	Recorder	
10. Gas decay tank pressure	1 per tank	0 to 200 psig	±3.5% of full span[b]	Indicator	

TABLE 7.5-4

Parameter	No. of Channels	Indicated Range	Available Indicated Accuracy[j]	Indicator/ Recorder	Comments
11. Incore temperature	65	0 to 2300°F	±5% of full span[g]	Recorder/indicator	
12. Liquid hold-up tank level	1 per tank	0 to 100%	±5% of full span	Indicator	
13. Containment spray pump discharge flow	1 per pump	0 to 3000 gpm	±5% of full span from 550 to 3000 gpm	Indicator	

(a) Deleted.

(b) Does not include sensor accuracy.

(c) Indicator on RMS panels - Recorder available on EARS until the Central Radiation Processor is available.

(d) Includes detector efficiency.

(e) Accident scenario: HELB inside containment.

(f) Indication accuracy is computed based on the expected detector efficiency. In calculating the offsite dose, however, the actual detector efficiency is taken into account for expected distribution of radioisotopes based on the accident condition.

(g) The stated accuracy is met in the instrument range needed for operator action.

(h) Levels ≤69.3% vessel span (top of hot leg) and coolant temperature ≤650°F.

(i) Top of vessel and coolant temperature 600°F.

(j) Changes which are within the stated accuracy band or within the reading accuracy of the indicator are not reflected in this table. Actual values are found in design documents.

TABLE 7.5-5

INFORMATION REQUIRED ON THE SUBCOOLEDMARGIN MONITORS (SCMMs)

Display	
Information displayed	TSAT - T, P - PSAT
Display type	Digital and analog
Continuous or on demand	Continuous
Single or redundant display	Redundant
Location of displays	Control board, (indicator from SCMM B) PAM 1 (recorder from SCMM A) PAM 3 and 4 (indicator and trend)
Alarms	30°F, 20°F Subcooling from SCMM A or B
Overall uncertainty	<+20°F when RCS pressure >900 psig, temperature ≤ 700°F
Range of display	-40 to +200°F
Qualifications	Seismic
Calculator (Processors)	
Type	Digital (shared with RVLIS)
If process computer is used, specify availability	N/A
Single or redundant calculators	Redundant
Selection logic	High T
Qualifications	Seismic
Calculational technique	Steam tables 0.1 to 3000 psi 150 to 750°F

	TABLE 7.5-5	Sheet 2 of 2

Input

Temperature	4 RTDs, hottest T/C
Temperature	Hottest core exit T/C (per train) and 2 Reactor Hot Leg (per train)
Range of temperature sensors	0 to 700°F (RTDs) (useful 150°F to 700°F) 100 to 2300°F (T/Cs) (useful 150°F to 750°F)
Uncertainty[(a)] of temperature signal	< +12°F (up to 700°F), < +23°F (up to 1200°F)
Qualifications	Seismic, environmental
Pressure	Barton Model 763 or Rosemount Model 1153
Pressure	1 on loop 3 hot leg (train A input) 1 on loop 4 hot leg (train B input)
Range of pressure sensors	0 to 3000 psi
Uncertainty[(a)] of pressure signal	≤±35 psi
Qualifications	Seismic, environmental

(a) Uncertainties must address conditions of forced flow and natural circulation

TABLE 7.5-6

SUMMARY OF COMPLIANCE WITH REGULATORY GUIDE 1.97 REV. 3

TYPE A VARIABLES

RCS cold leg water temperature (see Item 4)

RCS hot leg water temperature (see Item 5)

RCS pressure (see Item 7)

Core exit temperature (see Item 8)

Containment sump water level - wide range (see Item 12)

Containment sump water level - narrow range (see Item 13)

Containment pressure - normal range (see Item 14)

Refueling water storage tank level (see Item 38)

Pressurizer level (see Item 41)

Steam generator level - narrow range (see Item 46)

Steam generator level - wide range (see Item 46)

Steam generator pressure (see Item 47)

Auxiliary feedwater flow (see Item 50)

Condensate storage tank level (see Item 51)

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
TYPE B VARIABLES												
Reactivity Control												
1. Neutron flux	NRC	1	10^{-6}-100% Full power	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	10^{-8}-100% Full power	Yes	Yes	Yes	Yes	1E	Continuous indication& recording	No	No	Note 27 Note 57
2. Control rod position	NRC	3	Full in or not full in	No	No	Yes	No	--	Continuous indication			
	DCPP	3	Full range indication	No	No	Yes	No	Non-1E	Continuous indication	Yes	Yes	
3. RCS soluble boron concentration												Note 1
4. RCS cold leg water temp.	NRC	1	50-700°F	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	50-700°F	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	Note 47 Note 48 Note 58
Core Cooling												
5. RCS hot leg water temp	NRC	1	50-700°F	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	0-700°F	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	Note 47 Note 48 Note 58
6. RCS cold leg water temp (see Item 4)												
7. RCS pressure	NRC	1	0-3000 psig	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	0-3000 psig	Yes	Yes	Yes	Yes	1E	Continuous indication & recording	Yes	Yes	Note 27 Note 48
8. Core exit temperature	NRC	1	200-2300°F	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	0-2300°F	Yes	Yes	Yes	Yes	1E	Continuous indication & recording	Yes	Yes	Note 48

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category	Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
9. Coolant level in reactor	NRC 1	Bottom of hot leg to top of vessel	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP 1	Bottom to top of vessel	Yes	Yes	Yes	Yes	1E	Continuous indication & recording	Yes	Yes	
10. Degrees of subcooling	NRC 2	200°F subcooling to 35°F superheat	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	200°F subcooling to 40°F superheat	Yes	Yes	Yes	Yes	1E	Continuous indication & recording	Yes	Yes	Note 46
Maintaining Reactor Coolant System Integrity											
11. RCS pressure (see Item 7)											
12. Containment sump water level (WR)	NRC 1	Plant specific	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP 1	64 ft (CNT bottom) to 98 ft	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	Note 48
13. Containment sump water level (NR)		Sump depth	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 1	88.5-96.6 ft	Yes	Yes	Yes	Yes	1E	Continuous indication	No	No	Note 48
14. Containment pressure	NRC 1	-5 psig to 3 times design pressure	Yes	Yes	Yes	Yes	1E	Continuous recording			
Normal range	DCPP 1	-5 to +55 psig	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 48
Wide range	DCPP 1	-5 to 200 psig	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	N0te 39
Maintaining Containment Integrity											
15. Containment isolation valve position	NRC 1	Closed-not closed	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP 1	Closed-not closed	Yes	Yes	Yes	Yes	1E	Indication	Yes	Yes	Note 28 Note 36 Note 49 Note 59
16. Containment pressure (see Item 14)											

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
TYPE C VARIABLES												
Fuel Cladding												
17. Core exit temperature (see Item 8)												
18. Radioactivity concentration in circulating primary coolant (see Note 18)												
19. Analysis of primary coolant - gamma spectrum (seeNote 55)												
Reactor Coolant Pressure Boundary												
20. RCS pressure (see Item 7)												
21. Containment pressure (see Item 14)												
22. Containment sump water level (see Items 12 and 13)												
23. Containment area radiation (see Item 65)												
24. Effl. radio-activity-noble gas effl. from condenser air removal sys. exhaust	NRC	3	10^{-6} to 10^{-2} μCi/cc	No	No	Yes	No	-	Recording			
	DCPP	3	10^{-4} to 3 μCi/cc	No	No	Yes	No	non-1E	Continuous indication, recording	Yes	Yes	Note 3 Note 34
Containment												
25. RCS pressure (see Item 7)												
26. Containment hydrogen concentration	NRC	3	0-10%	No	No	Yes	No	Highly Reliable	Continuous recording			
	DCPP	3	0-10%	No	No	Yes	Yes	Highly Reliable	Continuous recording	Yes	Yes	
27. Containment pressure (see Item 14)												
28. Containment effluent radioactivity - noble gases from identified release points (see Item 67)												
29. Effluent radioactivity - noble gases from buildings or areas where penetrations and hatches are located (see Item 67)												

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
TYPE D VARIABLES												
Residual Heat Removal System												
30. RHR system flow	NRC	2	0-110% design flow	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-1500 gpm (Lo) 0-5000 gpm (Hi) 0-7000gpm (HL)	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 50
31. RHR heat exchanger outlet temp.	NRC	2	40-350°F	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	50-400°F	Yes	No	Yes	No	1E	Continuous recording	Yes	Yes	Note 6
32. Accumulator tank level	NRC	2	10%-90% volume	No	No	Yes	No	Highly reliable	Continuous indication			Note 51
	DCPP	3	10%-90% volume	No	No	Yes	No	Highly reliable, non-1E	Continuous indication	No	No	
33. Accumulator tank pressure	NRC	2	0-750 psig	No	No	Yes	No	Highly reliable	Continuous indication			Note 51
	DCPP	3	0-700 psig	No	No	Yes	Yes	Highly reliable, non-1E	Continuous indication	Yes	Yes	Note 7
34. Accumulator isolation valve position	NRC	2	Closed or open	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	3	Closed or open	No	No	Yes	No	1E	Continuous indication	No	No	Note 32
35. Boric acid charging flow (charging inj header flow)	NRC	2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-1000 gpm	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
36. Flow in HPI system (SI pump disch.)	NRC	2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-750 gpm	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
37. Flow in LPI system - RHR system (see Item 30)												

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
38. Refueling water storage tank level	NRC	2	Top to bottom	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	1	0-100%	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 8 Note 28 Note 41 Note 48
Primary Coolant System												
39. Reactor coolant pump status	NRC	3	Motor current	No	No	Yes	No	--	Continuous indication			
	DCPP	3	Motor current 0-400 amp	No	No	Yes	No	non-1E	Continuous indication	Yes	Yes	Note 21
40. Primary system safety relief valve position	NRC	2	Closed-not closed	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	Closed-not closed	Yes	Yes	Yes	No	1E	Continuous indication	Yes	Yes	Note 9 Note 46
41. Pressurizer level	NRC	1	Bottom to top	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	0-100%	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 8 Note 28 Note 33 Note 48
42. Pressurizer heater status	NRC	2	Electric current	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	Electric power 0-600 kW	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 45
43. Quench tank (PRT) level	NRC	3	Top to bottom	No	No	Yes	No	--	Continuous indication			
	DCPP	3	0-100%	No	No	Yes	No	Highly reliable, non-1E	Continuous indication	Yes	Yes	Note 8
44. Quench tank (PRT) temperature	NRC	3	50-750°F	No	No	Yes	No	--	Continuous indication			
	DCPP	3	50-350°F	No	No	Yes	No	Highly reliable, non-1E	Continuous indication	Yes	Yes	Note 10

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
45. Quench tank (PRT) pressure	NRC	3	0 design	No	No	Yes	No	--	Continuous indication			
	DCPP	3	0-100 psig	No	No	Yes	No	Highly reliable, non-1E	Continuous indication	Yes	Yes	
Secondary System (Steam Generator)												
46. Steam generator level	NRC	1	From tube sheet to separators	Yes	Yes	Yes	Yes	1E	Continuous recording			
Narrow range	DCPP	1	From within the transition cone to separators.	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 26 Note 28 Note 48
Wide range	DCPP	1	From 12 inches above tube sheet to separators	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	Note 26 Note 36 Note 47 Note 48
47. Steam generator pressure	NRC	2	From atm. press. to 20% above the lowest safety valve setting	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	1	0-1200 psig	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 11 Note 28 Note 41 Note 48
48. Main steam flow	NRC	2	--	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-4.5 x 10^6 lb/hr	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
49. Main feedwater flow	NRC	3	0-110% design	No	No	Yes	No	--	Continuous indication			
	DCPP	3	0-4.5 x 10^6 lb/hr	No	No	Yes	No	1E	Continuous indication	Yes	Yes	
Auxiliary Feedwater or Emergency Feedwater System												
50. Auxiliary or emergency feedwater flow	NRC	2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	1	0-300 gpm	Yes	Yes	Yes	Yes	1E	Continuous indication	Yes	Yes	Note 26 Note 28 Note 47 Note 48 Note 52

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category	Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
51. Condensate storage tank	NRC 1	Plant specific	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP 1	0-100%	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	Note 37 Note 48
Containment Cooling Systems											
52. Containment spray flow	NRC 2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-3000 gpm	Yes	No	Yes	No	1E	Continuous indication	No	No	
53. Heat removal by containment fan heat removal system	NRC 2	Plant specific	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	See Note 12	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 12
54. Containment atmosphere temperature	NRC 2	40-400°F	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-400°F	Yes	No	Yes	Yes	1E	Continuous indication	No	No	
55. Containment sump water temperature	NRC 2	50-250°F	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-300°F	Yes	No	Yes	Yes	1E	Continuous indication	No	No	
Chemical and Volume Control System											
56. Makeup flow-in	NRC 2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-50 gpm 0-200 gpm	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 53
57. Letdown flow-out	NRC 2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-200 gpm	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
58. Volume control tank level	NRC 2	Top to bottom	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP 2	0-100%	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 8

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
Cooling Water System												
59. CCW temp. to ESF system	NRC	2	40-200°F	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-200°F	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
60. CCW flow to EFS system	NRC	2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	0-12,000 gpm	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	
Radwaste Systems												
61. High level radioactive liquid tank level	NRC	3	Top to bottom	No	No	Yes	No	--	Continuous indication			
	DCPP	3	0-100%	No	No	Yes	No	1E	Continuous indication	No	No	Yes Yes
62. Radioactive gas holdup tank pressure	NRC	3	0-150% design	No	No	Yes	No	--	Continuous indication			
	DCPP	3	0-200 psig	No	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 54
Ventilation Systems												
63. Emergency ventilation damper position	NRC	2	Open-closed	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	Open-closed	Yes	No	Yes	No	1E	Continuous indication	No	No	Note 24
Power Supplies												
64. Status of standby power and other emergency sources	NRC	2	Voltages, currents	Yes	No	Yes	No	Highly reliable	Continuous indication			
	DCPP	2	Voltages, currents	Yes	No	Yes	No	1E	Continuous indication	Yes	Yes	Note 13 Note 43
TYPE E VARIABLES												
Containment Radiation												
65. Containment area radiation - high range	NRC	1	1 to 10^7 R/hr	Yes	Yes	Yes	Yes	1E	Continuous recording			
	DCPP	1	1 to 10^7 R/hr	Yes	Yes	Yes	Yes	1E	Continuous recording	Yes	Yes	

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category		Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
Area Radiation												
66. Radiation exposure rate (inside bldgs or areas)	NRC	3	10^{-1} to 10^{4} mR/hr	No	No	Yes	No	--	Recording			
	DCPP	3	10^{-1} to 10^{4} mR/hr	No	No	Yes	No	Non-1E	Local indication and alarm	No	No	Note 5 Note 34
Airborne Radioactive Materials Released From Plant												
67. Noble gases and vent flow rate: Containment or purge effluent (see Note 14) Reactor shield building annulus (see Note 14) Auxiliary building (see Note 14) Condenser air removal system exhaust (see Item 24)												
Noble gases from common-plant vent + discharging any of above releases (including cont. purge)	NRC	2	10^{-6} to 10^{4} μCi/cc	Yes	No	Yes	No	Highly reliable	Continuous recording			
	DCPP	2	10^{-6} to 10^{4} μCi/cc	Yes	No	Yes	No	Highly reliable	Continuous indication, recording	Yes	Yes	Note 34
Plant vent flow	NRC	2	0-110% design	Yes	No	Yes	No	Highly reliable	Continuous recording			
	DCPP	2	0-30x10^{4} cfm	Yes	No	Yes	No	Highly reliable	Continuous recording			
Vent from steam generator safety relief valves or atmospheric dump valves	NRC	2	10^{-1} to 10^{3} μCi/cc	Yes	No	Yes	No	Highly reliable	Continuous recording			
	DCPP	2	10^{-1} to 10^{3} μCi/cc	Yes	No	Yes	No	1E	Continuous recording			
All other identified release points (see Note 56)												
68. Particulates and halogens	NRC	3	10^{-3} to 10^{2} μCi/cc	No	No	Yes	No	--	Recording			
	DCPP	2	Note 15	Yes	No	Yes	No	Highly reliable	Continuous indication, recording	Yes	Yes	Note 15 Note 34

TABLE 7.5-6

Reg Guide 1.97 Variable	RG 1.97 Category	Instrument Range[a]	Envr. Qual[b]	Seismic Qual[c]	QA[d]	Redundant	Power Supply	Control Room	Display at TSC[e]	Display at EOF	Comments
Environs Radiation and Radioactivity											
69. Airborne radiohalogens & particulates (portable with on-site analysis)	NRC 3	10^{-9} to 10^{-3} μCi/cc	No	No	Yes	No	--	--			
	DCPP 3	10^{-9} to 10^{-3} μCi/cc	No	No	Yes	No	--	--	--	--	
70. Plant and environs radiation (portable instrumentation)	NRC -	As specified in RG 1.97, Rev. 3	No	No	Yes	No	--	--			
	DCPP -	As specified in RG 1.97, Rev. 3	No	No	Yes	No	--	--	--	--	
71. Plant and environs radioactivity (portable instrumentation)	NRC 3	Isotopic analysis	No	No	Yes	No	--	--			
	DCPP 3	Multichannel gamma-ray spectrometer	No	No	Yes	No	--	--	--	--	Note 16
Meteorology											
72.	NRC	As specified in RG 1.97, Rev. 3	No	No		No	--	Recording			
	DCPP	As specified in RG 1.97, Rev. 3	No	No		No	non-1E	Indication, recording	Yes	Yes	Note 38 Note 40
Accident Sampling Capability											
73.											Note 55

(a) Instrument Range - Where the NRC and Diablo Canyon instrument ranges are not directly comparable, the Diablo Canyon ranges meet or exceed the NRC ranges, unless otherwise noted

(b) EQ (Environmental Qualification) - A "Yes" entry means that the instrumentation complies with 10 CFR 50.49. A "No" entry means there is no specific provision for environmental qualification of this instrumentation

(c) Seismic Qualification - A "Yes" entry means that the instrumentation complies with Regulatory Guide (RG) 1.100. A "No" entry means there are no specific provisions for seismic qualification of this instrument.

(d) QA (Quality Assurance) - A "Yes" entry means that the instrumentation complies with the applicable quality assurance provisions contained in RG 1.97 for the category of the instrument.

(e) This column represents the TSC and the Alternate TSC/OSC.

1. Elimination of the boron concentration monitoring system (BCMS) and utilization of the post-accident monitoring system (PASS) was approved by NRC letter dated December 4, 2000. Elimination of the PASS was approved by License Amendments 149 (Unit 1) and 149 (Unit 2), dated July 13, 2001

2. Deleted in Revision 4.

3. Installed range is adequate since air ejector exhaust is routed to the plant vent.

4. Deleted in Revision 11.

5. The Reg Guide 1.97 instrument range is erroneously stated as 10-1 to 104 R/hr for this variable.

6. Installed range is adequate for the Diablo Canyon site as the RHR outlet temperature is not expected to be less than 50°F.

7. Installed range is adequate. Tank pressure limited to 700 psig by relief valve.

8. Zero to 100% indicates usable volume of tank.

9. Position indication for safety valves is provided by acoustic monitors and by position switches for the power operated relief valves.

10. Quench tank pressure is limited to 100 psig by a rupture disk, so water temperature cannot exceed the saturation temperature at 100 psig, or 338°F. Therefore, the range of 50-350°F is adequate.

11. Installed ranged is adequate. Redundant instrumentation is installed and all safety valves lift before 1200 psig. The relieving capability of the safety valves is greater than rated steam flow. Hence, pressure cannot physically reach 1200 psig.

12. Containment fan cooler unit (CFCU) operation is verified by white monitor lights (that confirm proper CFCU response to ESF actuation), CFCU ammeters, and CFCU motor speed indicating lights. Category 1 containment pressure (Variable 14) and Category 2 containment temperature (Variable 54) provide an overall indication of CFCU system performance. CFCU operation is an indirect measurement of these containment parameters that are of primary importance to plant operators.

13. Category 2 indications for vital 4 KV voltage, EDG wattage and amperage, 4 KV/480 V transformer primary side amperage, 480 V voltage, and battery voltage and amperage are provided. All indications are Class 1E except for battery voltage and amperage.

14. Not needed if effluent discharges through common plant vent.

15. The particulate monitor has a range of 10^{-12} to 10^{-7} μCi.cc. Additional range is achieved through use of particulate filters installed on postaccident grab sampling equipment. The iodine monitor has a range of 10^{-7} to 10^{-2} μCi/cc. Additional range is provided by postaccident grab sampling equipment up to 102 μCi/cc.

16. An offsite laboratory with gamma spectroscopy equipment is available for environmental analysis.

17. Deleted in Revision 4.

18. Category 1 instrumentation to monitor radiation level in circulating primary coolant is not provided. Routine reactor coolant sampling verifies fuel cladding integrity during normal operation. During an accident, rapid assessment of cladding failures can be obtained from the Category 1 containment high range area radiation monitors in conjunction with a DCPP emergency procedure titled, “Core Damage Assessment Procedure”.

19. Deleted in Revision 4.

20. Deleted in Revision 7.

21. Display at TSC, Alternate TSC/OSC, and EOF is circuit breaker status.

22. Deleted in Revision 4.

23. Deleted in Revision 4.

24. Most of the critical damper positions are indicated at the TSC, Alternate TSC/OSC, and EOF, enough to assure that the system is working as expected.

25. Deleted in Revision 11.

26. The narrow range steam generator level is the key variable for monitoring secondary heat sink if the water level is within the narrow range span. If the water level is below the narrow range span, auxiliary feedwater flow in conjunction with steam generator wide range level meet the Category 1 requirements for monitoring steam generator status.

27. Category 1 recording is provided for one channel.

28. This post-accident monitoring data is recorded/stored in the Transient Recording System (TRS). The TRS provides the data storage and recall functions associated with ERFDS. The TRS is a Class II, highly reliable computer system with uninterruptible battery backed power.

29. Deleted in Revision 11.

30. Deleted in Revision 7.

31. Deleted in Revision 7.

32. Accumulator isolation valve position indication is Category 3. Power is removed from the valve actuator during normal operation; hence, following an accident the valve is known to be in its correct (open) position. Power to these valves may be manually restored following a LOCA, but operation of the valves, and thus the position indication, is not critical for post-LOCA accident mitigation or plant shutdown. Power is also restored to these valves during certain (non-LOCA) emergency conditions when operation of the valves is required. However, the position switches will not be exposed to a harsh environment under these conditions, so the position switches will remain operable.

33. Pressurizer water level indication meets Category 1 requirements; the recorder for this variable is Instrument Class II and is common for all the channels. This combination of Category 1 indication and Class II recording is sufficient to meet the Regulatory Guide requirements.

34. Recording as necessary on EARS, ERFDS and/or TRS.

35. Deleted.

36. Redundant channels are powered from different Class 1E power supplies; however, electrical cabling does not meet separation criteria.

37. Zero to 100% indicates contained volume of tank.

38. The plant process computer is used as the indicating device to display meteorological instrument signals. In addition, a Type E, Category 3 multi-point recorder is located at each meteorological tower building.

39. Normal range containment pressure channels provide indication from -5 to +55 psig. Wide range channels provide recording from -5 to 200 psig, but only the positive pressure range is credited as Category 1. Recording negative pressures is not required as negative pressures would not be the range of interest during an accident when containment pressures can be expected to increase.

40. Control room indication is processed for display upon demand.

41. Recording of this Category 2 variable which PG&E classifies as Category 1 is not provided because variable trending does not provide essential information.

42. DCPP instrument ranges are in terms of CPM or mR/hr., with conversion factors and graphs that allow easy conversion.

43. 480V and 4160V bus voltages are indicated on an indicator scale of 0 to 150; actual voltage is determined by applying a scaling factor (4 for the 480V bus, and 35 for the 4160V bus).

44. The recording capability associated with this variable is provided by a Category 3 multi-channel recorder.

45. Pressurizer heater power consumption is indicated, for groups 2 and 3 only, at CC-1 and (via ERFDS) the TSC and EOF. Although not credited for RG 1.97, circuit breaker status is also available at the TSC and EOF for groups 1 and 4.

46. Seismic qualification in accordance with NUREG-0737 requirements.

47. Redundancy is provided on a system basis as opposed to a per loop basis. Loop 1 and 2 channels are redundant to loop 3 and 4 channels.

48. Instrument channels are designated as Type A variables as they provide information required for operator action.

49. CIV position indication redundancy is provided on a per penetration basis as opposed to a per valve basis.

50. Each RHR train is monitored by 0-1500 gpm and 0-5000 gpm flow indicators in all modes of RHR operation except hot leg recirculation. The 0-7000 gpm flow indication monitors RHR system flow in the hot leg recirculation mode of operation.

51. In accordance with NRC guidance subsequent to issuance of Reg Guide 1.97, environmental qualification is not required for the accumulator tank pressure and level channels.

52. If flow exceeds instrument range, steam generator level instruments provide the necessary information to monitor steam generator status.

53. Emergency borate flowpath to charging pump suction monitored by 0-50 gpm flow indication. Charging pump discharge flow monitored by 0-200 gpm flow indication.

54. Gas decay tank pressure indication spans 0-200 psig. Control system maintains normal tank pressure in the range of 0-100 psig and relief valves limit tank pressure to 150 psig.

55. Post-accident sampling system requirements were deleted by License Amendments (LAs) 149 (Unit 1) and 149 (Unit 2), dated July 13, 2001. Three commitments were established to meet the conditions of LAs 149/149 to (1) maintain contingency plans for obtaining and analyzing highly radioactive samples of reactor coolant, containment sump, and containment atmosphere (T36279), (2) maintain a capability for classifying fuel damage events at the Alert level threshold (T36280), and (3) maintain the capability to monitor radioactive iodines that have been released to offsite environs (T36281).

56. The steam generator blowdown tank vent is a potential noble gas release point that is not discharged through the plant vent. However, the blowdown tank is only used intermittently and is automatically isolated on high radiation in the liquid blowdown effluent. This is not a credible noble gas release path. Grab sample capability is provided for the blowdown tank vent effluent.

57. Source, intermediate and power range nuclear instrumentation provide displays at TSC and EOF.

58. RCS loop 1 hot leg and cold leg temperature channels are not environmentally qualified for outside-containment line break accidents.

59. Containment isolation valves credited for RG 1.97 Category 1 position indication are defined as only those containment isolation valves that receive a Phase A, Phase B or containment ventilation isolation signal.

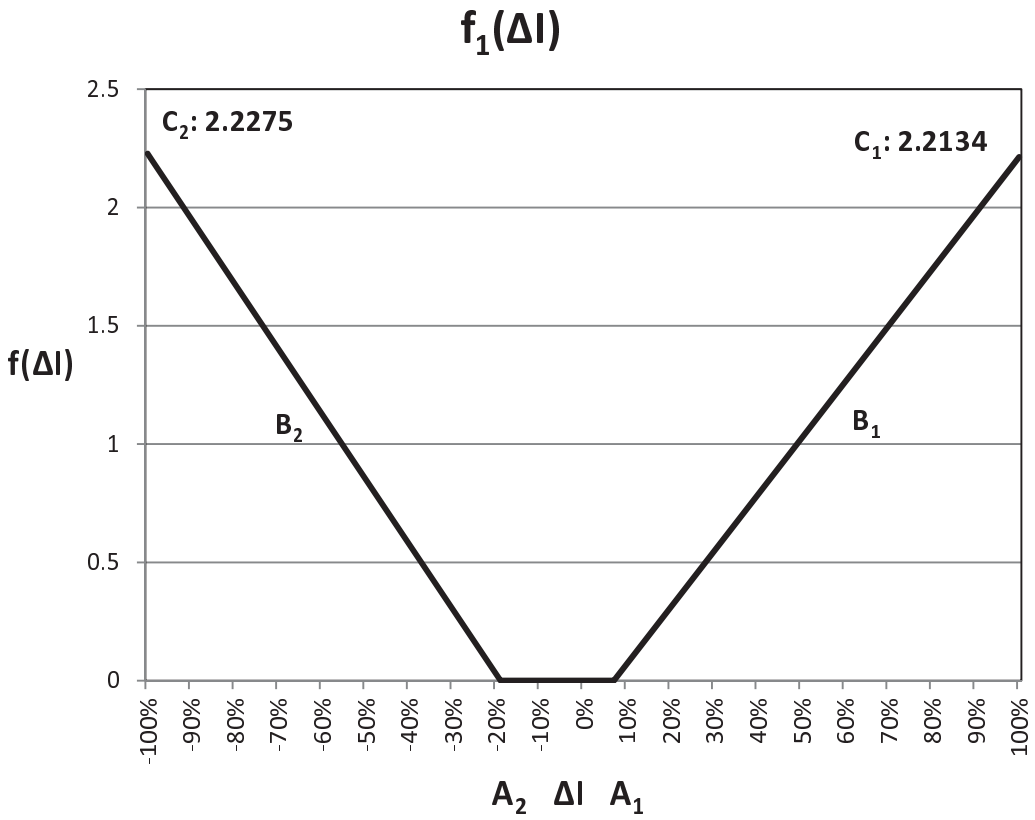
TABLE 7.7-1

PLANT CONTROL SYSTEM INTERLOCKS

Designation	Derivation	Function
C-1	1/2 Neutron flux (intermediate range) above setpoint	Blocks automatic and manual control rod withdrawal
C-2	1/4 Nuclear power (power range) above setpoint	Blocks automatic and manual control rod withdrawal
C-3	2/4 Overtemperature ΔT above setpoint	Blocks automatic and manual control rod withdrawal Actuates turbine runback via load reference Defeats remote load dispatching
C-4	2/4 Overpower ΔT above setpoint	Blocks automatic and manual control rod withdrawal Actuates turbine runback via load reference Defeats remote load dispatching
C-5	1/1 Turbine impulse chamber pressure below setpoint	Defeats remote load dispatching Blocks automatic control rod withdrawal
C-7A	1/1 Time derivative (absolute value) of turbine impulse chamber pressure (decreases only) above setpoint	Makes 40 percent condenser dump valves available for either tripping or modulation

TABLE 7.7-1

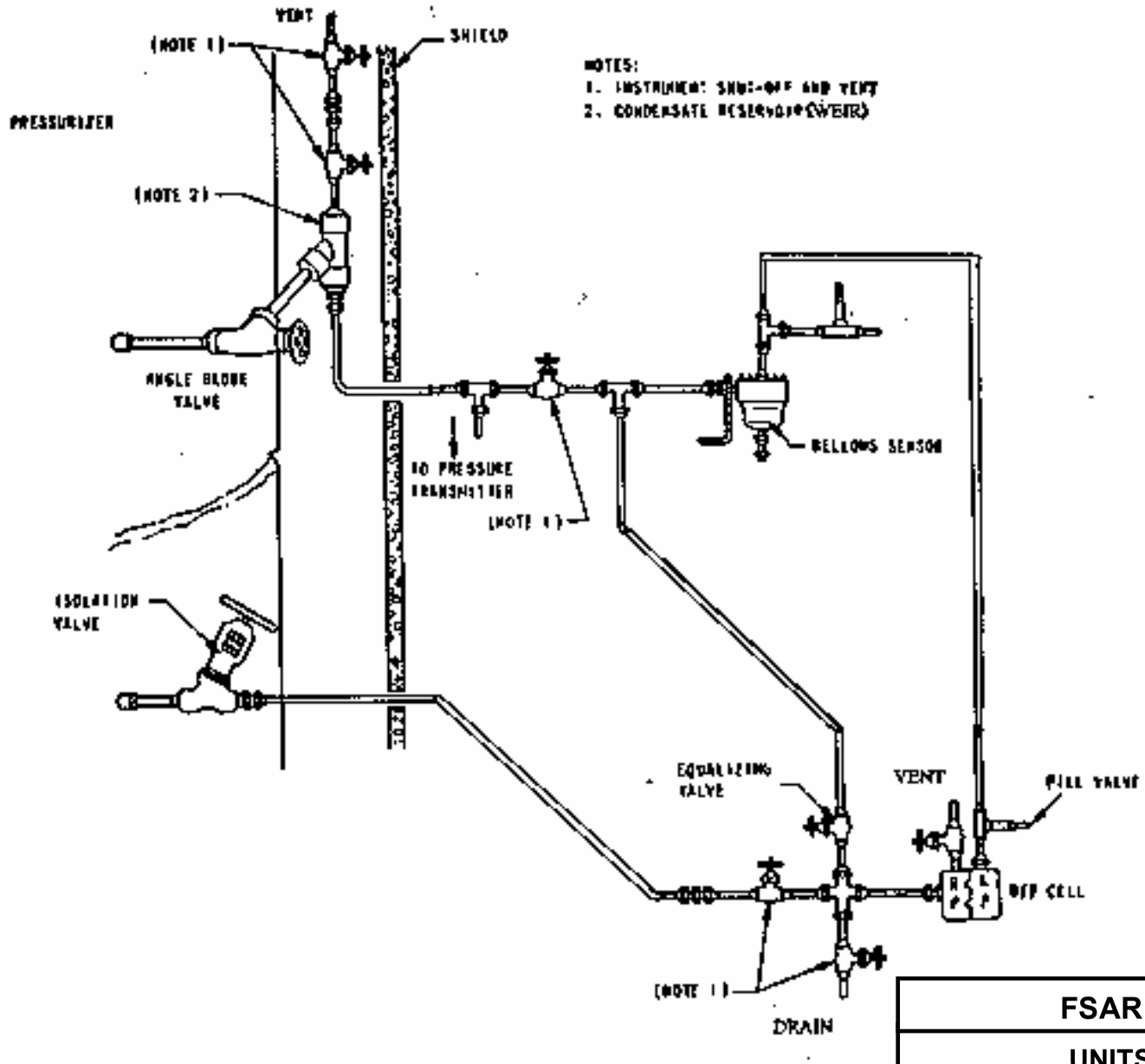
Designation	Derivation	Function
C-7B	1/1 Time derivative (absolute value) of turbine impulse chamber pressure (decreases only) above setpoint	Makes 10 percent atmospheric dump valves available for either tripping or modulation
P-4	Reactor trip	Blocks steam dump control via load rejection T_{avg} controller Makes 40 percent condenser dump valves available for either tripping or modulation Blocks 10 percent atmospheric dump valves Unblocks steam dump control via reactor trip T_{avg} controller
C-9	Any condenser pressure above setpoint or All circulating water pump breakers open	Blocks steam dump to condenser
C-11	1/1 Bank D control rod position above setpoint	Blocks automatic rod withdrawal



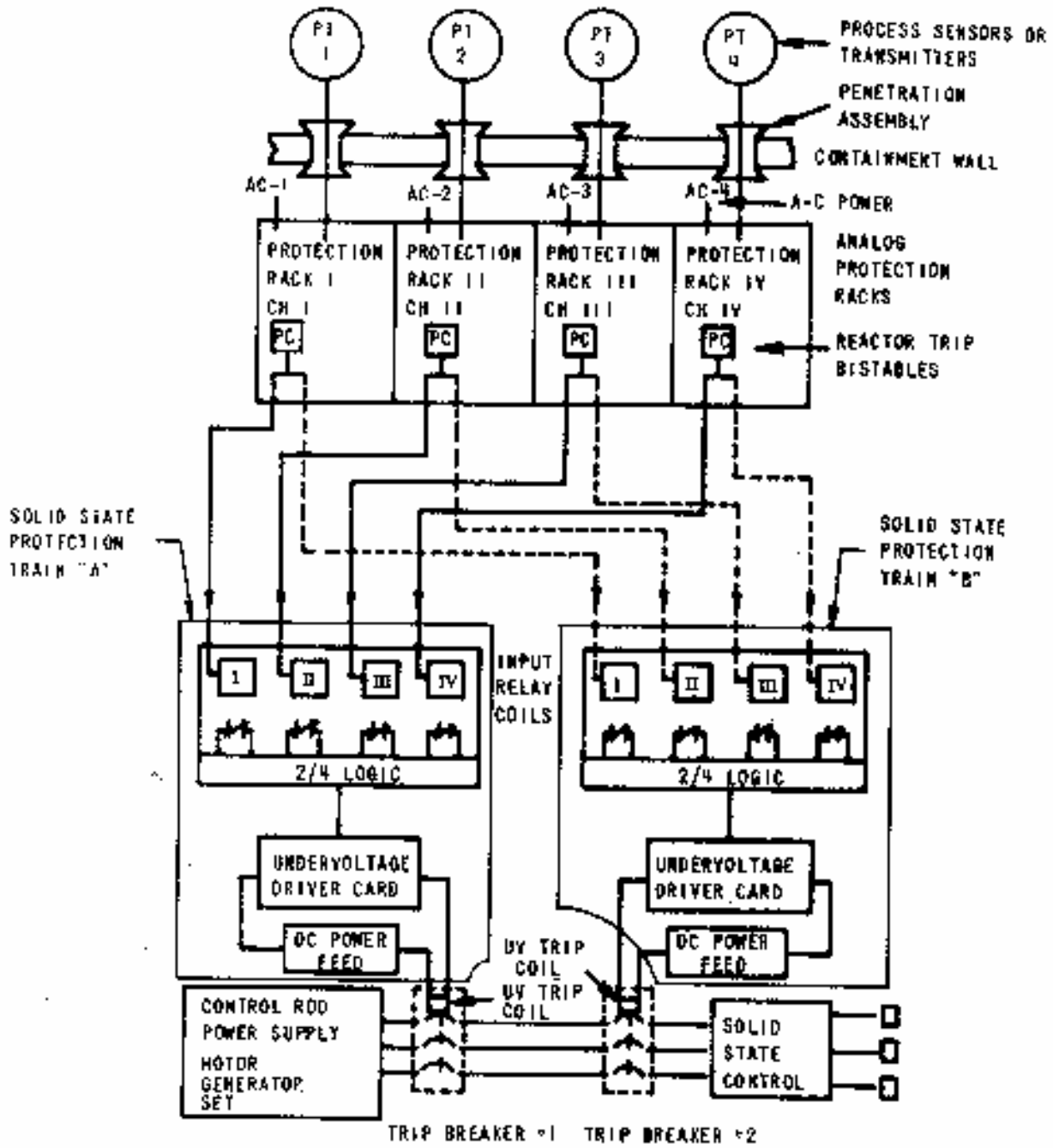
ΔI	–	NEUTRON FLUX DIFFERENCE BETWEEN UPPER AND LOWER LONG ION CHAMBERS
A_1 to A_2	–	LIMIT OF F(ΔI) DEADBAND (+7 TO -19)
B_1 and B_2	–	SLOPE OF RAMP; DETERMINES RATE AT WHICH FUNCTION REACHES ITS MAXIMUM VALUE ONCE DEADBAND IS EXCEEDED
C_1 and C_2	–	MAGNITUDE OF MAXIMUM VALUE THE FUNCTION MAY ATTAIN

NOTE:
- NOTE 1 IN TABLE 3.3.1-1 OF THE TECHNICAL SPECIFICATIONS GIVES THE REDUCTION FUNCTIONS FOR THE OTΔT AND OPΔT SETPOINTS.
- $F_2(\Delta I) = 0$ FOR ALL VALUES OF ΔI

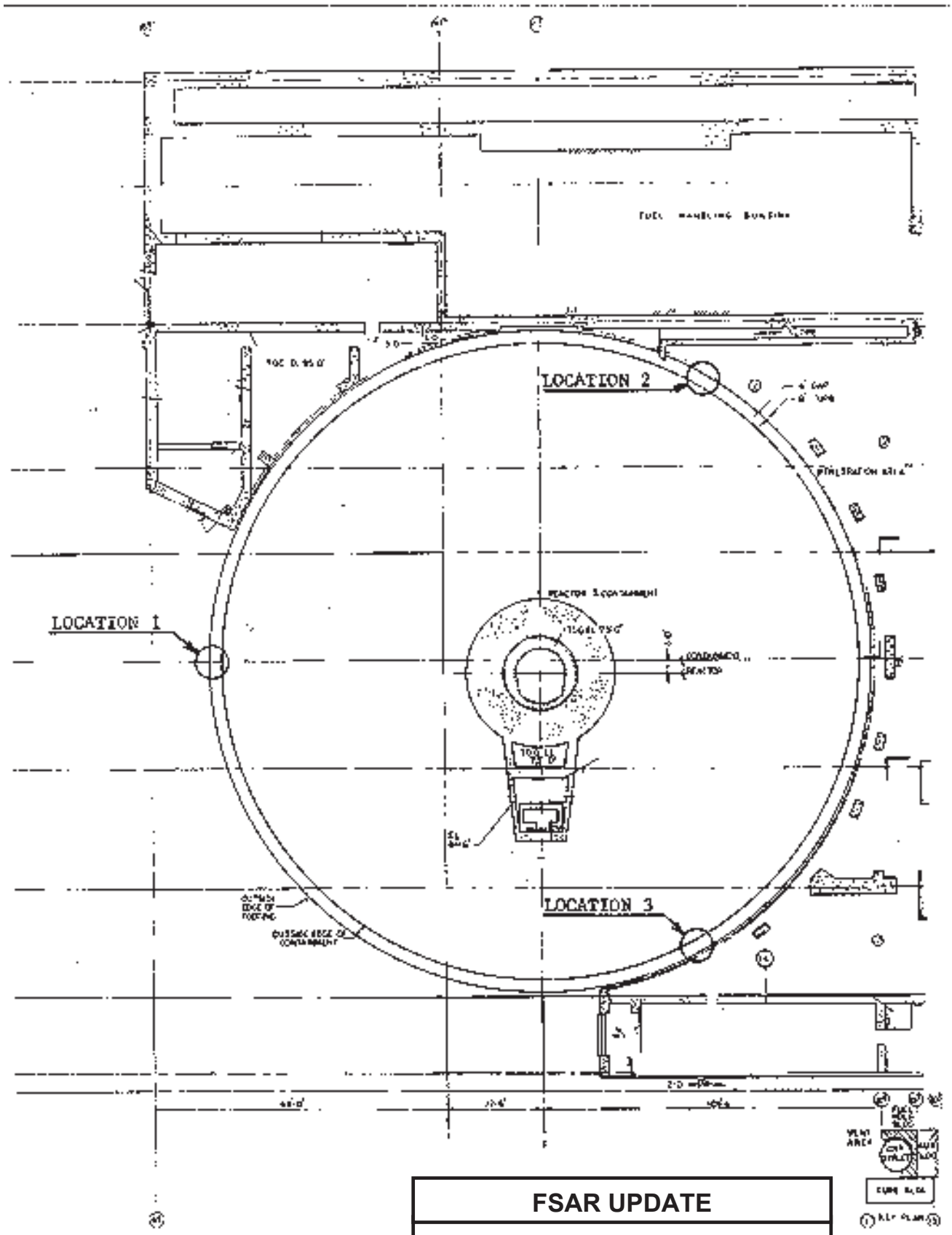
FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.2-2 SETPOINT REDUCTION FUNCTION FOR OVERPOWER AND OVERPRESSURE ΔT TRIPS



FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.2-4 PRESSURIZER SEALED REFERENCE LEG LEVEL SYSTEM

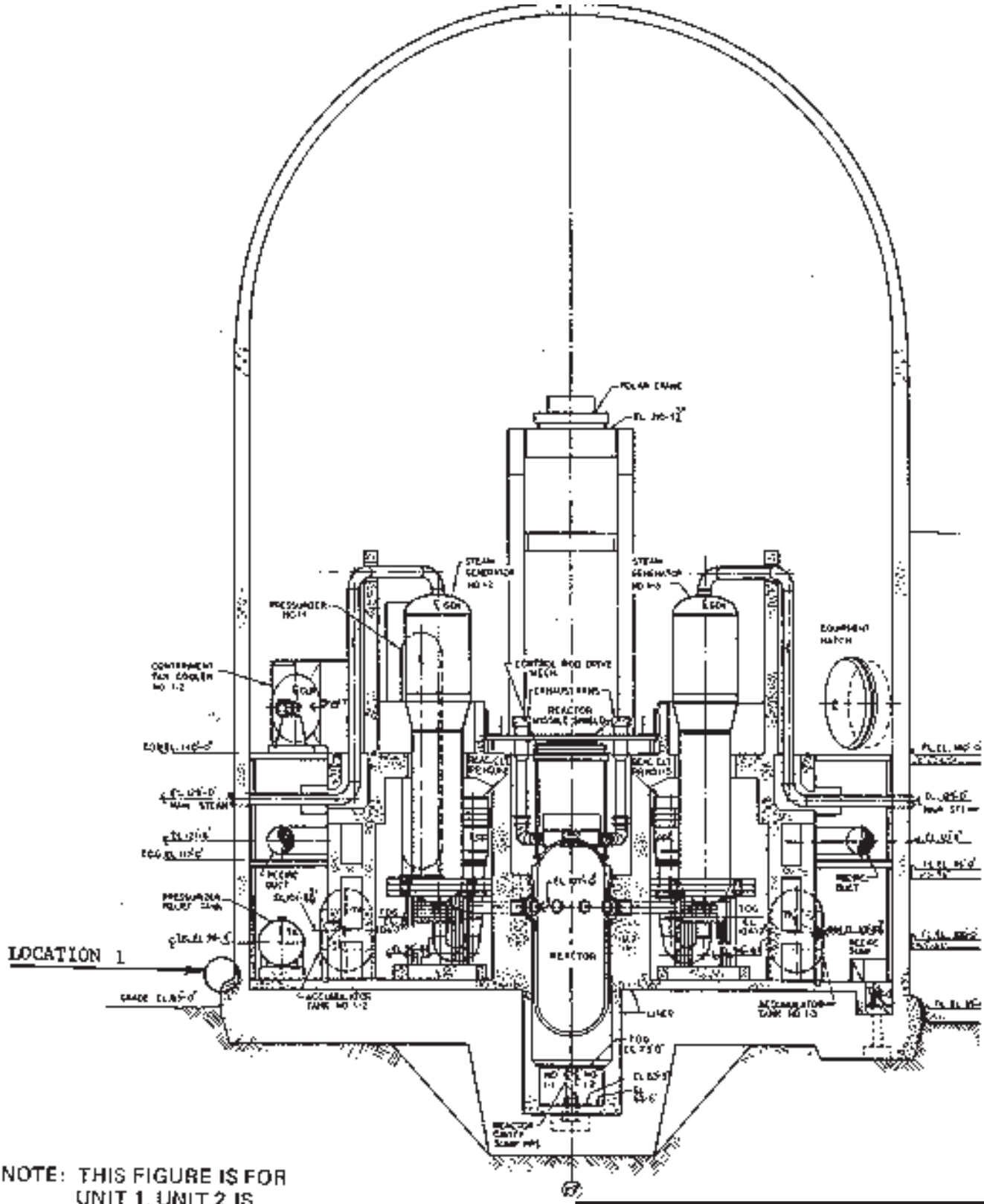


FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.2-5 DESIGN TO ACHIEVE ISOLATION BETWEEN CHANNELS



NOTE: THIS FIGURE IS FOR UNIT 1, UNIT 2 IS OPPOSITE HAND

FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.2-6 (Sheet 1 of 2) SEISMIC SENSOR LOCATIONS

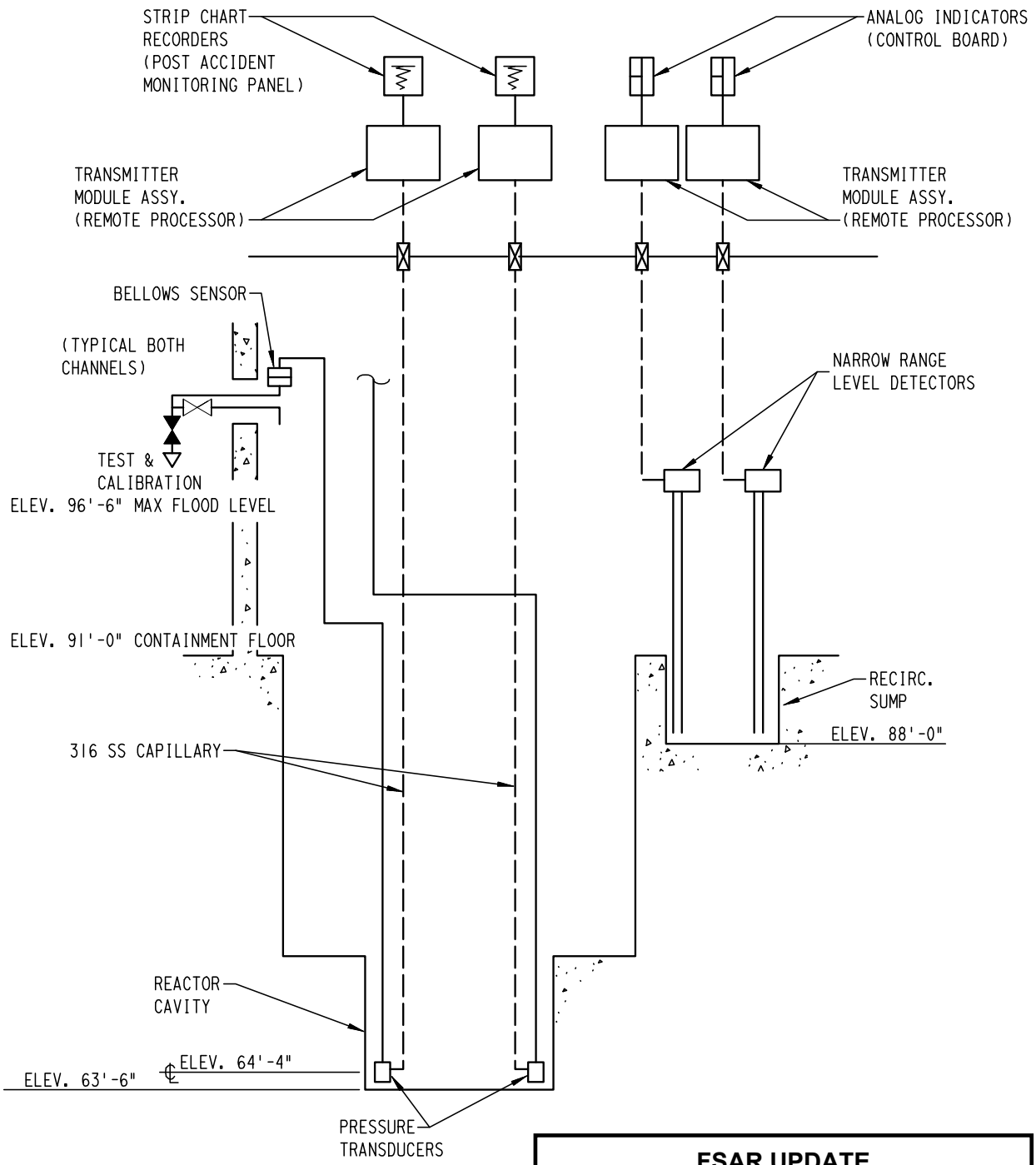


NOTE: THIS FIGURE IS FOR UNIT 1, UNIT 2 IS OPPOSITE HAND

FSAR UPDATE

UNITS 1 AND 2
DIABLO CANYON SITE

FIGURE 7.2-6 (Sheet 2 of 2)
SEISMIC SENSOR LOCATIONS

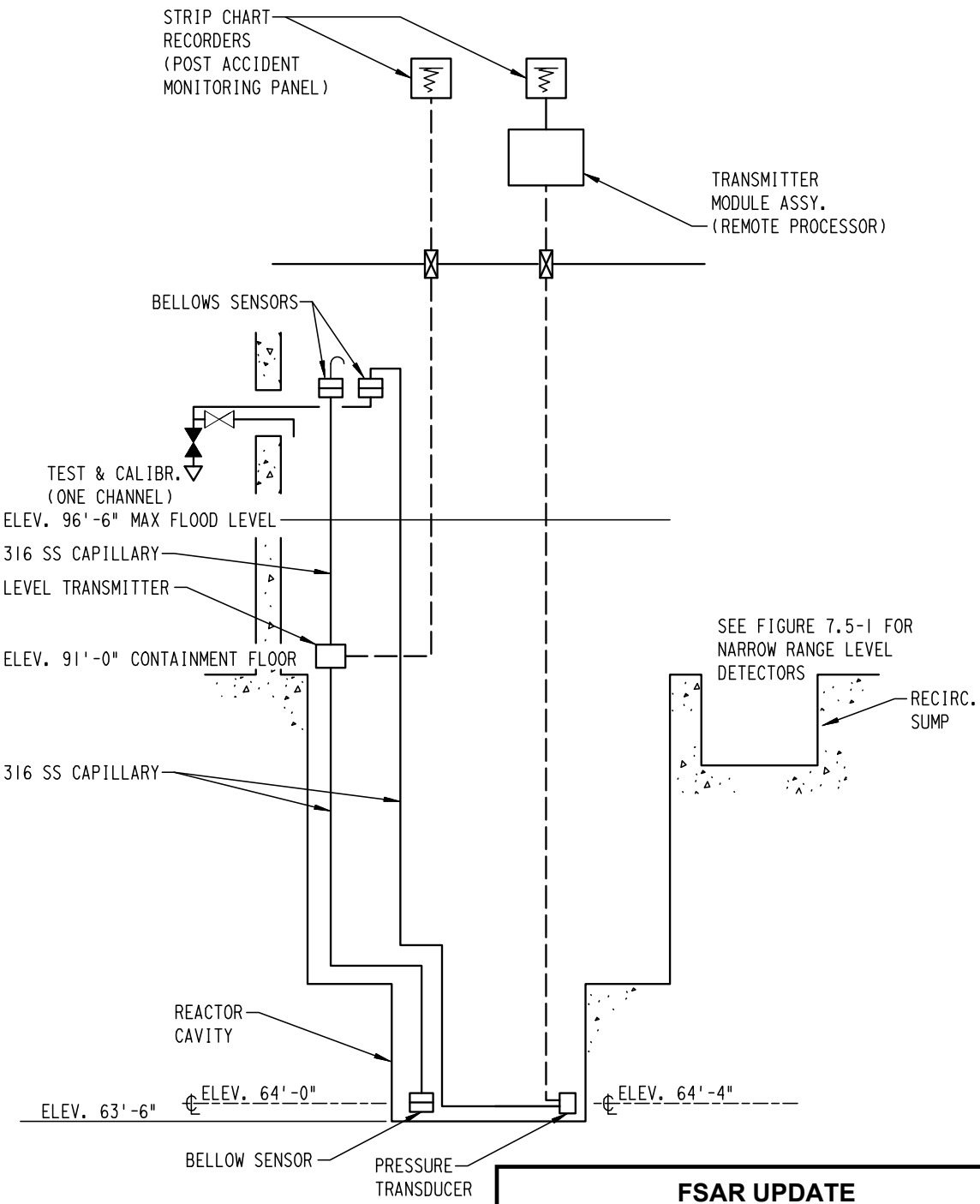


NOTE:
Refer to Figure 7.5-1B for
Unit 2 Wide-Range Diagram

FSAR UPDATE

UNITS 1 AND 2
DIABLO CANYON SITE

FIGURE 7.5-1
CONTAINMENT WATER LEVEL INDICATION
(NOT AN ACTUAL LAYOUT)

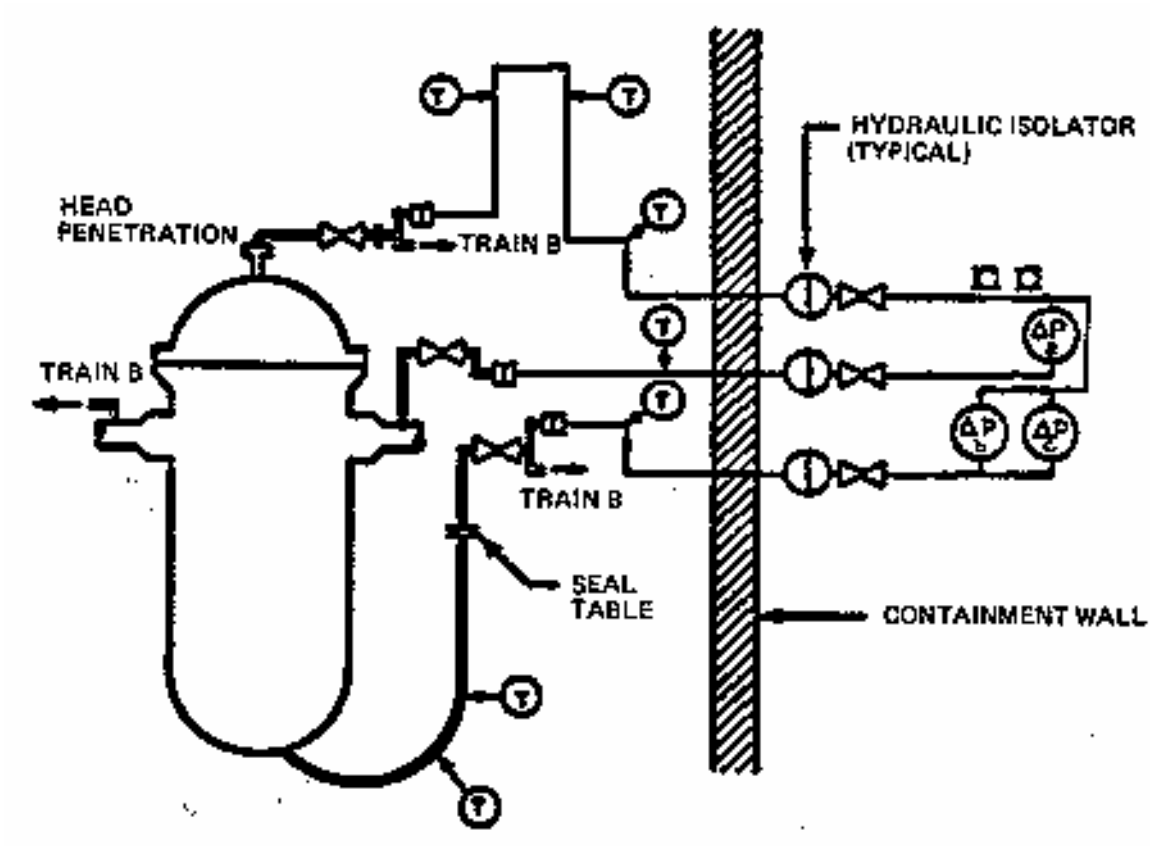


FSAR UPDATE

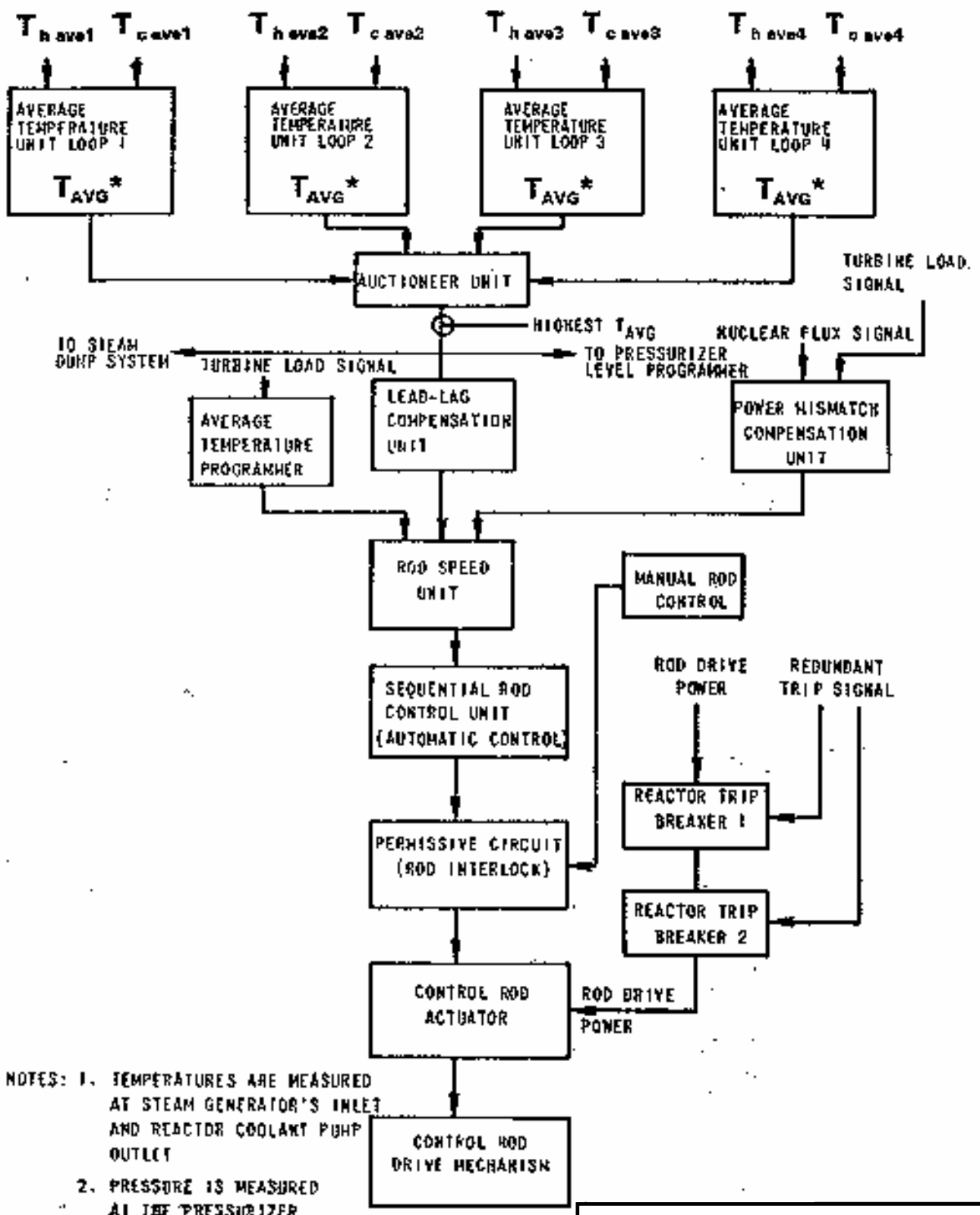
UNIT 2
DIABLO CANYON SITE

FIGURE 7.5-1B

CONTAINMENT WATER LEVEL WIDE-RANGE INDICATION WITH INSTALLED SPARE WIDE-RANGE LEVEL TRANSMITTER IN SERVICE (NOT AN ACTUAL LAYOUT)



FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.5-2 REACTOR VESSEL LEVEL INSTRUMENTATION PROCESS CONNECTION SCHEMATIC (TRAIN A)



NOTES: 1. TEMPERATURES ARE MEASURED AT STEAM GENERATOR'S INLET AND REACTOR COOLANT PUMP OUTLET

2. PRESSURE IS MEASURED AT THE PRESSURIZER

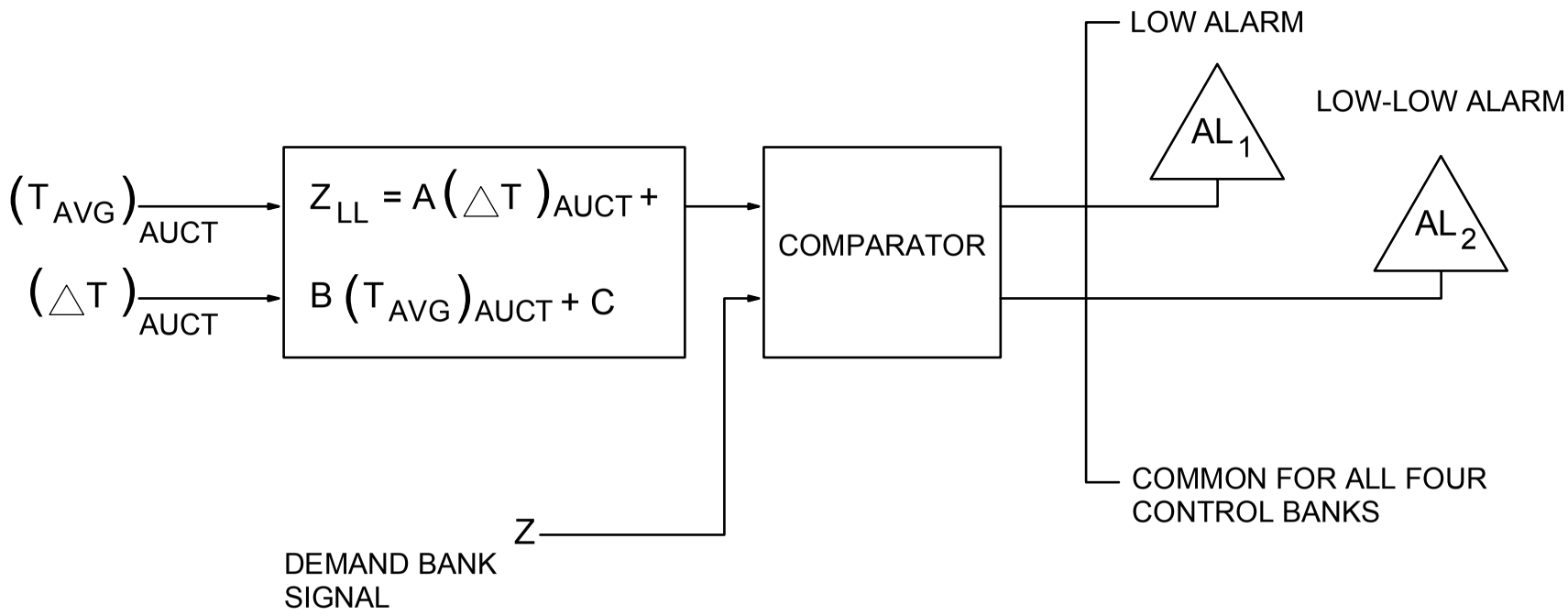
$$* \quad T_{AVG} = \frac{T_{h\,ave\,i} + T_{c\,ave\,i}}{2}$$

i = Loop numbers 1 → 4

FSAR UPDATE

UNITS 1 AND 2
DIABLO CANYON SITE

FIGURE 7.7-1
SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEM

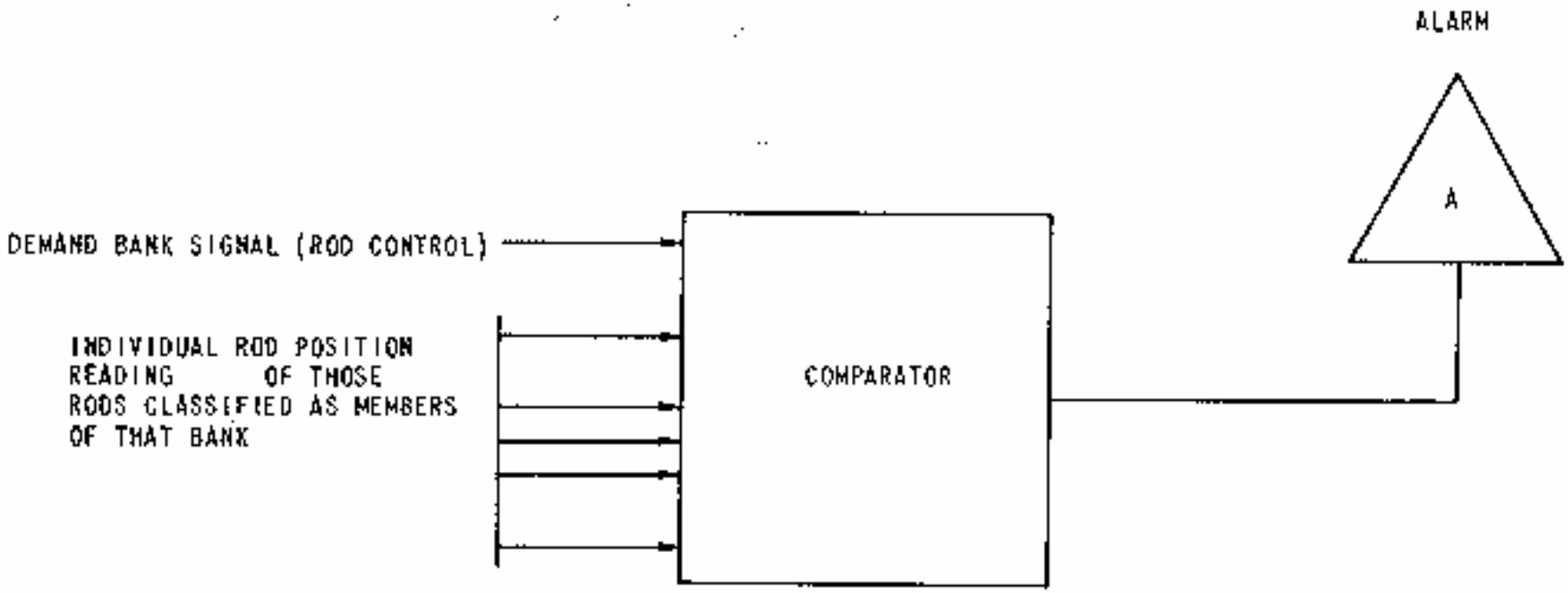


TYPICAL OF ONE CONTROL BANK

NOTES:
1. The PPC is used for the comparator network.
2. Comparison is done for all control banks.

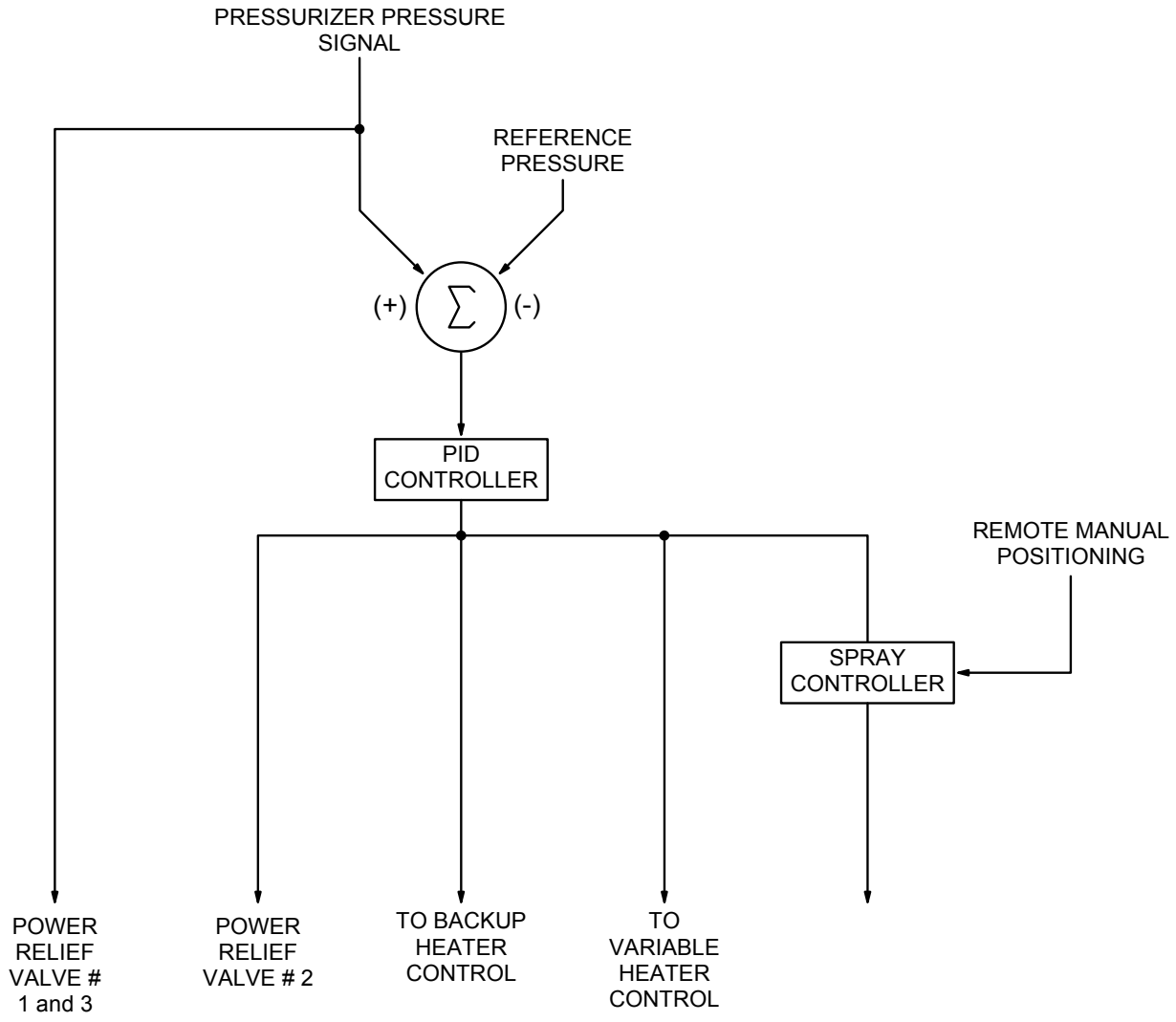
FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.7-2 CONTROL BANK ROD INSERTION MONIOTOR

Revision 16 June 2005



NOTE:
1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR COMPUTER INPUTS.
2. THE COMPARATOR WILL ENERGIZE THE ALARM IF THERE EXISTS A POSITION DIFFERENCE GREATER THAN A PRESENT LIMIT BETWEEN ANY INDIVIDUAL ROD AND THE DEMAND BANK SIGNAL.
3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS.

FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.7-3 ROD DEVIATION COMPARATOR



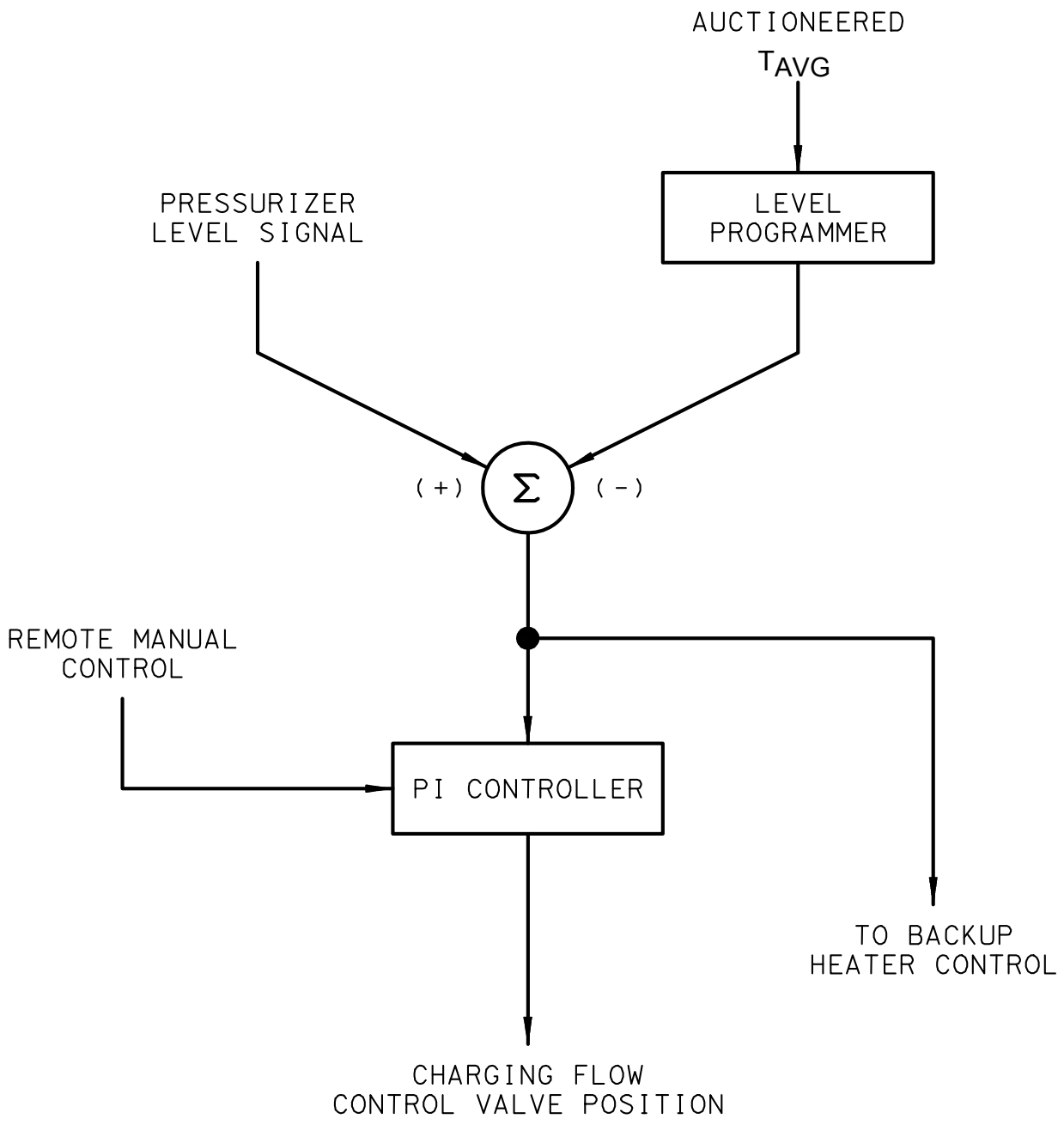
Note:
Valve 1 = PCV 456
Valve 2 = PCV 474
Valve 3 = PCV 455C

FSAR UPDATE

UNITS 1 AND 2
DIABLO CANYON SITE

FIGURE 7.7-4
BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM

Revision 16 June 2005

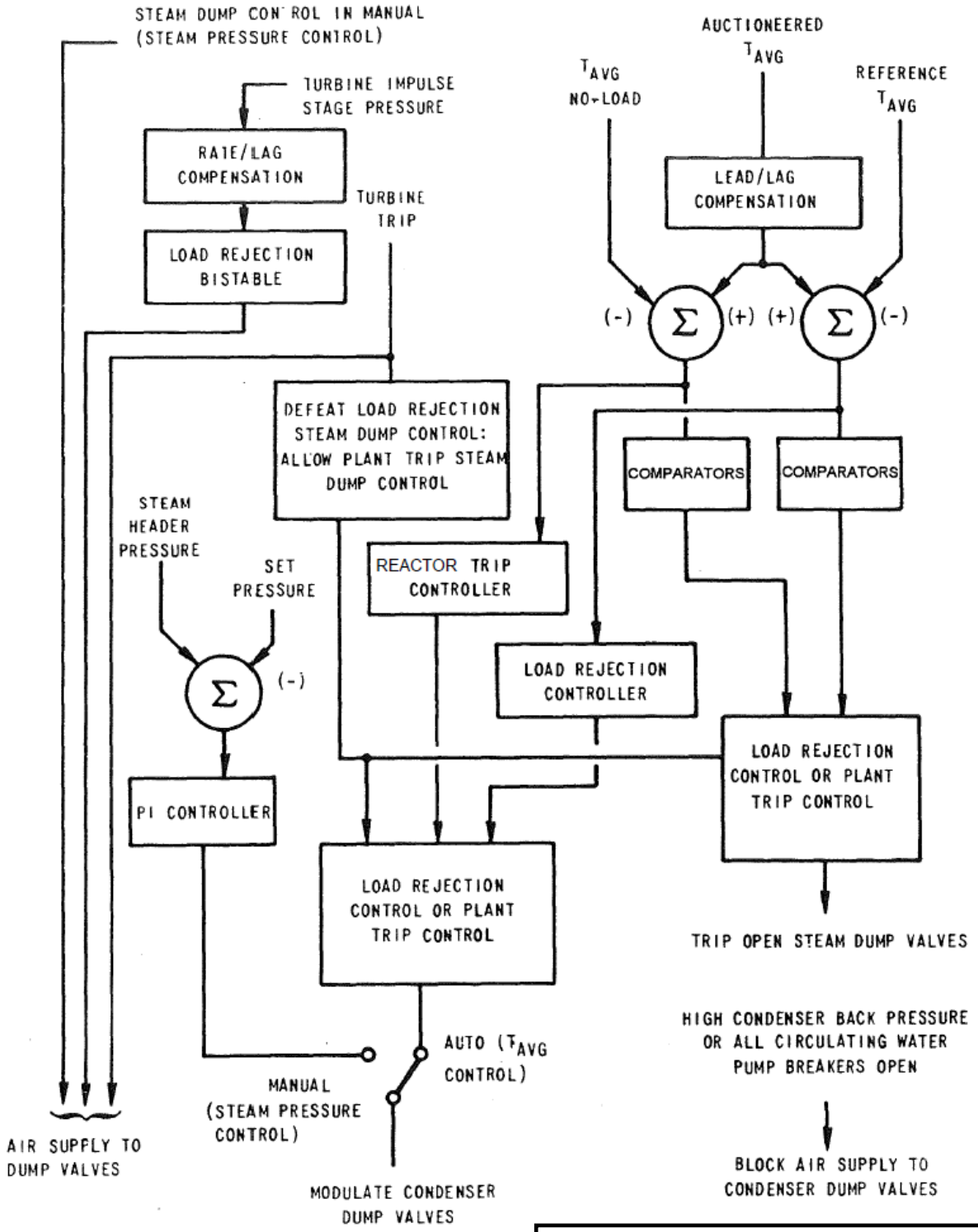


FSAR UPDATE

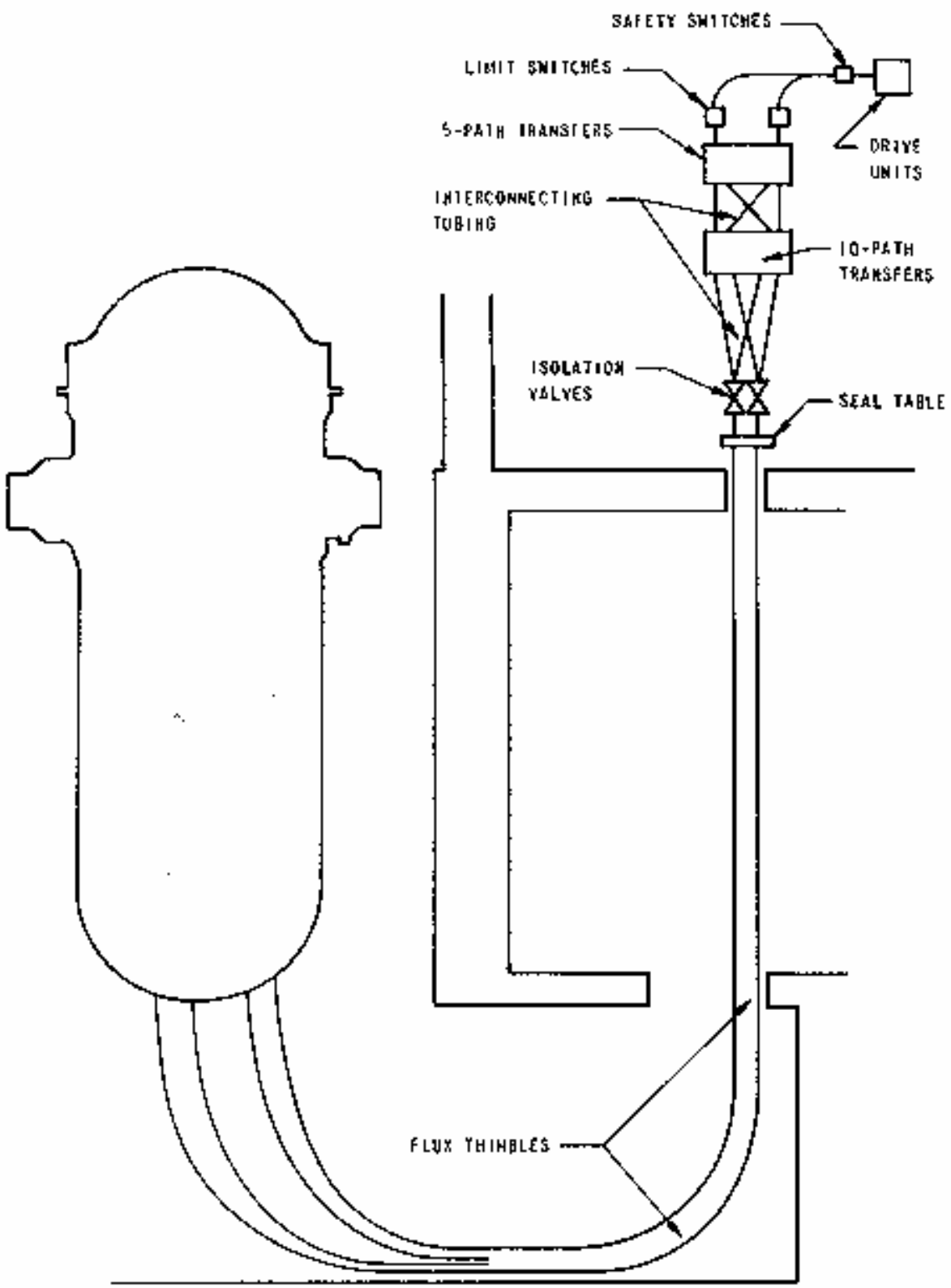
UNITS 1 AND 2
DIABLO CANYON SITE

FIGURE 7.7-5
BLOCK DIAGRAM OF PRESSURIZER LEVEL CONTROL SYSTEM

Revision 21 September 2013



FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.7-8 BLOCK DIAGRAM OF STEAM DUMP CONTROL SYSTEM



FSAR UPDATE
UNITS 1 AND 2 DIABLO CANYON SITE
FIGURE 7.7-9 BASIC FLUX MAPPING SYSTEM